Cloud Security Playbook Volume 1

February 11, 2025

Version 1.0

DISTRIBUTION STATEMENT A. Approved for public release: distribution is unlimited.

Approved By

MARTIN.CHARLES.L.1171456467 Digitally signed by MARTIN.CHARLES.L.1171456467 Date: 2025.02.21 15:02:45 -05'00'

February 21, 2025

Charles L. Martin

Date

Cybersecurity Lead
Cloud and Software Modernization Directorate
Department of Defense Office of the Chief Information Officer-Information Enterprise

LAMB.GEORGE.WILLIE.IV.1506724321 Digitally signed by LAMB.GEORGE.WILLIE.IV.1506724321 Date: 2025.02.21 14:58:40 -05'00'

February 21, 2025

George Lamb

Date

Director
Cloud and Software Modernization Directorate
DoD CIO, DCIO-Information Enterprise

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our readers, and do not constitute or imply endorsement by the Department of any non-Federal entity, event, product, service, or enterprise.

Table of Contents

List of Figures

List of Tables

Introduction

> "Individuals and organizations across the country rely on cloud services every day, and the security of this technology has never been more important. Nation-state actors continue to grow more sophisticated in their ability to compromise cloud service systems." – Secretary of Homeland Security, April 2024 [1].

The Department of Defense (DoD) hosts many of its server-side capabilities in various clouds. Cybersecurity can be as good in a cloud as in a non-cloud (on premises) environment, and since the Cloud Service Provider (CSP)[1] maintains the cloud services, it can be even better. CSPs offer significant cybersecurity services that help reduce cybersecurity risk. In general, CSPs are responsible for both the physical security and cybersecurity of the cloud infrastructure, while Mission Owners (MO) are responsible for the cybersecurity of the software they host in the cloud. But MOs are also responsible for securing and properly configuring and instantiating the cloud services that they use.

Proper cloud security[2] involves numerous actions. This playbook describes the most important actions to take to secure DoD capabilities in a cloud and reduce cybersecurity risk. Many of the plays described involve more detail than can be included here, so this playbook includes numerous references to documents that provide those details. Implementing all the applicable plays will significantly enhance cybersecurity and thus reduce mission risk.

The Cloud Security Playbook is divided into two volumes. This is the first volume.

Audience

This playbook is intended for Mission Owners, Software Development Managers, developers, and organizations that are developing software (or who have acquired software) to host in a cloud, including those using cloud native services.

Purpose

This document was created to make it easy to improve the cybersecurity of applications hosted in a cloud. It does not attempt to address all threats or to provide a comprehensive compendium of cloud security. Instead, it focuses on addressing the most common cloud security threats and vulnerabilities. It is also intended to help a Mission Owner hosting

[1] The definition of CSP and other common cloud terms can be found in Appendix B. Glossary.

[2] In this Playbook, the term "security" is synonymous with "cybersecurity," unless it is prefaced with "physical".

software in a cloud to obtain an Authorization to Operate (ATO) more rapidly. It pulls together information from numerous recent authoritative sources.

Although this document is not a tutorial on cloud security, it also introduces important concepts that are fundamental to cloud security, such as the shared security model, and it points to useful documents so that MOs know where to find more details.

There are many threats and vulnerabilities related to cloud security. Each play in this playbook contains an actions section that describes several actions that mission owners should take to mitigate these cloud vulnerabilities to reduce cybersecurity risk to their systems and missions.

Play Reading Order

Plays may be read in any order, but some plays use concepts described in earlier plays. It is not necessary to implement the plays in order. Indeed, the implementation of many plays may be accomplished in parallel. However, some plays rely on earlier plays having been accomplished. For example, a program should select a cloud (Play 3) before establishing network access to it (Play 5).

Begin with this volume, which includes many important plays to implement early, then read volume 2, which includes some more advanced plays, including plays on containers and microservices, defending DevSecOps Pipelines, and securing Artificial Intelligence (AI) systems; some of the advanced plays in volume 2 may not apply to all programs.

Why Cloud Security?

Cloud Service Providers are responsible for the physical security of their datacenters. They are also responsible for providing secure services. But cybersecurity in a cloud is a shared responsibility between the CSP and the MO. For example, the MO is responsible for properly configuring the cloud services, for example enabling encryption and logging. The MO is also responsible for any software they host in the cloud. This Playbook is intended to help MOs and others secure their systems in a cloud.

Software Development Managers and developers naturally focus on delivering new capabilities and fixing issues with existing software. Few developers focus on security, assuming that the security team is responsible for that. Yet secure systems require developers to implement them, and the more security that can be automated, the better. The risk can be greatly reduced by implementing security from the beginning of a project throughout the software lifecycle, involving developers as well as operations personnel in the security of the system.

The National Institute of Standards and Technology (NIST) defines a **threat** as “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”[3]

A **vulnerability** is a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”[4]

To understand *why* security must be implemented properly in a cloud, it is helpful to be aware of common threats and vulnerabilities for cloud services. The next few sections summarize some relevant recent information in those areas.

Top Threats

The next list comes from the *Top Threats to Cloud Computing: Pandemic Eleven, Cloud Security Alliance*, 2022, [2]. It was compiled from an industry survey, so it is not DoD-

[3] Source: https://csrc.nist.gov/glossary/term/threat

[4] Source: https://csrc.nist.gov/glossary/term/vulnerability.

specific. This list contains several important threats that apply to software hosted in a cloud.

1. Insufficient ID, Credential, Access and Key Management, Privileged Accounts
2. Insecure Interfaces and Application Programming Interfaces (APIs)
3. Misconfiguration and Inadequate Change Control
4. Lack of Cloud Security Architecture and Strategy
5. Insecure Software Development
6. Unsecure Third-Party Resources
7. System Vulnerabilities
8. Accidental Cloud Data Disclosure/ Disclosure
9. Misconfiguration & exploitation of cloud workloads[5]
10. Organized Crime/ Hackers/ Advanced Persistent Threat (APT). For the DoD, the APT is the source of many threats.
11. Cloud Storage Data Exfiltration

Artificial Intelligence Threats

Artificial Intelligence (AI), including Machine Learning (ML) is being used more since the development of Generative AI Large Language Models (LLM).[6] AI impinges on cloud security in several ways.

- AI threats
- AI use for cyber defense
- Securing AI systems in a cloud

This section discusses threats posed by AI. AI use for cyber defense is discussed in Play 12, while securing AI systems is the focus of Play 23 in Volume 2.

The United Kingdom's National Cyber Security Centre (NCSC) offers these points on AI threats in *The Near-term Impact of AI on the Cyber Threat*, 2024 [3].

Key judgements

- AI will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years. However, the impact on the cyber threat will be uneven, as expressed in Table 1, from [3].

[5] See the glossary for a definition of cloud workload.

[6] See the glossary for definitions of AI, ML, Generative AI and LLM.

Table 1. Extent of Capability Uplift Caused by AI over the Next Two Years

	Highly capable state threat actors	**Capable state actors, commercial companies selling to states, organized cyber-crime groups**	**Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists**
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift (from low base)
Tools (malware, exploits)	Realistic possibility of uplift	Minimal uplift	Moderate uplift (from low base)
Lateral movement	Minimal uplift	Minimal uplift	No uplift
Exfiltration	Uplift	Uplift	Uplift
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations - increasing volume of successful compromise of devices and accounts.

- The AI threat comes from evolution and enhancement of existing Tactics, Techniques and Procedures (TTPs).
- Cyber threat actors are already using AI.
- AI provides capability uplift in reconnaissance and social engineering, making both more effective, efficient, and harder to detect.
- More sophisticated uses of AI in cyber operations are highly likely to be restricted to threat actors with access to quality training data, significant expertise (in both AI and cyber), and resources, such as state actors.

- AI will almost certainly make cyber-attacks against the nation more impactful because malicious actors will be able to analyze exfiltrated data faster and more effectively and use it to train AI models.
- AI lowers the barrier for novice cyber criminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This enhanced access will likely contribute to the global ransomware threat.
- In the near future, commoditization of AI-enabled capability in criminal and commercial markets will almost certainly make improved capability available to cybercriminals and state actors.

Adversarial Techniques

MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK®) is a knowledge base of adversarial techniques. This service is described in Appendix A.

The 2024 Red Canary Threat Detection Report, though not specific to cloud threats, stated that cloud accounts was the fourth most prevalent ATT&CK technique they detected, increasing by a factor of 16 over the previous year. This technique uses cloud accounts to attack from within the cloud.

Common Vulnerabilities

There are several vulnerabilities common to software hosted in a cloud. A few of these are listed below. These can be addressed by various plays in this playbook, as indicated.

- Cloud Misconfiguration (not configuring a cloud service offering properly), is one of the most common errors in securing cloud environments, and it has been identified as a key vulnerability to exploit by [2], among others. Examples of misconfigurations for some cloud services can be found in Appendix A. This playbook discusses a way to mitigate this vulnerability in Play 6.
- Failure to follow good key (or secrets) management practices, addressed Play 14.
- Failure to implement the Principle of Least Privilege (PoLP), addressed in Plays 1 and 7.

The following list contains the most common security oversights in the cloud, according to the *Cloud Threat Report*, Vol. 7, 2024 [4]. For each item, there is at least one play that mitigates each vulnerability, as indicated in parenthesis.

- Hard-coded credentials, for example developers sometimes check-in files to the source code repository that include passwords or security tokens. There are tools that can search for these and identify them. (Play 7)
- Weak authentication (Play 7)

- Disabled logging (Play 10)
- No automated backup (Play 17, and backup access in Play 7)
- Unencrypted data at rest (Play 13)
- Inefficient alert handling (Play 11, Play 12)
- Exposed sensitive data (Play 13)
- Publicly exposed services, such as publicly accessible storage service buckets (Play 13)
- Unpatched vulnerabilities (see patching in Play 9 and Play 20 in Volume 2)

For more information, see Appendix A for resources on adversarial techniques and countermeasures.

Top Mitigation Strategies

Given all those vulnerabilities, how should they be mitigated? That is what this playbook addresses.

The following list of the top cloud security mitigations is from the *Top Ten Cloud Security Mitigation Strategies*, National Security Agency (NSA), 2024 [5]. The present document includes these mitigations, and each has at least one play associated with each one, indicated in parentheses.

1. Uphold the cloud shared responsibility model (Play 2)
2. Use secure cloud Identity and Access Management (IAM) practices (Play 7)
3. Use secure cloud key management practices (Play 14)
4. Implement network segmentation and encryption in cloud environments (Play 16)
5. Secure data in the cloud (Play 13)
6. Defend Continuous Integration/Continuous Delivery (CI/CD) environments (Play 20 in Volume 2)
7. Enforce secure automated deployment practices through Infrastructure as Code (IaC) (Play 6)
8. Account for complexities introduced by hybrid cloud and multi-cloud environments (Play 18)
9. Mitigate risks from managed service providers in cloud environments (Plays 3, 4, 12)
10. Manage cloud logs for effective threat hunting (Play 10)

The Orca Security *State of Cloud Security Report 2024* [6] offers some other recommendations.

- Patch strategically – although vulnerabilities should be patched quickly, patch those that reduce the most risk to the mission first.

- Do not neglect cloud workloads – ensure that all workloads in the cloud are using software that is currently supported by the vendor, and which receives vendor updates. Eliminate unsupported cloud workloads. This also reduces unnecessary cost.
- Maintain an updated cloud asset inventory and remove workloads from the cloud that are not in that inventory (Play 9).
- Implement the Principle of Least Privilege (PoLP) (Plays 1 and 7).
- Know where your crown jewels are – know where in the cloud the organization's most critical assets are located. Implement the most stringent security for these assets.
- Monitor and mitigate web and API risks – Implement robust security monitoring and regularly audit configurations to prevent mismanagement and misuse. Play 9 shows a way to do this automatically.
- Leverage malware detection (Play 10, Play 12).
- Use Infrastructure as Code (Play 6).

Physical and Virtual Isolation

Physical isolation means there is a different physical machine for each instance of each subsystem. The use of clouds, such as the Amazon Web Services (AWS) US GovCloud or Microsoft Azure for DoD or Government, approved at the appropriate impact level should alleviate that need for physical isolation, other than what the CSP provides. For example, US GovCloud is physically isolated from the commercial regions.

If it is deemed necessary based on additional security concerns, it is possible to reserve machines in a cloud. However, that is generally not a good practice, as it is not cost effective, and it removes some of the cloud's advantages, such as automatic scalability.

Play 1. Prepare the Organization

Before embarking on a cloud hosted project, the organization in charge should prepare by beginning to implement the suggestions in this play.

Define the roles and responsibilities of those who will have access to cloud services and the mission application. Use the Principle of Least Privilege (PoLP) access. That is, grant the minimum privileges necessary for that role to carry out their responsibilities.

Train the workforce on cloud security. Train them on what is unique in the cloud environment from a security perspective. This Playbook will help.

Set up a cloud governance team. Cloud governance is the process of defining, implementing, and monitoring a set of policies for cloud use by an organization. Risk management, compliance and administration are all elements of governance.

Why Cloud Governance

Cloud Governance helps to do the following.[7]

- Improve continuity and visibility across projects and missions.
- Optimize the use of resources and cloud services across projects. This includes cloud cost management.
- Improve operational efficiency by eliminating productivity bottlenecks and simplifying management processes.
- Set policies and ensure compliance with them. (See also Play 9).
- Minimize cybersecurity risks by setting up cybersecurity policies, including those related to identity and access management and continuous monitoring, so that cybersecurity teams are better able to identify and mitigate vulnerabilities and improve cloud security.

Cloud Governance Team

Create stakeholder forums, policies, roadmaps, technical standards (architecture and application development), data connectivity standards, resiliency and failover standards, and cloud migration approaches.

[7] Source: https://www.redhat.com/en/topics/automation/what-is-cloud-governance

The cloud governance team should enable cloud cost management. All major CSPs offer cost management services. This can both help to lower costs and identify all running Virtual Machines (VMs) and other used cloud services.

In that vein, the cloud governance team should create a role responsible for culling unused VMs and other cloud services. This has two advantages. First, it reduces the attack surface, and secondly it reduces costs by not accruing charges for unused services.

Consider a DevSecOps approach to developing new capabilities. Such an approach includes involving security throughout the software development lifecycle. More on DevSecOps can be found in the DoD CIO Library.

DoD Cloud Contract Compliance

There are several DoD cloud contract compliance requirements of which the governance team should be aware. These are stated in the *DoD Joint Warfighter Cloud Capability (JWCC) & Next Steps to Rationalize Cloud Use Across the DoD*, DoD CIO, 2023 [7], and include the following.

- Cloud contracts must include the cloud policy and contract clauses defined in Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 239.76.
- Compliance with the *DoD Cloud Computing Security Requirements Guide (CC SRG)*,[8] including only using cloud services that have been granted a DoD provisional authorization at the appropriate Impact Level. For a discussion of Impact Levels, see Play 3.
- Annual penetration testing and provisions in all contracts for classified cloud services that enable DoD red teams to conduct independent, adversarial assessments of the cloud environment that emulate the most capable, nation-state threats, as discussed in Play 12.
- Registering cloud use in System Network Approval Process (SNAP). See more in Play 5.
- Use of an approved Cloud Access Point (CAP). Commercial cloud services used for Impact Level 4 or higher must be connected to customers through the Defense Information Systems Network (DISN) Enterprise CAP or through a Component CAP solution approved by the DOD CIO. For more, see Play 5.

[8] The CC SRG is a set of files that can be downloaded here: https://public.cyber.mil/dccs/dccs-documents/.

- Cloud use will be supported by Cybersecurity Service Providers (CSSPs) in accordance with *DoD Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations* [8]. For more on CSSPs, see Play 12.

Cloud Migration Strategy

Develop a cloud migration strategy. This is a high-level plan on what to migrate. It is often best to use a phased approach, in which one or a few applications are migrated at a time. Create a repeatable migration process, backed with trained personnel and playbooks for onboarding. Establish a cloud migration budget to implement the cloud migration strategy. Create a team to help other projects through the migration process.

Cloud Exit Strategy

Create a cloud exit strategy, which is a plan to enable an organization to switch to another CSP, if necessary. It should include consideration of:[9]

- Data migration, including a strategy for migrating the data, either over a network or through physical devices, partly based on data volume and data formats.
- Application/workload migration, including a high-level assessment strategy to determine which applications or workloads to migrate. Actual workloads to migrate would be decided later, if the Exit Strategy is executed.
- Plan for a phased migration approach. Migrate some data and applications, then migrate more.
- Integration. Keep the systems integrated as portions migrate.
- Addressing upskilling personnel on the new cloud platform.
- Cybersecurity, including migrating encrypted data and its keys.
- Testing to validate and test the cybersecurity of the systems in the new environment.
- Continuous cybersecurity monitoring of the migration, in addition to monitoring both the source and target cloud environments.

In addition, ensure that the Service Level Agreement (SLA) with the CSP includes the following:[10]

- Establish the obligations of the existing CSP in the event of a transfer of data and applications to another CSP or back to the DoD.

[9] Source: Creating a Cloud Exit Strategy.

[10] Source: Top 3 Considerations for a Cloud Exit Strategy.

- Include a clause that obligates the CSP to support the MO in transferring the data and applications to the new host.
- If appropriate, set a transition period during which the original CSP would continue to provide service. (Note: this may not be necessary, as most CSP services are pay-as-you-go.)

Cybersecurity Activities

Be aware of cybersecurity activities for which the Mission Owner (MO) is responsible. The following table lists those activities. It is from *Directive-type Memorandum (DTM) 24-001, DoD Cybersecurity Activities Performed for Cloud Service Offerings*, DoD CIO, 2024 [9].

The following acronyms appear in the table but are not defined there: Impact Level (IL) (discussed in Play 3), DoD Cyber Red Team (DCRT), DoD Cyber Assessment Team (DCAT), and Cybersecurity Service Provider (CSSP) (see Play 12).

Table 2. Cybersecurity Activities for Cloud Service Offerings

Cybersecurity Activities		IaaS			PaaS			SaaS		
		IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6
Identify	Vulnerability Assessment and Analysis (VAA)									
	External Vulnerability Scans (EVS)	o	o	o	o	o	o	o	o	o
	Web Vulnerability Scans (WVS)	o	o	o	o	o	o	o	o	o
	External Assessment (Annual Assessment – See [9] Paragraph 3.a.(2))									
	DCRT Operations	●	●	●	●	●	●	●	●	●
	DCAT Operations	o	o	o	o	o	o	o	o	o
	Penetration Testing	o	o	o	o	o	o	o	o	o
	Intrusion Assessment	o	o	o	o	o	o	o	o	o
Protect	Awareness and Training	o	o	o	o	o	o	o	o	o
	Endpoint Security Capabilities	o	o	o	o	o	o	o	o	o
	Vulnerability Management Maintenance									
	Apply DoD required security configurations	o	o	o	o	o	o	o	o	o
	Perform actions to mitigate potential vulnerabilities or threats	o	o	o	o	o	o	o	o	o
	Monitor Vulnerability Management Compliance	o	o	o	o	o	o	o	o	o
	Malware Protection	o	o	o	o	o	o	o	o	o

Cybersecurity Activities		IaaS			PaaS			SaaS		
		IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6
Monitor and Detect	Attack Sensing and Warning (AS&W) for Anomalous Events									
	AS&W for Boundary Cyberspace Protection (BCP) Functions	N/A	●	●	N/A	●	●	N/A	●	●
	AS&W at the Application	o	o	o	o	o	o	o	o	o
	Warning Intelligence	●	●	●	●	●	●	●	●	●
	Information Security Continuous Monitoring (ISCM)									
	Maintain continuous visibility into endpoint devices	o	o	o	o	o	o	o	o	o
	Correlate asset and vulnerability data with threat data	★	★	★	★	★	★	★	★	★
	Malware Notification	★	★	★	★	★	★	★	★	★
	Detection Processes									
	Network Security Monitoring and Intrusion Detection for BCP Functions	N/A	★	★	N/A	★	★	N/A	★	★
	Network and Endpoint Security Monitoring at the Enclave Level	o	o	o	o	o	o	o	o	o
	DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program									
	Employ UAM capabilities to detect anomalous insider activity	o	o	●	o	o	●	o	o	●
	Maintain insider threat audit data	o	o	o	o	o	o	o	o	o
	Correlate insider threat audit data with Component Insider Threat Programs	●	●	●	●	●	●	●	●	●
	Cyber Protection Condition (CPCON) and Orders (e.g. TASKORD, Operational Order (OPORD), Fragmentation Order)									
	CPCON and Orders Implementation	o	o	o	o	o	o	o	o	o
	CPCON and Orders Notification and Assistance	★	★	★	★	★	★	★	★	★
Respond	Incident Categorization	★	★	★	★	★	★	★	★	★
	Incident Reporting	★	★	★	★	★	★	★	★	★
	Incident Handling Response	o	o	o	o	o	o	o	o	o
	Incident Response – Law Enforcement (LE)	★	★	★	★	★	★	★	★	★
	Incident Response – Counterintelligence	★	★	★	★	★	★	★	★	★
	Incident Response – Analysis	★	★	★	★	★	★	★	★	★

KEY

"★" = CSSP must perform this cybersecurity activity

"●" = DoD entity must perform this cybersecurity activity; commercial entity cannot be performing this activity

"○" = DoD entity or commercial entity can perform this cybersecurity activity

"N/A" = Not Applicable

Actions

The following actions help prepare an organization for using a cloud.

- □ Set up a cloud governance team.
- □ Develop a cloud migration strategy.
- □ Establish a cloud migration budget to implement the cloud migration strategy.
- □ Create a team to help other projects through the migration process.
- □ Develop organizational policies on cloud usage.
- □ Update workforce position descriptions.
- □ Determine the organizational approach to accessing the cloud.
- □ Create a Cloud Exit Strategy.
- □ Define the roles and responsibilities of those who will have cloud access; use the PoLP.
- □ Train the workforce on cloud security.
- □ Enable cloud cost management.
- □ Be aware of cybersecurity activities for which the MO is responsible, as indicated in in Table 2 above, from [9].

Play 2. Understand the Shared Responsibility Model

The cloud service provider (CSP) is responsible for some security aspects of their services. But the mission owner (MO) is responsible for many aspects of security. For example, the CSP is responsible for the physical security of the servers, but the mission owner is responsible for securing the mission data. **Responsibility varies depending on the service.** For example, when using a virtual machine service such as Amazon EC2 or Azure Virtual Machines (both examples of Infrastructure as a Service (IaaS)), the MO is responsible for securing everything installed on each virtual machine, including the operating system, applications, and data. On the other hand, a cloud database service, such as Azure Cosmos DB or Amazon DynamoDB secures the operating system and database but leaves other tasks to the MO. Figure 1 illustrates the relative differences in security responsibilities between cloud service models: IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS).

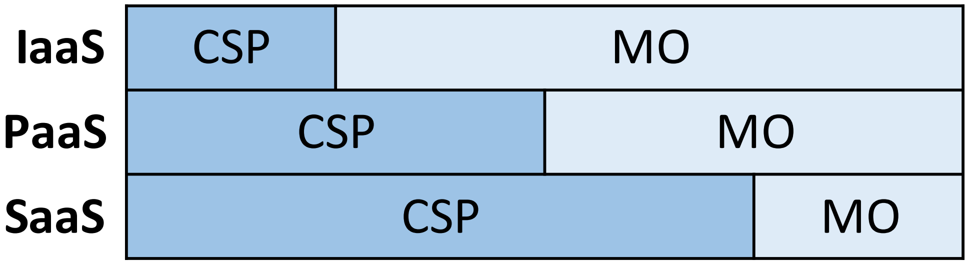

Figure 1. Mission Owner Authorizing Official Risk Decision Security Responsibility

The figure shows that an MO has the most responsibilities for security when using IaaS, and the least with SaaS services. It is important to understand the cybersecurity aspects for which the MO is responsible. Cybersecurity vulnerabilities arise when an MO assumes that the CSP is taking care of something for which the MO is responsible. To avoid that issue, follow best practices, read the CSP’s documentation, and engage directly with the CSP if the responsibility is not clear.

> “Customers should hold the CSP accountable for its part, while the customers must dutifully fulfill their own tenant responsibilities.” – Top Ten Cloud Security Mitigation Strategies, NSA, 2024 [5].

Mission Owner Responsibilities

This section on MO Responsibilities comes from the *Cloud Computing Mission Owner Security Requirements Guide Overview*, Defense Information Systems Agency (DISA), 2024 [10].

“Mission Owner responsibilities include but are not limited to ensuring the following architecture and devices are configured and approved:

- DOD demilitarized zone (DMZ) Extension – Implement cloud network(s) in accordance with the approved architecture for the type of application as defined in the DOD DMZ Security Technical Implementation Guide (STIG) and the Application Security and Development STIG, along with other operating system and application-specific STIGs. For example, a web service or application is typically required to have unrestricted/restricted DMZ zones with appropriate protections for internet/externally facing servers and private/“back-end” zones with appropriate protections for application/database servers and other supporting systems/servers.

- Virtual Datacenter Security Stack (VDSS) – A VDSS provides security capabilities such as firewall, intrusion detection, and intrusion prevention systems. It also provides application security capabilities such as Web Application Firewall (WAF) and proxy systems. The VDSS can reside within or outside of the CSP’s infrastructure (cloud-based or physically). VDSS capabilities can also be provided as a service by a third-party vendor (for IaaS) or a CSP (for IaaS and SaaS). VDSS feeds must be provided to a DOD CSSP performing boundary defense.

- Virtual Datacenter Managed Service (VDMS) – VDMS is designed to provide endpoint protections for Mission Owner applications such as DOD Assured Compliance Assessment Solution (ACAS), host-based/endpoint security solution, Identity and Access Management (IdAM), etc. It provides system management network and Mission Owner cloud service offering support services that form the management plane. VDMS provides secure management network connectivity between the Defense Information Systems Network (DISN), cloud host-based management services, and IdAM services for DOD Common Access Card (CAC) authentication to cloud systems. The VDMS is specifically tailored to operate at all DOD mission Impact Levels. VDMS functionality applies directly to IaaS environments but may not be specifically applicable to PaaS and SaaS Cloud Service Offerings (CSOs) as such functionality may be inherent to the associated CSP and validated through the DOD Provisional Authorization (PA).

- Cloud Storage – Implement Federal Information Processing Standard (FIPS) 140-2/3 compliant, data-at-rest encryption on all DOD files housed in CSP IaaS storage service offerings. The Mission Owner may choose from one or more CSP offerings or methods to accomplish this.

- Host-Based/Endpoint Security – Implement a host-based security suite to monitor servers and endpoints that complies with DOD regulations and Component needs.

Ensure there is a secure (encrypted) connection or path between the endpoint security agents and their control server.

- Vulnerability Scanning – Implement scanning using a vulnerability scanner that complies with DOD regulations and Component needs.
- DOD CAC/Public Key Infrastructure (PKI) – Implement a secure (encrypted) connection or path between the implemented systems/applications and the DOD Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) resources on Non-classified Internet Protocol Router Network (NIPRNet) or Secret Internet Protocol Router Network (SIPRNet) as applicable. Ensure all users connect to Mission Owner cloud NIPRNet and SIPRNet networks via a DoD CAC/PKI unless otherwise approved through the DOD Security/Cybersecurity Authorization Working Group (DSAWG).
- Active Directory (AD) (if used) and any associated trusts in accordance with the DOD Windows Operating System (OS) STIGs and/or other applicable DOD STIGs – This includes trusts between DOD Active Directory (AD) forests and CSP CSO AD forests. If such trusts are required, the implementation must be approved by the Authorizing Official (AO) responsible for the DOD AD forest.
- VM OS – Configure in accordance with the applicable OS STIG.
- CSP-provided applications – Configure in accordance with the appropriate application STIG. Applies to applications provided by the CSP under PaaS.
- Mission Owner applications – Configure in accordance with the appropriate application STIG.
- If Mission Owner allows data transfers, the transfer must use PA and AO/Mission Owner approved cloud native tools that ride the CSP's backbone per guidance in the *Cloud Service Provider SRG* [11], section 5.9.5.
- All National Security Systems (NSS) Cybersecurity Incidents must be reported in accordance with the NMM-2022-16 to Joint Force Headquarters-DoD Information Network (JFHQ-DODIN)." – [10].

Actions

In *Uphold the Cloud Shared Responsibility Model* [12], NSA recommends the following actions.

□ Incident response: The MO should review the CSP’s incident response procedures and put together incident response playbooks to prepare for how to handle a breach.

□ Actively Hunt for Intrusions in the Cloud: An organization’s cyber defenders should be trained on defending applications and data in the cloud and be equipped with cloud security tools integrated with the MO’s resources. CSPs are not responsible for detecting when cloud resources are exploited due to an MO mistake.

□ Implement a DevSecOps process: Focus on placing security in the earliest steps in the software development lifecycle.

□ Data security: MOs are responsible for the data stored in their cloud environment. A rigorous security strategy should be in place to protect that data.

□ Authentication: Organizations must have processes in place for secure access using phishing-resistant multifactor authentication.

□ Configure identity access management (IAM): Cloud IAM services implement access controls for cloud resources, following MO-defined policies.

□ Key management: Key management is a complex area of the shared responsibility model, with the MO’s area of responsibility varying greatly by option. For more, see Play 14.

□ Service level agreement (SLA): Reviewing and understanding the SLA enables full transparency and clear language outlining MO and CSP responsibilities. If the SLA is unclear regarding the MO’s responsibilities for securely using the Cloud Service Offering (CSO), contact the CSP for more information.

□ Adaptation: The CSP and MO should maintain cyber awareness as new threats emerge and strategies for defense change over time.

Play 3. Select a Cloud with the Proper Impact Level

Be aware of the cloud security information Impact Level (IL) and select a Cloud Service Offering (CSO) with the appropriate IL.

Cloud Information Impact Levels are "defined by the combination of:

- The sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and
- The potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information." – *Cloud Service Provider (CSP) Security Requirements Guide (SRG)*, Version 1, Release 1, DISA,14 June 2024 [11].

The *Cloud Computing Mission Owner Security Requirements Guide Overview* (MO SRG), DISA, 2024 [10] summarizes the Impact Levels as follows:

- Impact Level 2: Non-Controlled Unclassified Information.
- Impact Level 4: Controlled Unclassified Information.
- Impact Level 5: Controlled Unclassified Information requiring additional protection, including Unclassified National Security Systems (NSS).
- Impact Level 6: Classified Information up to Secret.

Typically, publicly available non-sensitive data and systems can use IL2. This is the IL of commercial clouds. For sensitive, non-classified data and systems, IL4 or IL5 are appropriate. Major CSPs offer U.S. Government CSOs certified at IL5. For SECRET data and systems, use CSOs certified for IL6.

MOs should determine the proper IL for their data and applications. "DOD Mission Owners must categorize mission information systems in accordance with DoDI 8510.01 and Committee on National Security Systems Instruction (CNSSI) 1253 [13] and then identify the Cloud Information Impact Level that most closely aligns with the defined categorization and information sensitivity." – CSP SRG [11].

Select a cloud with services authorized to handle the selected IL. Do not host higher IL data or code in a lower IL service. For example, Controlled Unclassified Information (CUI) for National Security Systems (NSS) must use cloud service offerings authorized for IL5 or higher, such as one of the United States Government Clouds.

Actions

- □ Categorize the system in accordance with DoDI 8510.01 [14] and CNSSI 1253 [13].
- □ Identify the Cloud Information Impact Level that most closely aligns with the defined categorization and information sensitivity
- □ Select a cloud with services authorized to handle the selected IL.
    - Do not host a system with a higher-level IL on a lower IL CSO. For example, do not host IL 5 data on an IL 2 cloud.
- □ Read the *Cloud Computing Mission Owner Security Requirements Guide Overview* (MO SRG), DISA, 2024 [10].

Play 4. Use Cloud Service Offerings with a DoD Provisional Authorization

“A CSP is an entity that offers one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third-party facilities such as data centers, carrier hotels/collocation facilities, and Internet Exchange Points). CSPs offering SaaS may leverage one or more third-party CSOs (i.e., for IaaS or PaaS) to build out a capability or offering. A CSO is the actual IaaS/PaaS/SaaS solution available from a CSP. This distinction is important since a CSP may provide several different CSOs.” – *Cloud Service Provider (CSP) Security Requirements Guide (SRG)*, Version 1, Release 1, DISA,14 June 2024 [11].

DISA’s *Cloud Computing Mission Owner Security Requirements Guide Overview* (MO SRG), June 2024 [10] includes cloud security requirements for MOs.

MOs must use Cloud Service Offerings (CSO) with a DoD Provisional Authorization (PA) or an Authorization to Operate (ATO) for the selected impact level. This section provides an overview of what that means.

Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program (FedRAMP) “is a federally mandated, government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the federal government. The Office of Management and Budget mandates that all federal agencies use FedRAMP as their systems and applications are migrated to the commercial cloud under the federal government’s Cloud First initiatives. As with all federal departments and agencies, DoD is required to use FedRAMP-approved CSPs and share Agency ATOs with the FedRAMP Secure Repository.” – CSP SRG [11].

The FedRAMP Authorization Act establishes FedRAMP as “a Government-wide program that provides a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process **unclassified** information used by agencies.”[11]

“FedRAMP leverages National Institute of Standards and Technology (NIST) standards and guidelines to provide standardized security requirements for cloud services; a conformity

[11] Source: https://www.fedramp.gov/program-basics/.

assessment program; standardized authorization packages and contract language; and a repository for authorization packages."[12]

The FedRAMP Authorization Act also established a "FedRAMP Board to provide input and recommendations to the Administrator regarding the requirements and guidelines for, and the prioritization of, security assessments of cloud computing products and services."

FedRAMP is an aid to many federal agencies, but for the DoD, **FedRAMP is not enough**. **The DoD requires either an ATO or a DoD PA** for cloud service offerings (CSO). This directive can be found in *DoD Joint Warfighter Cloud Capability (JWCC) & Next Steps to Rationalize Cloud Use Across the DoD*, DoD CIO, 2023 [7].

FedRAMP+

FedRAMP+ leverages the FedRAMP assessment but adds additional security controls and adjusts parameter values to meet and ensure DOD's critical mission requirements. The *CSP SRG* [11] lists the controls and outlines the assessment criteria necessary to obtain a DoD PA.

DOD Provisional Authorization

A DOD PA is "an acknowledgement of risk based on an evaluation of the CSP's CSO and the potential for risk introduced to DOD networks. DOD PAs are granted at all information Impact Levels. A PA provides a foundation that AOs responsible for mission applications must leverage in determining the overall risk to the missions/applications that are executed as part of a CSO. A DOD PA is granted to the CSP for a specific CSO, not the CSP itself." – *CSP SRG* [11].

The additional security controls will be addressed by the MO, the CSP, or both. The parameters will be the DOD Risk Management Framework (RMF) Technical Advisory Group (TAG) value, the CNSSI 1253 value if no DOD RMF TAG value exists, or the AO tailored value unless designated by the MO SRG. – MO SRG [10].

[12] Ibid.

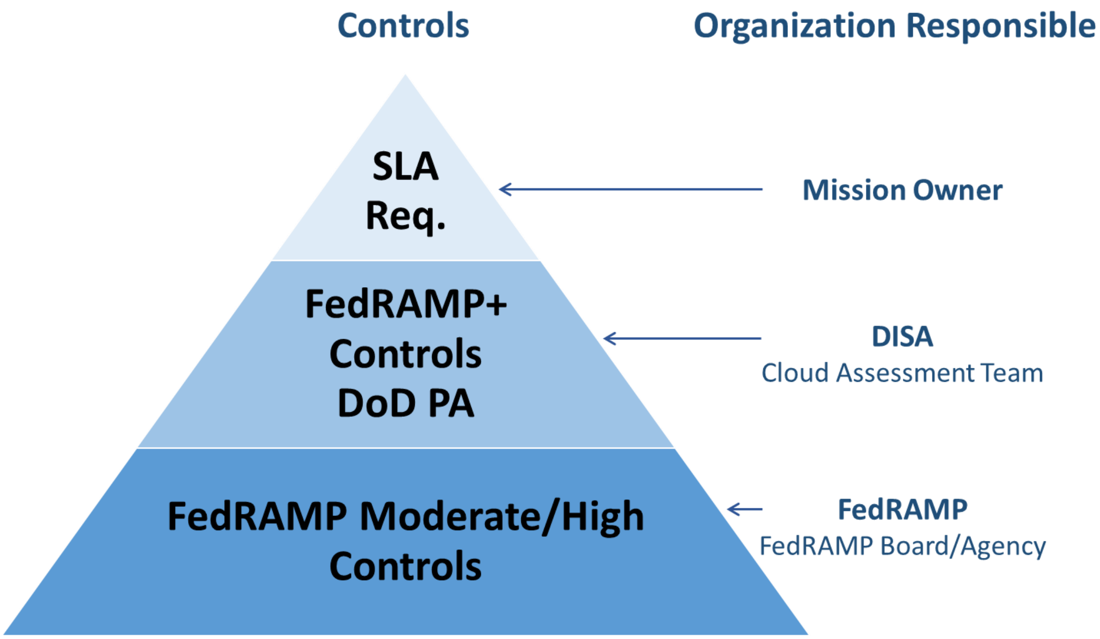

Figure 2. Ongoing Assessment Division of Responsibility

A DoD PA is primarily issued and or leveraged for enterprise/Mission Owner use. The *DoD Cloud Authorization Process*, DISA, June 2024 [15] provides information on the DoD PA process, including the following.

- When possible, DoD typically leverages a CSO’s FedRAMP Board P-ATO or Federal Agency’s ATO.
- The CSO’s security authorization package is assessed by a Third-Party Assessment Organization (3PAO) and is validated by Security Control Assessors from DISA and reviewers from the DoD Component sponsoring the CSO.
- Monthly Continuous Monitoring and Annual Assessments are performed on each CSO that is issued a DoD PA.
- Security controls can be leveraged from the enterprise Mission Assurance Support Service (eMASS).
- The DoD Component ATO
- ATO is issued by a DoD Component AO to a MO for its system/data that makes use of the CSO
- In accordance with the CC SRG, DoD MO must leverage a CSO’s DoD PA.

The MO “must choose a CSO that meets their operational needs and has a DOD PA at the information Impact Level corresponding to the categorization of the information being processed or stored in the CSO. The Mission Owner’s AO must then leverage the PA and supporting documentation in granting the required ATO for the mission system operating within the cloud.” – CSP SRG [11].

The *DoD Cloud Authorization Process* [15] discusses the reuse of authorized CSO packages, saying:

- The DoD authorization process promotes reuse of security authorization packages from FedRAMP and Federal agency authorizations.
- This allows the CSO to go through the authorization process once, and after achieving authorization, the security package can be reused.
- The FedRAMP Marketplace provides a list of cloud services authorized by both the FedRAMP Board and Agencies under FedRAMP.
- The DoD Cloud Authorization Services (DCAS) website provides a list of authorized cloud services with DoD PAs.[13]

Actions

- □ Use CSOs that have a DoD PA or ATO for the impact level of the system.
- □ Leverage the DoD PA to accelerate the ATO for the system.
- □ Become familiar with the *Cloud Computing Mission Owner Security Requirements Guide Overview* [10].
- □ If the project or system needs to use a CSO that does not have a DoD PA or ATO:
    - ○ Initiate the process of obtaining a DoD PA as described in the *DoD Cloud Authorization Process* [15].
    - ○ Read the *Cloud Service Provider (CSP) Security Requirements Guide (SRG)* [11].

[13] This site requires an account to access.

Play 5. Establish Secure Network Access

Establish secure network access to the CSP for the organization. Commercial cloud services used for IL 4 or higher must be connected to customers through the Defense Information Systems Network (DISN) Enterprise Cloud Access Point (CAP) or through a Component CAP solution approved by the DoD CIO [7].

A CAP is a system of network boundary protection and monitoring devices (e.g., firewall, Intrusion Protection System (IPS), Intrusion Detection System (IDS), proxy, etc.), through which CSP infrastructure and networks connect to the network the CAP protects. The DISN is a protected network that includes NIPRNet, SIPRNet, and other DISN-based Mission Partner and Community of Interest (COI) networks. The primary purpose of a CAP is to protect the DOD network from, and detect, unauthorized network access from the CSP's infrastructure, CSO management plane, CSP's corporate networks, CSP's connections to the internet, and unauthorized traffic generated from compromised Mission Owner systems/applications and virtual networks [11].

The secondary purpose of a CAP is "to protect the DODIN (i.e., DOD information) in general by facilitating protected connections for network users to access Impact Level 4–6 Mission Owner systems/applications instantiated on IaaS/PaaS, or using SaaS, and the information stored and processed there, without exposing that traffic to the internet. These purposes also apply to any CAP on any other DOD, Mission Partner, or COI network to protect those networks and the sensitive information they contain." [11].

So, a CAP helps protect the DODIN, but a "CAP does not protect the cloud-based application or the network enclave (physical or virtual) in which it resides. Each Mission Owner having control over what is built in the application's virtual environment in Infrastructure or Platform as a Service (I/PaaS) must provide for the protection of their application and virtual network enclave." [11].

Commercial cloud services used for IL 4 or higher must be connected through the DISN Enterprise CAP or through a Component CAP approved by the DoD CIO

Secure Cloud Computing Architecture (SCCA)

The Secure Cloud Computing Architecture (SCCA) is "a portfolio of enterprise-level cloud security services." – Secure Cloud Computing Architecture (SCCA) Program Overview, DISA, February 2024 [16]. That document includes the following points about SCCA.

- SCCA provides a standard approach for boundary and application-level security for some data hosted in commercial cloud environments
- SCCA protects the DISN from cloud-originating cyber-attacks
- SCCA uses Boundary Cloud Access Points (BCAPs) that allow connectivity to approved CSPs
- SCCA offers Virtual Datacenter Security Stack (VDSS)[14] network enclaves that protect applications and data hosted in off-premises cloud environments
    - These services are already in compliance with DISA and DOD CIO Cloud Security Guidance
- Contact DISA for more information regarding SCCA configurations. Find more information on the SCCA main page.

Boundary Cloud Access Point (BCAP)

Boundary Cloud Access Points provide connectivity to approved CSPs and protects the DISN from cloud attacks.

A BCAP establishes a protected boundary between the DISN and a CSP-CSO. A BCAP provides the capability to detect and prevent a cyber-attack from reaching the DODIN. The DoD CIO must approve a DoD Component BCAP in accordance with procedures in Appendix C of the *DoD Cloud Connection Process Guide* [17].

A BCAP provides the following protections, according to [11]:

- Provides DISN perimeter defenses and cyber defense sensing for traffic to and from applications hosted in the CSO.
- Protects the DODIN (i.e., DOD missions and information within the DISN), along with the DISN and its network services, from incidents that affect a particular CSP's infrastructure or supported missions.
- Protects DOD systems/applications instantiated in one CSP's infrastructure from incidents that affect a different CSP's infrastructure or supported missions.

BCAPs protect the DISN from cloud-based attacks by:

[14] See Play 2 for a description of VDSS.

- Filtering out unauthorized traffic
- Performing intrusion detection and prevention
- Establishing a protected boundary between the DISN and a CSP-CSO
- BCAPs include cyber-defense capabilities like firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- The CAP FRD [18] describes the architecture of a DoD-approved BCAP.
- Contact DISA for more information regarding BCAP configurations

For IL 4/5: “Except as approved (waivered) by DOD CIO, **all DOD traffic from NIPRNet** (or other DISN-based COI network) to and from off-premises CSP infrastructure serving Impact Level 4 and 5 missions and the mission virtual networks **must traverse one or more NIPRNet BCAPs**. No direct Impact Level 4/5 traffic is permitted to/from the internet except via the NIPRNet IAPs and DMZ capabilities provided by the Mission Owner, a DOD component, or DISA. The BCAP or an attached meet-me point provides for direct physical or logical connectivity between the DISN and CSP’s network through which the CSO is accessed.” – *CSP SRG* [11].

Connection Process

Connection from the DISN goes through a Boundary Cloud Access Point (BCAP), then into a Cloud Native Access Point (CNAP),[15] which is implemented using cloud native services, as illustrated in Figure 3.

Details of the connection process can be found in Appendix C of DISA’s *Defense Information Systems Network (DISN) Connection Process Guide (CPG)*, 2023 [19], and in the *DoD Cloud Process Guide* 2024 [20].

Cloud Native Access Point

The purpose of a CNAP “is to provide secure authorized access to DoD resources in a commercial cloud environment, leveraging Zero Trust Architecture (ZTA), by authorized DoD users and endpoints from anywhere, at any time, from any device.” – *DoD Cloud Native Access Point (CNAP) Reference Design (RD)*, Version 1.0, July 2021 [21].

“A CNAP creates an agile, highly scalable, and available security capability for access into Mission Owner cloud enclaves without going through a cloud access point that is hosted on the DoD Information Network (DODIN). By leveraging cloud native security services and tools, a CNAP is very efficient in terms of maintenance, management, monitoring, and

[15] Do not confuse a Cloud Native Access Point (CNAP) with a Cloud-Native Application Protection Platform (CNAPP), which is described later.

compliance. It is also very effective in facilitating a Zero Trust Architecture by utilizing conditional access policies, micro segmentation, and continuous monitoring. A CNAP is a virtual Internet Access Point (IAP) that provides modernized cybersecurity capabilities based on the DoD Zero Trust Reference Architecture. It is an access point for person entities and non-person entities to DoD resources in a commercial cloud environment from the internet (i.e., non-DODIN).” – [21].

A CNAP is part of Zero Trust Network Access (ZTNA). For more on Zero Trust (ZT), see Play 22 in Volume 2.

Figure 3, from [21], illustrates a CNAP used to access Software as a Service (SaaS) services. The diagram shows the connection from the DISN going through a BCAP to the CNAP.

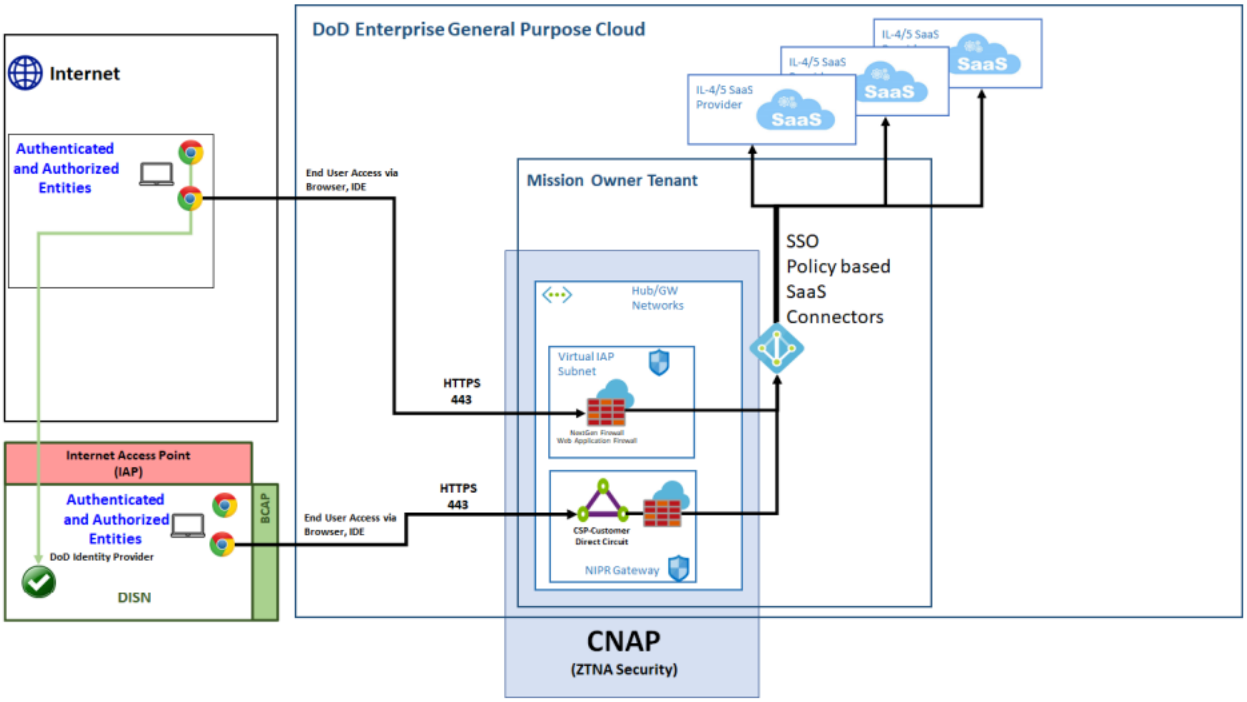

Figure 3. Using BCAP and CNAP to Access SaaS Services

System Network Approval Process (SNAP)

“Cloud use must be registered in the System Network Approval Process (SNAP) in accordance with the Defense Information Systems Network (DISN) connection Process Guide and Joint Force Headquarters-DoD Information Network direction.” – [7].

The SNAP process begins after issuance of the signed Interim Authorization to Test (IATT) or Provisional Authorization (PA). This is provided to the Connection Approval Office (CAO).

Once issued, the CAO creates the SNAP CSP-CSO registration and issues the signed Cloud Authorization to Connect (CATC) to the MO.

Once the CATC is issued, the Mission Owner must complete the Cloud Information Technology Project (C-ITP) Registration in SNAP. This includes the Cybersecurity Service Provider (CSSP) agreement as one of the supporting documents.

Then the CAO reviews the C-ITP registration, and if it passes, the CAO approves it and issues a Cloud Permission to Connect (CPTC) to the Mission Owner.

More on the SNAP process can be found in the *DoD Cloud Process Guide* 2024 [20], and in the DISN Connection Process Guide [19], as well as on the SNAP Portal.

Software Defined Perimeter

If moving toward Zero Trust (ZT), use a Software Defined Perimeter (SDP) for IL2, IL4, IL5, as discussed in the *DoD Zero Trust Reference Architecture*, Version 2.0 July 2022, Defense Information Systems Agency (DISA) and NSA [22].

The "Software Defined Perimeter will move away from the strong network perimeter concept and move towards conditional authorization with micro-segmentation and encryption. While creating an end-to-end encrypted communication path, all data and applications will have direct visibility removed from the public internet. Devices wanting to access resources would be required to pass a ZT-enabled SDP. During requests, all communication will be assumed untrusted and require conditional access based on device identity, device hygiene, and user identity with confidence level scoring." – [22].

Actions

- □ Commercial cloud services used for IL 4 or higher must be connected to customers through the DISN Enterprise CAP or through a Component CAP solution approved by the DoD CIO [7].
- □ All DOD traffic from NIPRNet (or other DISN-based COI network) to and from off-premises CSP infrastructure serving IL 4 and 5 missions and the mission virtual networks must traverse one or more NIPRNet BCAPs [11].
- □ Cloud use must be registered in the System Network Approval Process (SNAP).
- □ If moving toward Zero Trust (ZT), use a Software Defined Perimeter (SDP) for IL2, IL4, IL5, as discussed in the *DoD Zero Trust Reference Architecture* [22].

Play 6. Deploy with Infrastructure as Code

Infrastructure as Code (IaC) files are human and machine-readable text files that specify the intended state of the service they are instantiating. All the service parameters are set in these files, which are placed under version control. The IaC is then used to instantiate the cloud services. Many organizations in both the DoD and industry use IaC to automate deployment of secure cloud services.

Cloud misconfiguration is one of the most critical issues for securing cloud environments and it has been identified as a key vulnerability that is being exploited by [2], among others. For more on that, see Appendix A. Deploying cloud services using IaC helps to mitigate this critical vulnerability.

Immutable Artifacts

These IaC files should only be modified in development, not operations, though there should be a tight feedback loop from operations to development, so that development can address their needs quickly. The idea is to deliver immutable artifacts; that is, artifacts such as IaC that are not edited or manually configured when deploying them into production or another hosting environment (e.g., test or staging environments).

In addition to the use of IaC, deploy other components using immutable artifacts, such as immutable containers. The point is to modify these artifacts (IaC and containers) in development, not in operations, to put them under strict version control, and to make sure they are tested before being deployed. This practice of immutable artifacts avoids environmental drift, so that software that works in development and testing also works in production. For more on containers, see Play 19 in Volume 2.

Allowing no human to modify production environments (e.g., disabling Secure Shell (SSH) for remote access) reduces the attack surface, reduces insider threat, and stops configuration and environment drift. In general, treat Everything as Code (EaC). This includes infrastructure, configuration, networking, policy, compliance, and tests.

DoD Infrastructure as Code Templates

IaC can be established to enable many security aspects, such as encryption. Using such IaC provides better security, easier and faster. To do that, start with the DoD Cloud IaC templates, then modify as appropriate. The DoD Cloud IaC templates may be found here: https://www.hacc.mil/Portfolio/DOD-Cloud-IaC/.

Using these DoD IaC templates enables an Authorization to Operate (ATO) for the services they instantiate from the DISA Risk Management Executive (RME). Systems may leverage reciprocity from that ATO, but systems still need their own ATO.

Declarative vs. Imperative

The IaC language may be either declarative or imperative. The declarative style describes the desired system state without details on how to achieve that state. The imperative style describes how to achieve the desired state typically as a sequence of steps.

The imperative style of IaC is more flexible and allows more control. But it is more complex, and there can be redundant actions because it does not keep track of the state of the system.

The declarative style of IaC is less flexible than the imperative style, but it is simpler to write and maintain. Declarative tools keep track of the system state, so that they only change what needs to change, avoiding the redundant actions possible with the imperative style.

Naturally, the language the MO selects for IaC will likely be determined by the IaC template language.

Actions

- □ Only deploy cloud services using IaC.
- □ To create IaC, start with the IaC templates provided by DISA.
- □ Place IaC under version control.
- □ Treat IaC as an immutable artifact.
- □ Select the IaC language used by the DISA IaC templates.

The following are some best practices for IaC from *Enforce Secure Automated Deployment Practices through Infrastructure as Code*, NSA, 2024 [23].

Before deploying IaC, use these best practices:

- □ Create a threat model to identify attack vectors and mitigations that can be put into place to reduce the likelihood of compromise.

- □ Decide which organizational rules are best encoded as declarative or imperative.

- □ Run static analysis against templates to test for misconfigurations and security gaps.

- □ Enable version control on IaC.

□ Integrate IaC deployment into existing Continuous Integration / Continuous Delivery (CI/CD) pipelines.

After deploying IaC, use these best practices:

□ Perform dynamic analysis to ensure resources deployed correctly and threat vectors are properly addressed.

□ Enable access control on IaC.

□ Avoid making manual changes to resources deployed through IaC.

□ Enable continuous logging and monitoring to detect unauthorized changes.

□ Audit changes to IaC.

Play 7. Implement Secure Identity, Credential and Access Management

> "Malicious actors can compromise accounts using phishing techniques, exposed credentials, or weak authentication practices to gain initial access into cloud tenants." - *NSA's Top Ten Cloud Security Mitigation Strategies*, 2024 [5].

Identity, Credential, and Access Management (ICAM) is important to implement correctly. ICAM includes Identity and Access Management (IAM). ICAM applies not only for Person Entities (PE) (i.e., people or roles), but also for Non-Person Entities (NPE) and Federated Entities (FE). NPEs include software running on a machine and physical devices (e.g., a smart phone), while FEs are from entities outside the DoD such as mission partners. The next diagram illustrates the high-level DoD vision for ICAM, it is from the *DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design*, Version 1.0, June 2020, DoD CIO [24].

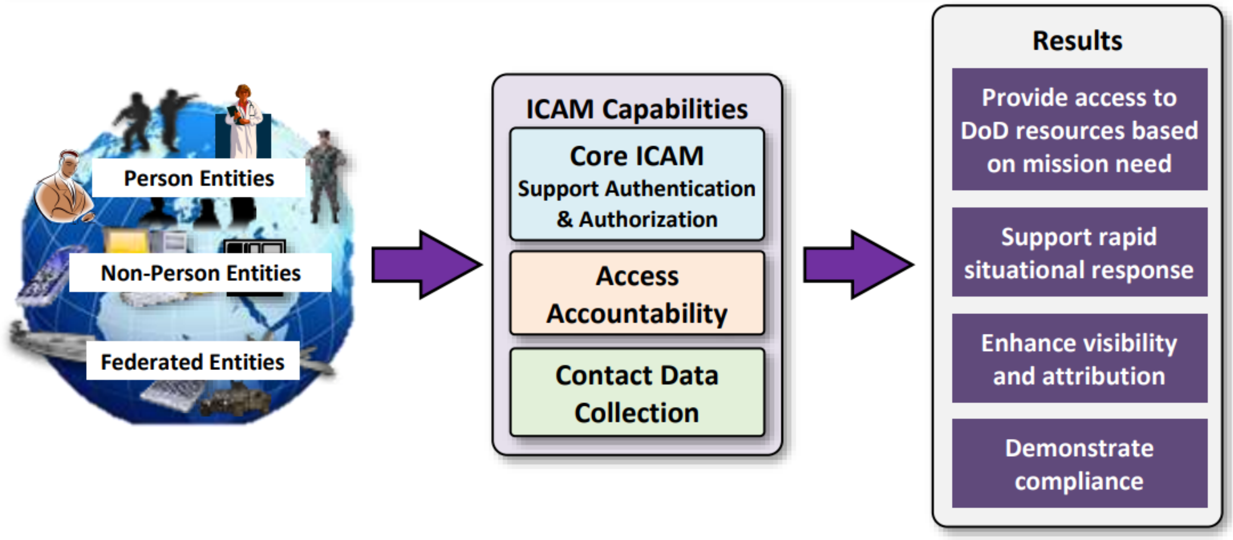
Person Entities
Non-Person Entities
Federated Entities
ICAM Capabilities
Core ICAM
Support Authentication & Authorization
Access Accountability
Contact Data Collection
Results
Provide access to DoD resources based on mission need
Support rapid situational response
Enhance visibility and attribution
Demonstrate compliance

Figure 4. DoD ICAM Vision

Select or Create an ICAM Solution in accordance with Department of Defense Instruction (*DoDI) 8520.03, Identity Authentication for Information Systems*, May 2023, DoD CIO [25]. This includes phishing-resistant Multi-Factor Authentication (MFA).

There are two main types of phishing-resistant MFA. One is based on Public Key Infrastructure (PKI) and uses a smart card such as a Common Access Card (CAC). This is the only type approved for DoD use.

The other type of phishing-resistant MFA is based on Fast IDentity Online (FIDO) WebAuthn authentication. "In addition to being 'something that you have,' FIDO authentication can incorporate various other types of factors, such as biometrics or Personal Identification Number (PIN) codes." – *Implementing Phishing-Resistant MFA*, Cybersecurity and Infrastructure Security Agency (CISA), Oct 2022 [26].

For the DoD, authentication based on DoD approved PKI is preferred for all use cases [25]. However, FIDO may be useful in a Mission Partner Environment (MPE), if a CAC or similar is not available for partners. In such a case, an AO could approve the use of FIDO, if it passes a security review and meets the AO's risk tolerance.

Secure Identity Servers

> "Identity servers are frequent targets for malicious cyber actors as they can be leveraged to retrieve user credentials that would grant access to on-prem and cloud environments." – *Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments*, NSA, March 2024 [27].

It is important to secure the identity servers (or services) themselves, since they are prime targets.

In the cloud, the cloud Instance Metadata Service (IMDS) can be a target. It can be "queried from virtual instances in the cloud for general information about the tenant. However, this service can also be used to retrieve a variety of information, including IAM credentials that malicious actors can use to gain additional access to the cloud tenant." – [28].

To secure the identity servers, implement and enforce the Principle of Least Privilege (PoLP), and audit identity federation to detect attempts by Malicious Cyber Actors (MCAs) to abuse trust relationships.

DoD ICAM Resources

Here are some important DoD resources on ICAM.

- *DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, May 2023, DoD CIO, [29]
- *DoDI 8520.03, Identity Authentication for Information Systems*, May 2023, DoD CIO [25]
- *DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design*, Version 1.0, June 2020, DoD CIO, [24].
- *DoD Mobile Public Key Infrastructure (PKI) Credentials*, DoD CIO, 2019 [30]
- *Identity, Credential, and Access Management (ICAM) Strategy*, March 2020 [31]

Actions

- □ Select or Create an ICAM Solution in accordance with *DoDI 8520.03, Identity Authentication for Information Systems*, May 2023, DoD CIO [25].

Principle of Least Privilege

- □ Implement and Enforce the PoLP.
- □ Implement PoLP on user accounts and service accounts.
- □ Implement PoLP for each cloud resource; lock down the 'identity' boundary for each cloud resource.
- □ Implement least privilege for resources, such as limiting source and destination connection access privileges (what entities are allowed to connect to a source). Techniques to accomplish this include whitelisting and micro segmentation, which is discussed in Play 16.
- □ Implement least-privilege policies for access to the DevSecOps pipeline. Team members (developers, testers, administrators, etc.) should only have access to components they need for their tasks, not the entire environment.
- □ Implement separation of duties, which is the principle that no user should be given enough privileges to misuse the system on their own [32]. There are several ways to do that. One is to require two-person controls for performing particularly sensitive operations. Another way is to have separate administrator roles to control how resources are accessed and managed. "For example, access control administrators of the Key Management System (KMS) with the necessary privileges to grant access to keys protecting sensitive data or capabilities should not be able to grant themselves access to use those issued keys." – [28].
- □ Restrict write-access to backups. This helps counteract ransomware Tactics, Techniques, and Procedures (TTP) used by Malicious Cyber Actors (MCA) to target data backups [28].
- □ Provision separate backup management accounts for administrators who require access to the backups. This reduces the risk of cloud environment data backup breaches [28].
- □ Do not use privileged accounts for ordinary activities, just use them for activities such as systems administration, cybersecurity, or similar that require privileged access. Frequently (ideally automatically, see Play 9) audit IAM configurations to confirm that only necessary privileges are granted [28].

ICAM Best Practices

Here are some best practices from *Use Secure Cloud Identity and Access Management Practices*, NSA, 2024 [28].

Identity management:

- □ Require phishing-resistant multi-factor authentication (MFA) for user accounts, with DoD PKI preferred.
- □ Use a secrets manager to store server Transport Layer Security (TLS) certificates; do not store them in plain text.
- □ Rapidly revoke compromised or unnecessary Public Key Infrastructure (PKI) certificates and prevent their unauthorized collection.
- □ Only use secret keys when required and provision them for short-term access with the least privileges necessary.
- □ Secure identity federation servers and audit identity federation to detect attempts by MCAs to abuse trust relationships.

Access management:

- □ Use context-based access control policies and review policies prior to deployment and periodically after deployment to identify potential gaps.
- □ Consider requiring administrators to access cloud resources using Privileged Access Workstations (PAWs).
- □ Limit use of administrative accounts and use Just-in-Time (JIT) security practice, where increased privileged access to applications or a system is limited to predetermined periods for specified activities, to limit privileged access and improve tracking of privileged actions in the tenant. Privilege elevation with JIT should be logged.
- □ Connect to cloud resources over an encrypted channel using secure protocols such as TLS 1.2 or higher and Commercial National Security Algorithm (CNSA) approved cipher suites (preferably CNSA Suite 2.0).
- □ Assign privileges according to best practices for access control by carefully applying the separation of duties and least privilege principles, and audit privilege assignments and access requests.
- □ Consider using policy as code (Play 9) to allow for improved tracking and review of access control policies, and frequently check for drift.
- □ Secure the cloud IMDS by restricting users/services with the privilege to query the IMDS, using the most up to date version, implementing vendor specific best

practices, and implementing best practices to secure cloud-hosted applications and prevent Server-Side Request Forgery (SSRF) attack vulnerabilities.[16]

[16] For more on SSRF, see the Common Weakness Enumeration (CWE) at https://cwe.mitre.org/data/definitions/918.html

Play 8. Define or Identify a Cloud Landing Zone

If there are multiple cloud accounts, define or identify a Cloud Landing Zone. A landing zone is a multi-account cloud environment. It helps engineers quickly deploy new cloud environments that meet the organization's standards. The essential components of a landing zone are indicated in the next figure.

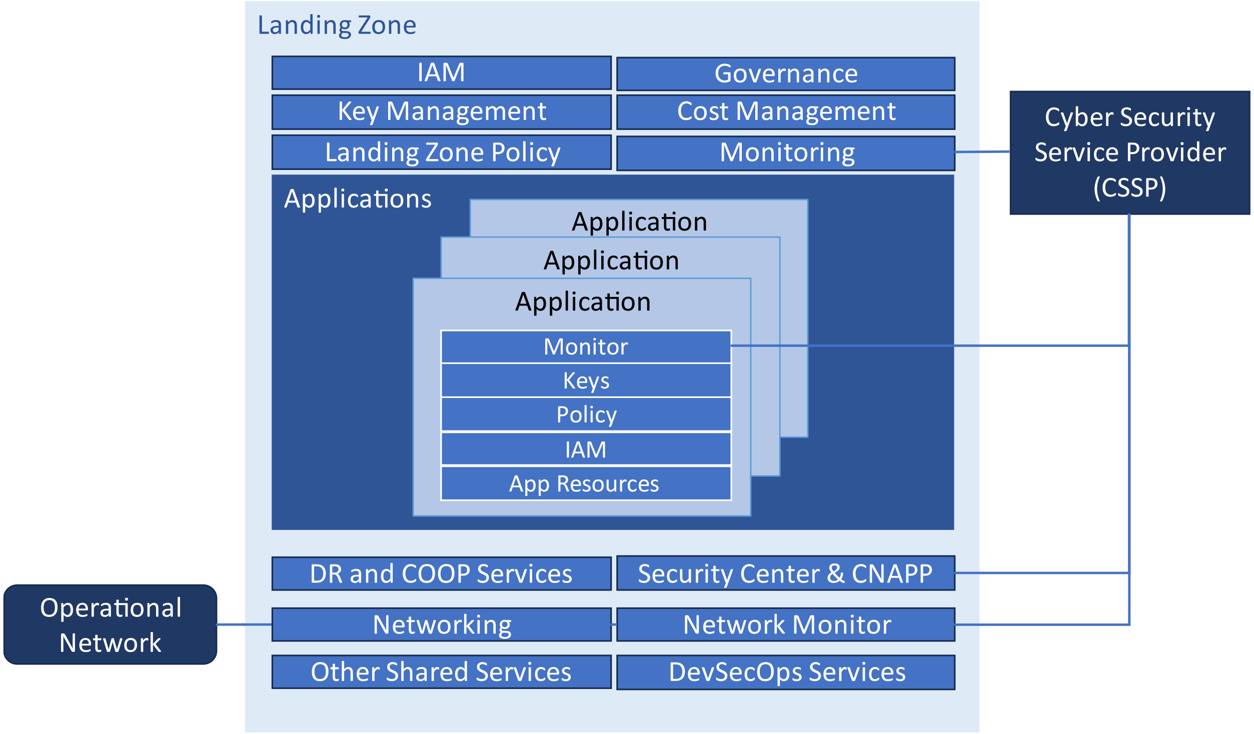

Figure 5. Notional Cloud Landing Zone

The landing zone includes setting up Disaster Recovery (DR) and Continuity of Operations (COOP) services. This is part of implementing Cyber Resiliency, as discussed in Play 17.

The landing zone should also include a Cloud-Native Application Protection Platform (CNAPP), [17] which is described in Play 11.

Each major CSP has a way to build a landing zone. For example, on Amazon Web Services (AWS), consider the AWS Control Tower, and on Azure consider the Azure landing zone accelerator. Both services offer initial templates to accelerate the process of building a landing zone.

[17] CNAPP should not be confused with Cloud Native Access Point (CNAP).

There must also be a Cybersecurity Service Provider (CSSP) that has been granted access to cloud monitoring capabilities.

Landing zones differ between CSPs. Further information on landing zones for some popular CSPs can be found on these sites:

- Microsoft Azure landing zone
- AWS landing zone prescriptive guidance
- Landing Zone Accelerator on AWS

Actions

- □ Create a cloud landing zone.
- □ Integrate a CSSP and provide it with access to cloud monitoring capabilities.
- □ Create a Disaster Recovery (DR) plan and test it.
- □ Create a Continuity of Operations (COOP) plan and test it.

Play 9. Implement Policy as Code

> "Codify security and compliance best practices through policy as code." – NSA [27].
>
> "Automate security processes to take policy-based actions across the enterprise with speed and at scale." – *DoD Zero Trust Reference Architecture*, 2022 [22].

Policy as Code (PaC) is the description and enforcement of configuration to ensure compliance, security and governance.

Define policies in a machine-readable format and implement PaC. In tandem, enable automation that uses these policies to check for compliance; this is compliance as code. Major hyperscale cloud providers offer compliance checking services;[18] there are also third-party policy tools available for on-prem systems. So, there is no need to develop a compliance mechanism; simply create the policies in the proper format and use a cloud-native or third-party tool to perform compliance checking.

One example is to enable automatic checking for security patches and send an alert when components are out of compliance.

Some types of policies include:

- Security, such as ensuring data is encrypted at rest (a common vulnerability).
- Availability, such as ensuring enough instances are running to handle the computational load.
- Cost Optimization, such as killing unnecessary containers or virtual machines that have been left running.
- Observability, ensuring that logging and telemetry is enabled.

Some policies can be implemented with static checks, while others can be checked dynamically. Both can trigger automated responses, such as sending an alert, or killing a virtual machine and instantiating a replacement.

Configuration as Code

Configuration as Code uses text files for configuration and handles them like code (i.e., the files are checked into version control, etc.). Configuration as Code aids in the automation,

[18] E.g., Implementing a compliance and reporting strategy for NIST SP 800-53 Rev. 5 on AWS, or Details of the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative on Microsoft Azure.

provisioning, and management of infrastructure and applications. It helps maintain state and helps avoid configuration drift.

Configuration as Code works with PaC, since it provides configuration files for the policies that validate configurations.

Given the proper PaC, existing tools (e.g., Azure Policy, AWS Config) can continuously validate cloud resource configurations. This is much better than standard manual checking that is performed infrequently. For example, suppose a malicious actor gained access to a component, and changed the configuration. Since configuration is checked continuously, such a change would be detected and acted upon.

Actions

- □ Define policies in a machine-readable format and implement policy as code (PaC).
- □ Enable automation that uses these policies to check for compliance.
- □ Use Configuration as Code.

Play 10. Set up Logging and Manage the Logs

> "During the SolarWinds incidents, Russian actors were able to use cloud APIs to exfiltrate data from their targets' cloud environments. They were also able to add credentials, authenticate to cloud services, add permissions to applications, and move laterally throughout the cloud using specific cloud APIs, which **prevented their activity from being logged in conventional web console logs.**" – *Manage Cloud Logs for Effective Threat Hunting*, NSA, 2024 [33].

Defending applications hosted in a cloud requires creating and maintaining good logs with the proper level of detail to enable cyber defense. The logs must also be protected so that malicious actors cannot alter the logs, even when they act as system administrators.

"Cloud access policies, system logs, and administrative audits must be controlled and monitored by security engineers and system administrators to prevent access abuse." – [33].

What to Log

Projects must enable logging for applications, hosts, networks, and cloud service API calls. Cloud logs should include the following, according to [33]:

- Authentication and authorization, including changes to user roles or permissions.
- Network and security, including firewall services blocking incoming network connections, network flows, intrusion detection system events, and network configuration changes.
- System and application, such as changes to system configurations and security policy violations.
- Application programming interface (API) calls to cloud services, such as provisioning, usage and cost analysis, and service configuration changes.
- Short-term cloud resources, such as virtual machines, containers, or functions as a service.

It is important to include enough details in the logs to provide the necessary security information for forensic analysis. Also ensure that the CSP has enabled critical logs and that they are available for threat hunting and other cybersecurity investigations [33]. It may be necessary to incur additional cost to make all the CSP-logged data available to the CSSP [34]. This should be detailed in the CSP SLA.

Managing Logs

It may not be possible to log and analyze every event, due to the size of the logs, so it is essential to have a good log management strategy.

Use a centralized logging solution, as recommended by [27] and [33]. All major CSPs provide such a tool. Generally, it is best to keep the logs in the cloud and send back analysis and query responses to external sources (e.g., the CSSP), rather than exporting the logs themselves, which would be unnecessarily expensive.

There are also tools to help manage logs. Currently, there are three types of such tools:

- Security Information and Event Management (SIEM) tools "collect information from various security tools, aggregate it in a central log, and flag anomalies" [35].
- Security Orchestration, Automation, and Response (SOAR) software "enables security teams to integrate and coordinate separate security tools, automate repetitive tasks and streamline incident and threat response workflows" [35]. "SOAR improves security and decreases response times" [22].
- Extended Detection and Response (XDR) "solutions collect and analyze security data from endpoints, networks, and the cloud. Like SOARs, they can automatically respond to security incidents. However, XDRs are capable of more complex and comprehensive incident response automations than SOARs. XDRs can also simplify security integrations, often requiring less expertise or expense than SOAR integrations" [35].

DoD organizations should "collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or Security Operations Center (SOC). Logs and events follow a standardized format, and rules/analytics are developed as needed." – *DoD Zero Trust Capability Execution Roadmap (COA1)*, DoD CIO, 2023 [36].

SIEM tools should include these features.

- Collect logs and cybersecurity data from all assets deployed in the cloud, including those generated by all cloud services that are used.
- Enable threat detection use cases created by DoD cybersecurity personnel.
- Enable tuning of alerts so that only important alerts are displayed on the dashboard.
- Provide support for incident response actions.
- Generate reports to support compliance and audit activities.

It is important to have a well-defined data onboarding policy for SIEM, including:[19]

- Data onboarding use cases that the SIEM will support
- Data normalization procedures to standardize the format and structure of ingested data
- The essential fields and data types required for each data source
- Standardized dashboard templates to present relevant data visualizations and insights to security analysts and stakeholders. Typically, a SIEM offers dozens of pre-built dashboards, but it should also offer customizable dashboards. Some information to include on some dashboards includes:
    - Threat Intelligence
    - Network Events
    - Alerts, backed by alert prioritization to identify the most important active threats
    - Application Server Events
    - Web Server Events
    - System Events
    - Identity Management
    - Database Access Control
    - File Access Control
    - Behavior anomalies such as abnormal user logons, logon failures, unusual user accesses, etc.
- Detection rules tailored to the specific data sources and use cases.

A CSSP, Computer Network Defense Service Provider (CNDSP) or security operations center (SOC) should "monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM" [36].

SOAR allows DoD organizations to orchestrate and automate policies and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, and triggering automated responses and remediation. The automated responses are defined in playbooks that span the gamut from collection to incident response and triage. These playbooks enable automation that speeds cybersecurity decision and response speed [36].

[19] Source: Harnessing the Power of Security Information and Event Management (SIEM).

Actions

- □ To enable logging for cloud services, use the IaC templates (see Play 6).
- □ Log as much security relevant information as possible, see the section What to Log in this play.
- □ Implement a management plan for the logs.
- □ Use the cloud native log aggregation tools provided by the CSP.
- □ Use a SIEM, SOAR, or XDR to analyze logs and improve hunt and forensic operations
- □ Deploy SIEM, SOAR, and XDR tools in the cloud, where the logs reside. Do not use an on-premises solution for logs generated and stored in the cloud.
- □ Use a SIEM to help organize and process log data so that defenders can properly analyze events to discover and respond to threats.
- □ Most CSPs offer machine-learning-based log analytic tools. This can be beneficial, as traditional SIEM tools may not effectively map actions across cloud resources.
- □ Protect the logs – “Malicious agents can target logs and logging infrastructure to hide their presence, erase evidence, or otherwise repudiate their actions” [33].
    - o Implement controls on who may access and modify logs, primarily using a log administrator role that is distinct and isolated from other administrator roles [33].
    - o Network communications with log data should be encrypted to help protect the integrity of logs [33].

Play 11. Use a Cloud-Native Application Protection Platform

One tool that helps enable Defensive Cyberspace Operations (DCO) and provides several cybersecurity functions is the use of a Cloud-Native Application Protection Platform (CNAPP). A CNAPP is "an integrated set of security and compliance capabilities to secure and protect cloud-native applications across development and production." – *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [37]. Do not confuse a CNAPP with a Cloud Native Access Point (CNAP).

Select and use a CNAPP, which may be set up as part of the cloud landing zone.

A good set of capabilities for a CNAPP is indicated in the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [37].

- Artifact Scanning:
    - Software Composition Analysis to review artifacts to find open-source libraries included. This should be addressed in the creation of the Software Bill of Materials (SBOM).
    - Application Security Testing such as Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Interactive Application Security Testing (IAST)
- Cloud Configuration:
    - Cloud Security Posture Management (CSPM) for continuous monitoring, detection, and remediation of cloud security misconfigurations.
    - Cloud Infrastructure Entitlement Management (CIEM) for management of access rights, permissions, or privileges for the identities of a single or multi-cloud environment.
    - Infrastructure as Code (IaC) Scanning to find security flaws before pushing to production.
- Runtime Protection:
    - Cloud Workload Protection (CWP) provides runtime enforcement.
    - Cloud Detection and Response (CDR) provides advanced threat detection, incident response, and continuous monitoring capabilities specifically designed for cloud environments. This includes intrusion detection.

Actions

- □ Select a CNAPP.
    - ○ Ensure that the CNAPP includes the capabilities listed in this play, including intrusion detection.
- □ Integrate the selected CNAPP into the mission’s cyber processes.

Play 12. Employ Defensive Cyberspace Operations

Select a Cybersecurity Service Provider (CSSP) and integrate them with the Cloud Service Provider (CSP). This helps enable Defensive Cyberspace Operations (DCO), which consists of "passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[20] Large DoD organizations typically have already selected a preferred CSSP that their programs must use.

As part of the Shared Responsibility Model, establish and document which organization is responsible for which parts of incident detection and response.

It may be necessary to incur additional cost to make all the CSP-logged data available to the CSSP [34]. This should be enabled early, or the logs may not be available, depending on the CSP.

DoD Manual (DoDM) 8530.01, *Cybersecurity Activities Support Procedures*, DoD CIO, 2023 [38] specifies the following for the CSSP:

> "DoD Components must designate a Component-level organization to direct and manage network operations and cybersecurity activities mapped to the NIST Framework for Improving Critical Infrastructure Cybersecurity as the focal point for implementing and conducting Component-wide cybersecurity activities for DODIN operations and Defensive Cyberspace Operations (DCO) Internal Defensive Measures (IDM). Where cybersecurity services for a Component are distributed among multiple authorized external providers, supporting providers will assist the designated Component-level organization in the coordination and integration of Component cybersecurity through information sharing in accordance with DoDI 8320.02 and DoDD 8000.01."

Cyber Incident Reporting and Response

Use the Cloud Detection and Response (CDR) aspects of the Cloud-Native Application Protection Platform (CNAPP)[21] (see the CNAPP play for more) to provide advanced threat detection, incident response, and continuous monitoring capabilities designed for cloud environments.

[20] NIST Glossary https://csrc.nist.gov/glossary/term/defensive_cyberspace_operations

[21] CNAPP should not be confused with Cloud Native Access Point (CNAP).

The *Cloud Service Provider (CSP) Security Requirements Guide (SRG)*, 2024 [11] states that the CSSP performing Mission Cyberspace Defense (MCD) actions “will be the DOD point of contact to which the CSP’s operational entity will coordinate responses to incidents affecting the security posture of the CSP and the CSP’s cloud service.

- For CSOs supporting **Impact Levels 2 to 5** that are multitenant or shared across federal agencies outside of the DOD, incidents will be reported to Department of Homeland Security (DHS) United States - Computer Emergency Readiness Team (US-CERT) as well as the CSSP contracted to perform MCD actions.

- For CSPs supporting **Impact Levels 4 to 6** that provide dedicated infrastructure to the DOD, incidents regarding that infrastructure and CSOs will not be directly reported to the CSSP contracted to perform MCD actions or to US-CERT. USCYBERCOM/JFHQ-DODIN, upon receiving reports for these Impact Levels, will coordinate with US-CERT and other entities as appropriate.”

Cyberspace Defense Actions

This section is from the CSP SRG [11]. It discusses defense actions in cyberspace. It provides the following list of “cyberspace defense actions and their responsibilities as they relate to cloud operations.

- DODIN Cyberspace Defense (DCD) Actions: The primary objective of the organization that performs DCD actions is to oversee a coordinated response to DODIN-wide attacks. DCD builds a broad picture of the operating environment across Mission Owners, Mission Cyberspace Defense (MCDs), Boundary Cyberspace Defense (BCDs), CSOs, and CSPs. The DCD identifies patterns of incidents or events, consolidates related incident tickets, directs mitigations, and assigns DODIN Cyber Protection Teams (CPTs) to focus efforts on a specific threat or adversary. Specific cyberspace defense actions include:
  - Protect the DODIN and DOD mission systems in commercial cloud infrastructure through cross-BCAP correlation and analysis of events/data.
  - Direct or recommend cybersecurity actions regarding DODIN-wide incident and system health reporting involving a BCAP or CSP.
  - Establish and maintain external communications with the CSP for DODIN-wide incidents and ensure internal DOD communications are established between all entities, which include the MCD and BCD.
  - Interface with the U.S. Computer Emergency Readiness Team (US-CERT) to obtain relevant CSP information; ensure cross-sharing of information across all organizations performing BCD/MCD actions.

- Boundary Cyberspace Defense (BCD) Actions: The primary objective of organizations that perform BCD actions is to protect the DISN from events or incidents that use public, private, hybrid, or community clouds. BCD actions support CSSPs performing MCD actions in their objectives of defending DOD systems, applications, and data hosted in the cloud. Specific cyberspace defense actions include:
    - Protect the DISN via the BCAP.
    - Provide timely access to BCD-collected indications and warnings relevant to organizations performing MCD actions.
    - Support DCD actions to identify correlations between related events or incidents that impact multiple Mission Owners, CSOs, or CSPs.

- Mission Cyberspace Defense (MCD) Actions: The primary objective of organizations that perform MCD actions is to defend Mission Owners' systems, applications, and data hosted in the cloud. MCD actions are performed by CSSPs on behalf of their organic organizations and subscribers. Specific cyberspace defense actions include:
    - Analyze cyber incidents and events for Mission Owners.
    - Monitor, protect, and defend Mission Owners' cloud-based systems, applications, and virtual networks, including privileged actions (e.g., cloud management or application administration) in the CSP's CSOs infrastructure.
    - Monitor for events or incidents against the Mission Owner applications (e.g., Structured Query Language [SQL] injection).
    - Monitor, protect, and defend Mission Owners' cloud-based data in the CSO.
    - Defend all connections to the CSO, whether via BCAP, Virtual Private Network (VPN), IAP, direct internet access to public servers, or other.
    - Support DCD efforts to identify correlations between related events or incidents that impact multiple Mission Owners, CSOs, or CSPs.
    - Ensure internal DOD communications are established between all entities, which include the Mission Owner and other organizations performing MCD and BCD actions.
    - Provide visibility and awareness of cyber incidents or events impacting Mission Owner systems, applications, virtual networks, and data to JFHQ-DODIN" – [11].

Penetration Testing

Penetration testing (pen testing) simulates an attack on a system to discover any vulnerabilities.

“Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application-level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies.” – National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5 [39].

The DoD CIO JWCC Memo [7] requires annual penetration testing and provisions in all contracts for classified cloud services that enable DoD red teams to conduct independent, adversarial assessments of the cloud environment that emulate the most capable, nation-state threats.

This annual penetration testing must be performed by a DoD Cyber Red Team (DCRT). However automated penetration testing can be performed much more frequently in addition to the annual DCRT testing. It is a best practice to include frequent automated penetration testing.

Intrusion Detection

An Intrusion Detection System (IDS) generates an alert when it detects suspicious behavior. An IDS offers one of two types of monitoring. If the IDS monitors network traffic, it is a Network Intrusion Detection System (NIDS). On the other hand, an IDS that monitors activity on a host is a Host Intrusion Detection System (HIDS). A NIDS is placed on the network and monitors network traffic. A HIDS is agent-based, with agents installed in each Virtual Machine, physical device, or container [40].

For more information on network infrastructure security, see the *Network Infrastructure Security Guide*, 2023, NSA [41].

Intrusion detection should be provided by the CNAPP discussed in Play 11.

Sidecar Security Container (SSC)

For those using containers and Kubernetes, a best practice is to install a HIDS agent in a sidecar security container and configure Kubernetes to install that sidecar automatically in the same pod with each application container. The sidecar container shares disc and network resources with the application container in that pod. For more on the SSC, see Play 19 in Volume 2, and the *DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes* [42].

Defensive Cybersecurity AI

AI is being employed by adversaries to attack systems. But AI is also used for defensive cybersecurity as well. This is a relatively new area, so this section includes brief descriptions of some recent tools for two popular CSPs: AWS and Azure.

Amazon Web Services

Recent defensive cybersecurity AI additions for AWS include enhancements to the following:[22]

- Amazon Inspector – expands AWS Lambda code scanning with generative AI-powered remediation. It can assess custom AWS Lambda code for security issues such as injection flaws and data leaks. Provides actionable security findings, including affected code snippets and remediation suggestions, simplifying updates to vulnerable code.
- Amazon CodeWhisperer – provides code suggestions to help remediate identified security and code quality issues tailored to the application code. Security scanning is available for several popular languages, including Java, Python, and JavaScript, TypeScript, C#, CloudFormation, and others.
- Amazon Detective – uses generative AI to create finding group summaries. Amazon Detective finding group summaries help more quickly locate and review key insights on suspicious activity identified in finding groups in natural language. This makes it simpler to investigate and understand unusual or suspicious activities.
- AWS Config – launches generative AI-powered natural language querying. This feature simplifies the investigation and search of AWS resource configurations and compliance metadata.

[22] Source: AWS re:Invent 2023: Security, identity, and compliance recap | AWS Security Blog (amazon.com).

Microsoft Azure

Generative AI defensive cybersecurity tools on Azure include:[23]

- Microsoft Copilot for Security – uses natural-language guidance from Generative AI to perform tasks such as:[24]
    - Synthesizing data into actionable recommendations and insights to help guide incident investigations.
    - Creating human-readable reports and presentations.
    - Answering questions about an incident or vulnerability in natural language or graphics.
- Copilot in Microsoft Defender XDR – Detect and disrupt cross-domain cyberattacks with unified visibility and integrated AI assistance.
- Copilot in Microsoft Intune – Simplify data and device protection with cost-effective endpoint management that includes Copilot.
- Copilot in Microsoft Purview – Secure and govern data.
- Copilot in Microsoft Entra – Protect any identity and secure access to any resource, with a generative AI assistant.
- Copilot in Microsoft Defender for Cloud – Strengthen multicloud and hybrid environments in development and in runtime.
- Copilot in Microsoft Defender External Attack Surface Management – Manage the rapidly changing, global external cyberattack surface in real time with help from an AI assistant.
- Azure OpenAI Service for building custom copilots with generative AI models.

[23] Source: https://www.microsoft.com/en-us/security/business/solutions/generative-ai-cybersecurity

[24] Source: https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity

Actions

- □ Engage a DoD-approved CSSP.
- □ Establish and document which organization is responsible for which parts of incident detection and response.
- □ Ensure that all CSP-logged data is available to the CSSP.
- □ Perform Penetration Testing
  - Implement automated penetration testing.
  - Follow guidance on penetration testing in DTM 24-001, *DoD Cybersecurity Activities Performed for Cloud Service Offerings*, DoD CIO, 2024 [9].
  - Use a DCRT to perform a penetration test at least annually.
  - Address vulnerabilities found in both automated and DCRT penetration testing.
- □ Set up a HIDS. This should be part of the CNAPP.
- □ Set up a NIDS. This should be part of the CNAPP.
- □ If using containers and Kubernetes, consider adding an appropriate HIDS agent in an automatically deployed security sidecar, as described in Play 19 in Volume 2, and the *DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes* [42].

Play 13. Encrypt Data at Rest and in Transit

Failure to implement encryption is one of the most common cloud security errors. For example, one recent study of industry found a 90% failure rate for encryption-related controls of a database server in one cloud, a 71% failure rate in securing serverless functions on another cloud, and a 98% failure rate of encryption-related controls for both compute and storage services in a third cloud [43].

To avoid such issues, enable encryption-in-transit and encryption-at-rest. All sensitive data should be both encrypted at rest and encrypted in transit using FIPS 140-2 approved certification and algorithms. Also use good Key Management (KM) practices, as discussed in Play 14.

“Mission systems at all Impact Levels must have the capability for DOD data to be encrypted at rest with exclusive DOD (Mission Owner) control of encryption keys and key management.” – MO SRG [10].

Encrypting data at rest with MO control of encryption keys and key management “maintains the confidentiality and integrity of CUI at Impact Levels 4 and 5 with the following benefits:

- Limits the insider threat vector of unauthorized access by CSP personnel by increasing the work necessary to compromise/access unencrypted DOD data.
- Limits the external threat vector of unauthorized access by hackers by increasing the work necessary to compromise/access unencrypted DOD data.
- Enables high-assurance data destruction for CSP offboarding through cryptographic erasure without the involvement or cooperation of a CSP.
- Enables high-assurance data spill remediation through cryptographic erasure without the involvement or cooperation of a CSP.” – CSP SRG [11].

The MO SRG states that “for all Information Impact Levels:

- Encrypt all data at rest:
    - Stored in VM virtual hard drives.
    - Stored in mass storage facilities/services whether at the block or file level.
    - Stored in database records (whether PaaS or SaaS where the Mission Owner does not have sole control over the database and database management system).

- Use FIPS 140-2 or FIPS 140-3 validated cryptography modules (minimally Impact Level 1) operated in FIPS mode in accordance with federal government policy/standards for the protection of all CUI.
    - Cryptography module is defined as cryptographic algorithm, RNG, KMI, HASH, etc. (all approved functions).
- CSP Mission Owner maintains control of the keys, from creation through storage and use to destruction.
    - Implement Hardware Security Modules (HSMs) or Key Management Servers as needed to store, generate, and manage keys within the DISN; or
    - Order a CSP service that provides a dedicated HSM that is managed solely by the MO; or
    - Order a CSP KMS service that has been evaluated by NSA." – MO SRG [10].

When possible, use an approved CSP-provided encryption and Key Management Service (KMS) "for management of customer keys by the customer while preventing CSP access to the keys. It is recommended that such CSP KMS services be evaluated by NSA." – CSP SRG [11].

Enable encryption in the IaC templates discussed in Play 6.

National Security Systems (NSS) must use the algorithms in the NSA-approved Commercial National Security Algorithm (CNSA) Suite as described in Annex B of Committee on National Security Systems Policy (CNSSP) 15 [44].

In the future, quantum computing will obsolete some algorithms, but there are other quantum-resistant algorithms.

Actions

- ☐ Enable encryption-in-transit.
- ☐ Enable encryption-at-rest.
- ☐ Enable encryption in IaC templates.
- ☐ Use an approved CSP-provided encryption and Key Management Service (KMS).
- ☐ Use approved encryption algorithms.

Play 14. Use Secure Cloud Secrets Management Practices

It is critical to manage keys and other secrets as these are literally keys to other information in the systems. An example of this was a 2023 attack on Microsoft by a state actor that used a Microsoft Services Account consumer token signing key to forge tokens to access Microsoft Exchange Online accounts [34] [45].

Use cloud native Key Management (KM) services. These services are integrated with other cloud services, simplifying protection. These cloud native KM services can provide audit information about keys, including creation, usage and destruction. It is also possible to use keys generated outside the cloud [46].

Actions

Actions to take include:

- □ Manage secrets (e.g., keys) both for person entities (PEs) and non-person entities (NPEs).
- □ Use CSP tools such as AWS Secrets Manager or Azure Key Vault to manage secrets.

There are also three mitigation actions related to keys discussed in *Top Threats to Cloud Computing: Pandemic 11 Deep Dive*, 2023 [47].

- □ Key Rotation - Rotate cryptographic keys per the calculated cryptographic period, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.
- □ Key Suspension - Define, implement, and evaluate processes, procedures, and technical measures to monitor, review, and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.
- □ Key Deactivation - Define, implement, and evaluate processes, procedures, and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.

Play 15. Deploy User and Entity Behavior Analytics

Deploy User and Entity Behavior Analytics (UEBA) to detect anomalous behavior. This is typically implemented with a tool provided by the CSP. The CSSP should monitor the resulting behavioral analytics.

UEBA uses “behavioral analytics, machine learning algorithms and automation to identify abnormal and potentially dangerous user and device behavior” – [48].

UEBA analyzes both person entity (PE) and non-person entity (NPE) behavior patterns. NPEs include servers, routers and Internet of Things (IoT) devices. UEBA detects anomalous behavior that could indicate an attack in progress.

UEBA is “effective at identifying insider threats—malicious insiders or hackers who use compromised insider credentials—that can elude other security tools because they mimic authorized network traffic.” – [48].

UEBA is part of a zero trust (ZT) architecture (for more on ZT, see Play 22 in Volume 2).

UEBA should be employed along with other cybersecurity tools. Indeed, some UEBA functions may be part of SIEM, SOAR, or XDR solutions (for a discussion of those terms, see Play 10).

Capabilities

This section discusses known capabilities of some commonly used CSPs in the DoD.

AWS Guard Duty has some UEBA capabilities, though its description here does not currently mention UEBA; instead, it offers Machine Learning (ML) enabled threat detection.

On Azure, Microsoft Sentinel includes UEBA capabilities. It uses machine learning to correlate various attributes such as action type, geo-location, device, resource, Internet Service Provider, and others to trigger anomaly detection [49].

As an example of the kinds of anomalies a UEBA can detect, Microsoft Sentinel currently detects these anomalies [49]:

- Anomalous Account Access Removal
- Anomalous Account Creation
- Anomalous Account Deletion
- Anomalous Account Manipulation
- Anomalous Code Execution
- Anomalous Data Destruction
- Anomalous Defensive Mechanism Modification

- Anomalous Failed Sign-in
- Anomalous Password Reset
- Anomalous Privilege Granted
- Anomalous Sign-in

Actions

□ Enable the UEBA feature for the selected CSP.

□ Put in place a plan to execute when an anomaly is found. Realize that there will be many false positives to handle.

□ The CSSP should monitor the resulting UEBA analytics.

Play 16. Apply Network Segmentation

Network segmentation provides a mechanism to isolate or segregate assets from other assets; it is a kind of network isolation. Network Isolation techniques prevent network hosts from accessing non-essential system network resources.[25] Network isolation is illustrated in the next figure.[26]

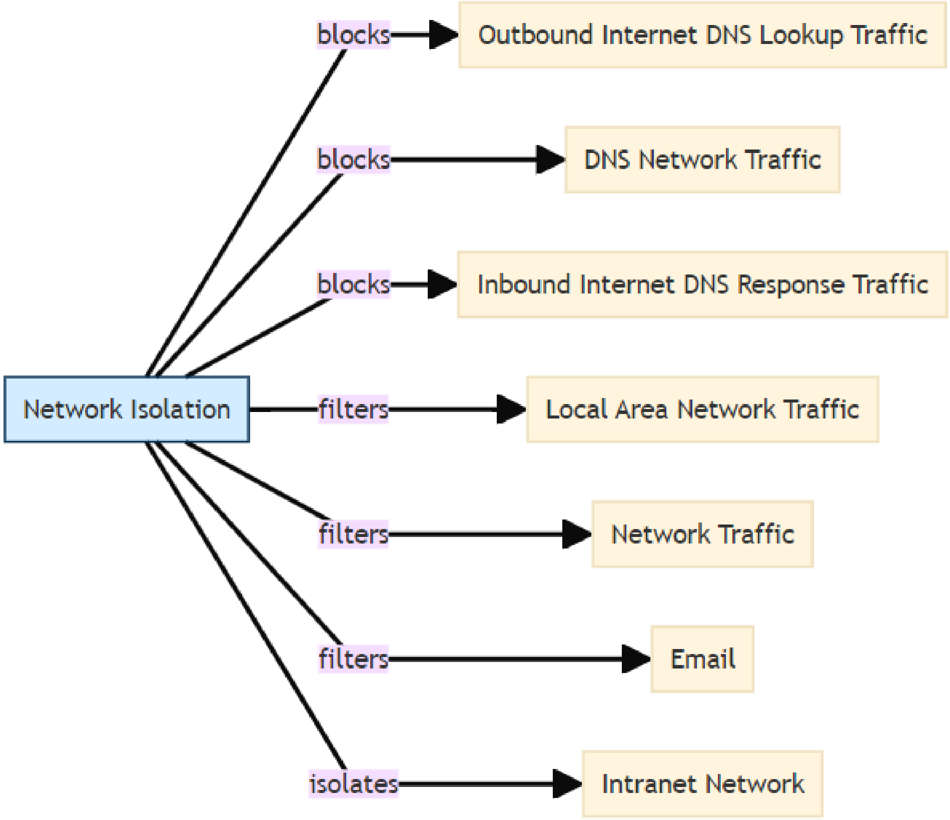

Figure 6. Network Isolation

There are two types of network segmentation: macro segmentation and micro segmentation.

Macro segmentation is traditional network segmentation, in which the network is separated into segments of Internet Protocol (IP) addresses to create security zones. For example, there should be at least these segments: development, test, and production. Most will also have staging or pre-production, and some will have an integration segment as well.

[25] Network Isolation - Technique D3-NI | MITRE D3FEND™

[26] Figure source: Network Isolation - Technique D3-NI | MITRE D3FEND™

Macro Segmentation capabilities are perimeter-oriented services that include but are not limited to cloud-based firewalls, web/API gateways, virtual networks, and subnets.

Cloud Service Providers use software defined networking to create Virtual Networks (VNets) or Virtual Private Clouds (VPCs), which are macro segments.

One action is to configure separate virtual private cloud (VPC) instances on AWS, or Virtual Network (VNet) instances on Microsoft Azure to isolate critical systems hosted in the cloud.[27] In addition, both AWS and Microsoft Azure provide logical boundary constructs to provide an additional capability to segment networks and cloud workloads[28] using Azure subscriptions and resource groups for Azure, and AWS accounts and resource groups in AWS.

Micro segmentation further sub-divides the network into smaller segments. For example, two micro services that interact frequently might use their own micro segment for that interaction; in other words, they might only use a restricted set of IP addresses. If all calls between the two services are restricted to this micro segment, it reduces the attack surface for those micro services. For example, suppose an entity makes a call to the API of one of those micro services from an IP address outside that micro segment, then the call can be rejected since calls are only allowed within the micro segment.

Micro Segmentation capabilities are workload or storage-oriented network security services that include, but are not limited to cloud service firewalls, virtual workload security groups, and host-based firewalls.

Cloud Service Providers (CSP) provide network security services and capabilities that enable an organization to apply macro and micro segmentation in their environment [5]. Applying macro and micro segmentation in a cloud environment to isolate workloads and resources by function achieves a defense-in-depth approach for network security, increasing the complexity and difficulty for adversaries to move laterally[29]. Implementation of network segmentation and the macro and micro level aligns to DoD's Network/Environment pillar of Zero Trust [18]. This can be further supplemented by dividing a cloud environment into different network segments that isolate and distinguish an organization's development, test, and production workloads that aligns with DoD's Enterprise DevSecOps Reference Design [42].

[27] https://attack.mitre.org/mitigations/M1030/

[28] See the glossary for a definition of cloud workload.

[29] https://attack.mitre.org/mitigations/M1030/

CSPs' Software Defined Networking (SDN) capabilities enable organizations to logically separate control and data planes, effectively establishing an out-of-band network, that is in alignment with DoD Zero Trust and NSA guidance [50] [36].

In addition, monitoring and logging of these network segmentation capabilities' network access decisions and configuration changes can help detect adversary lateral movement.[30]

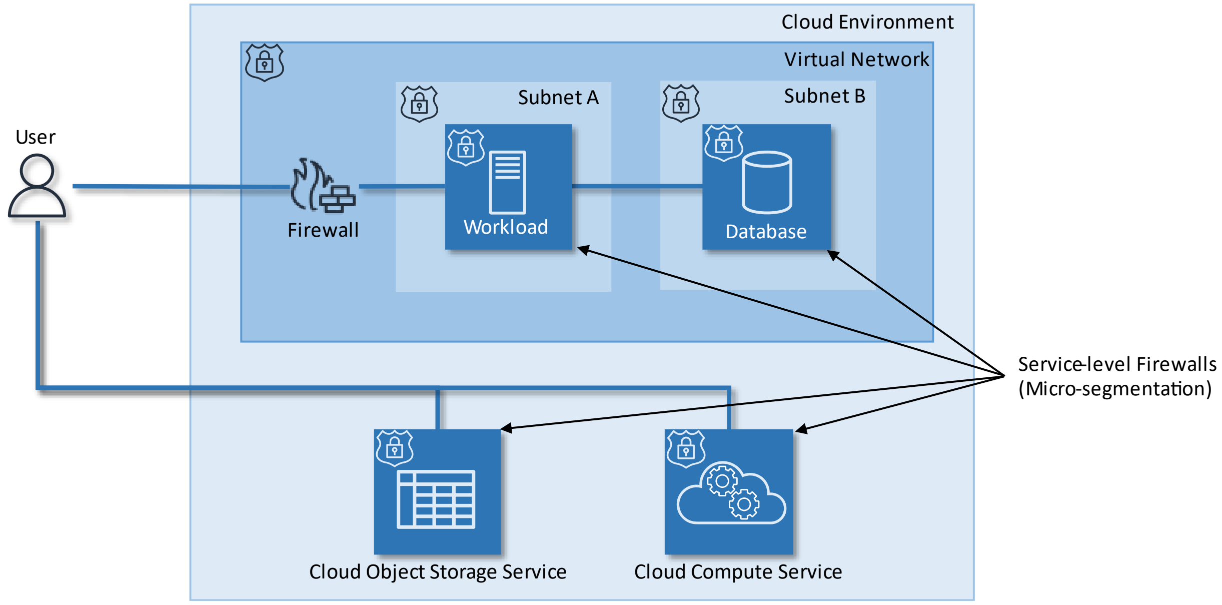

Figure 7. Network Segmentation in the Cloud

Actions

- ☐ Implement macro-segmentation to establish a secure cloud perimeter.
- ☐ Configure separate virtual private cloud (VPC) or virtual network (VNet) instances to isolate mission critical systems that are hosted in a cloud.[31]
- ☐ Implement micro segmentation to further isolate cloud workloads by function.
- ☐ Implement out-of-band networks to separate data and control planes, enabling management of cloud workloads through approved connections.
- ☐ Log network segmentation capabilities' network access decisions along with configuration changes.
- ☐ Conduct periodic reviews of network segmentation design and update to align with changes in the network architecture.

[30] https://attack.mitre.org/tactics/TA0008/

[31] https://attack.mitre.org/mitigations/M1030/

Play 17. Implement Cyber Resiliency

Cyber resiliency is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.[32]” – *NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* [51].

Implementing cyber resiliency is an important part of mission assurance.

Cyber Resiliency Goals

The cyber resiliency goals, as stated in [51] are:

- Anticipate – maintain a state of informed preparedness for adversity.
- Withstand – continue essential mission functions despite adversity.
- Recover – restore mission functions during and after adversity.
- Adapt – modify mission functions or supporting capabilities in response to predicted changes in the technical, operational, or threat environments.

Cyber Resiliency Objectives

Cyber resiliency objectives are “specific statements of what a system is intended to achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security” [51]. The following are from [51].

- Prevent or Avoid - Preclude the successful execution of an attack or the realization of adverse conditions.
- Prepare - Maintain a set of realistic courses of action that address predicted or anticipated adversity.
- Continue - Maximize the duration and viability of essential mission or business functions during adversity.
- Constrain – Limit damage from adversity.
- Reconstitute - Restore as much mission or business functionality as possible after adversity.
- Understand - Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.
- Transform - Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.

[32] A **cyber resource** is “an information resource which creates, stores, processes, manages, transmits, or disposes of information in electronic form and that can be accessed via a network or using networking methods” [51].

- Re-architect - Modify architectures to handle adversity and address environmental changes more effectively.

Cyber Resiliency Techniques

The following 14 techniques, from [51], are part of the cyber resiliency engineering framework:

1. Adaptive Response: Implement agile courses of action to manage risks.
2. Analytic Monitoring: Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.
3. Contextual Awareness: Construct and maintain current representations of the posture of missions or business functions while considering threat events and courses of action.
4. Coordinated Protection: Ensure that protection mechanisms operate in a coordinated and effective manner.
5. Deception: Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.
6. Diversity: Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.
7. Dynamic Positioning: Distribute and dynamically relocate functionality or system resources.
8. Non-Persistence: Generate and retain resources as needed or for a limited time.
9. Privilege Restriction: Restrict privileges based on attributes of users and system elements, as well as on environmental factors.
10. Realignment: Structure systems and resource use to align with mission function needs, reduce current and anticipated risks, and accommodate the evolution of technical, operational, and threat environments.
11. Redundancy: Provide multiple protected instances of critical resources.
12. Segmentation: Define and separate system elements based on criticality and trustworthiness.
13. Substantiated Integrity: Ascertain whether critical system elements have been corrupted.
14. Unpredictability: Make changes randomly or unpredictably.

Recommended Approaches

The following recommended approaches for cloud and virtual environments come from *Resiliency Mitigations in Virtualized and Cloud Environments* [52].

1. Analytic Monitoring: Monitoring & Damage Assessment - monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.
2. Analytic Monitoring: Sensor Fusion & Analysis - fuse and analyze monitoring data and preliminary analysis results from different components, together with externally provided threat intelligence.
3. Non-Persistence: Non-Persistent Information - refresh information periodically, or generate information on demand, and delete the information when no longer needed.
4. Non-Persistence: Non-Persistent Services - refresh services periodically or generate services on demand and terminate services after completion of a request.
5. Privilege Restriction: Privilege-Based Usage Restrictions - define, assign, maintain and apply usage restrictions on cyber resources based on mission criticality and other attributes.
6. Privilege Restriction: Privilege Management- define, assign, and maintain privileges associated with end users and cyber entities, based on established trust criteria, consistent with principles of least privilege.
7. Segmentation: Predefined Segmentation - define and separate components based on criticality and trustworthiness.
8. Coordinated Defense: Technical Defense-in-Depth - use multiple protective mechanisms at different architectural layers or locations.
9. Coordinated Defense: Coordination and Consistency Analysis - apply processes, supported by analytic tools, to ensure that defenses are applied, and cyber courses of action are defined and executed in a coordinated, consistent way that minimizes interference.
10. Realignment: Restriction - remove or disable unneeded risky functionality or connectivity or add mechanisms to reduce the risk.
11. Substantiated Integrity: Behavior Validation - validate the behavior of a system, service, or device against defined or emergent criteria.

Actions

- □ Create a cyber resilience plan. It should include the following from *Advancing Cyber Resilience with Cloud Computing* [53].
    - ○ Identify key threats and assess their impact on critical systems and functions.
    - ○ Identify and prioritize critical services.
    - ○ Set cyber resilience goals and objectives.
    - ○ Develop desired cyber resilience outcomes and identify and test capabilities.
    - ○ Define roles and responsibilities for cyber resilience and determine resources needed.
- □ Enable automatic scaling (both up and down) for the software system. This will help with resilience, for example when there is a high load on the system.
- □ Deploy immutable artifacts (e.g., immutable containers that are not manually configured), and use IaC for cloud services.
    - ○ This makes it possible to stand up another instance of a service or a container (or VM) quickly in another location that is identical.
    - ○ It also provides the ability to kill containers, VMs, or cloud service instances and bring up a fresh instance. This can be done periodically and at random. This is easier to do if the software in the containers is stateless.
- □ Set up automated backups.
- □ Restrict write-access to backups. This helps counteract ransomware TTPs used by malicious cyber actors to target data backups [28].
- □ Provision separate backup management accounts for administrators who require access to the backups. This reduces the risk of cloud environment data backup breaches [28].
- □ Ensure that there is at least one other availability zone (or data center) containing the data and software. The MO may also specify that more than two are necessary.
- □ Implement a Disaster Recovery (DR) plan and test it.
- □ Enable Continuity of Operations (COOP) and test it.

Play 18. Account for Complexities of Hybrid Cloud and Multi-Cloud Environments

A hybrid cloud environment means that some software components run in a cloud, while some run in on-premises infrastructure. In a multi-cloud environment, some components run in one cloud and some in another. Each of these options introduces significant complexities. These complexities include:

- Learning the services and interfaces of each cloud or on-premises vendor
- Maintaining data flows between clouds and on-premises
- Controlling user access to all environments. For example, there have been several instances of hackers breaking into an on-premises environment and using that access to break into the cloud environment.
- Lack of overall visibility into cloud resources and services
- Maintaining compliance in each environment
- Knowledge of how to secure each environment.

For organizations new to the cloud, consider focusing on one cloud before implementing a multi-cloud approach.

Actions

The following best practices to protect these environments come from *Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments*, NSA, 2024 [27].

- □ Use infrastructure as code to deploy infrastructure resources from a centralized location.
- □ Ensure training is ongoing for all cloud environments in use to avoid gaps in skillsets.
- □ Minimize data flows between environments to paths necessary for day-to-day operations.
- □ Ensure CNSA Suite approved algorithms are used.
- □ Follow NSA and NIST guidelines to determine the best IAM solution to meet organizational needs.
- □ Define access control policies uniformly to ensure user access is consistent across all environments.
- □ Use a centralized solution to aggregate logs and facilitate active monitoring and threat hunting.
- □ Avoid vendor lock-in and enable redundancy across multiple environments to ease disaster recovery efforts for cloud assets and resources.

□ Codify security and compliance best practices through policy as code.

Conclusion

This playbook has taken the reader on a cloud security journey from preparing their organization and understanding key concepts like the shared responsibility model, the impact level, and the requirement of a DoD PA or ATO for cloud services.

Now continue to Volume 2 of the Cloud Security Playbook, which includes some advanced plays, such as plays to secure containers and to defend DevSecOps pipelines. These pipelines can be part of a DoD Software Factory. Using such a factory with a Continuous Authorization to Operate (cATO) is typically the quickest way to achieve authorization to deploy an application into production in a cloud.

While the Playbook is not a compendium of all cloud security mitigations, it provides numerous actions that mission owners can take to significantly improve their security in a cloud.

References

[1] United States Department of Homeland Security, "Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023," 2 April 2024. [Online]. Available: https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer.

[2] Cloud Security Alliance, "Top Threats to Cloud Computing: Pandemic Eleven," 2022. [Online]. Available: https://cloudsecurityalliance.org/research/working-groups/top-threats.

[3] National Cyber Security Centre (NCSC), "The Near-term Impact of AI on the Cyber Threat, NCSC," 24 January 2024. [Online]. Available: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

[4] Unit 42, Palo Alto Networks, "Cloud Threat Report, Navigating the Expanding Attack Surface, Volume 7," 2024.

[5] NSA, "NSA's Top Ten Cloud Security Mitigation Strategies," 2024. [Online]. Available: https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF.

[6] Orca Security, "State of Cloud Security Report 2024," 2024. [Online]. Available: https://orca.security/lp/2024-state-of-cloud-security-report/.

[7] DoD CIO, "DoD Joint Warfighter Cloud Capability (JWCC) & Next Steps to Rationalize Cloud Use Across the DoD," 2 August 2023. [Online]. Available: https://dodcio.defense.gov/Library/.

[8] DoD CIO, "DoD Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations," 25 July 2017. [Online]. Available: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/853001p.pdf.

[9] DoD CIO, "Directive-type Memorandum (DTM) 24-001 – DoD Cybersecurity Activities Performed for Cloud Service Offerings," 27 February 2024. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-24-001.pdf?ver=0Em4aRFXCliZK833wVS3IA%3D%3D.

[10] DISA, "Cloud Computing Mission Owner Security Requirements Guide Overview," 14 June 2024. [Online]. Available: https://public.cyber.mil/dccs/dccs-documents/.

[11] DISA, "Cloud Service Provider (CSP) Security Requirements Guide (SRG), Version 1, Release 1," 14 June 2024. [Online]. Available: https://public.cyber.mil/dccs/dccs-documents/.

[12] NSA, "Uphold the Cloud Shared Responsibility Model," 2024. [Online]. Available: https://media.defense.gov/2024/Mar/07/2003407863/-1/-1/0/CSI-CLOUDTOP10-SHARED-RESPONSIBILITY-MODEL.PDF.

[13] Commitee on National Security Systems, "Committee on National Security Systems (CNSS) Instruction No. 1253, Categorization and Control Selection for National Security Systems," 29 July 2022. [Online]. Available: https://www.cnss.gov/cnss/.

[14] DoD CIO, "DoDI 8510.01, Risk Management Framework (RMF) for DoD Systems," 19 July 2022. [Online]. Available: https://dodcio.defense.gov/Library/.

[15] DISA Cloud Assessment Division (RE2), DISA Risk Management Directorate, "DoD Cloud Authorization Process," June 2024. [Online]. Available: https://public.cyber.mil/dccs/dccs-documents/.

[16] DISA, "Secure Cloud Computing Architecture (SCCA) Program Overview," February 2024. [Online].

[17] DISA, "DoD Cloud Connection Process Guide, Version 2," March 2017. [Online]. Available: https://www.disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf.

[18] DISA Risk Management Office, "Cloud Access Point (CAP) Security Functional Requirements Document (FRD) V1.7," 2 April 2015. [Online]. Available: https://disa.deps.mil/disa/applications/ESPortal/EntResAna/RAO/Project%20Documents/Clo ud%20Access%20Point%20(CAP)%20-%2033/CAP%20FRD%20draft%2004-10- 2015%20v1.6.pdf.

[19] DISA, "Defense Information Systems Network (DISN) Connection Process Guide (CPG), Version 6.1," August 2023. [Online]. Available: https://dl.cyber.mil/connect/pdf/unclass-DISN_CPG.pdf.

[20] DISA Cloud Assessment Division (RE2), DISA Risk Management Directorate, "DoD Cloud Process Guide," June 2024. [Online]. Available: https://public.cyber.mil/dccs/dccs-documents/.

[21] DISA, "Department of Defense (DoD) Cloud Native Access Point (CNAP) Reference Design (RD), Version 1.0," 29 July 2021. [Online]. Available: https://dodcio.defense.gov/Library/.

[22] Defense Information Systems Agency (DISA) and National Security Agency (NSA), "DoD Zero Trust Reference Architecture Version 2.0," July 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[23] NSA, "Enforce Secure Automated Deployment Practices through Infrastructure as Code," 7 3 2024. [Online]. Available: https://media.defense.gov/2024/Mar/07/2003407857/-1/-1/0/CSI-CLOUDTOP10-INFRASTRUCTURE-AS-CODE.PDF.

[24] DoD CIO, "DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0," June 2020. [Online]. Available: https://dodcio.defense.gov/Library/.

[25] DoD CIO, "DoDI 8520.03, Identity Authentication for Information Systems," May 2023. [Online]. Available: https://dodcio.defense.gov/Library/.

[26] CISA, "Implementing Phishing-Resistant MFA," Oct 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[27] NSA, "Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments," 7 3 2024. [Online]. Available: https://media.defense.gov/2024/Mar/07/2003407865/-1/-1/0/CSI-CLOUDTOP10-HYBRID-MULTI-CLOUD.PDF.

[28] NSA, "Use Secure Cloud Identity and Access Management Practices," 2024. [Online]. Available: https://media.defense.gov/2024/Mar/07/2003407866/-1/-1/0/CSI-CloudTop10-Identity-Access-Management.PDF.

[29] DoD CIO, "DoDI 8520.02, Public Key Infrastructure and Public Key Enabling," May 2023. [Online]. Available: https://dodcio.defense.gov/Library/.

[30] DoD CIO, "DoD Mobile Public Key Infrastructure (PKI) Credentials," December 2019. [Online]. Available: https://dodcio.defense.gov/Library/.

[31] DoD CIO, "Identity, Credential, and Access Management (ICAM) Strategy," March 2020. [Online]. Available: https://dodcio.defense.gov/Library/.

[32] National Institute of Standards and Technology, "Separation of Duty," 2017. [Online]. Available: https://csrc.nist.gov/glossary/term/separation_of_duty.

[33] NSA, "Manage Cloud Logs for Effective Threat Hunting," 7 March 2024. [Online]. Available: https://media.defense.gov/2024/Mar/07/2003407864/-1/-1/0/CSI_CLOUDTOP10-LOGS-FOR-EFFECTIVE-THREAT-HUNTING.PDF.

[34] Cyber Safety Review Board, "Review of the Summer 2023 Microsoft Exchange Online Intrusion," 20 March 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

[35] IBM, "What is SOAR (security orchestration, automation and response)?," [Online]. Available: https://www.ibm.com/topics/security-orchestration-automation-response. [Accessed July 2024].

[36] DoD CIO, "DoD Zero Trust Capability Execution Roadmap (COA1)," 6 Jan 2023. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilitiesActivities.pdf.

[37] DoD CIO, "DevSecOps Continuous Authorization to Operate Evaluation Criteria," 2024. [Online]. Available: https://rmfks.osd.mil.

[38] DoD CIO, "DOD Manual (DODM) 8530.01, Cybersecurity Activities Support Procedures," 31 May 2023. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/853001p.PDF?ver=BFUagWhkQR8fBXzxRjIqxQ%3D%3D.

[39] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," 10 December 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5.

[40] NSA, "Continuously Hunt for Network Intrusions," 2019. [Online]. Available: https://media.defense.gov/2019/Sep/09/2002180360/-1/-1/0/Continuously%20Hunt%20for%20Network%20Intrusions%20-%20Copy.pdf.

[41] NSA, "Network Infrastructure Security Guide," October 2023. [Online]. Available: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF.

[42] DoD CIO, "DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes, Version 2.1," Sep 2021. [Online]. Available: https://dodcio.defense.gov/Library/.

[43] A. Parmar, "TotalCloud Insights: Securing Your Data—The Power of Encryption in Preventing Threats," June 2024. [Online]. Available: https://blog.qualys.com/product-tech/2024/06/04/totalcloud-insights-securing-your-data-the-power-of-encryption-in-preventing-threats.

[44] Committee on National Security Systems Policy (CNSSP), "Annex B of Committee on National Security Systems Policy (CNSSP) 15," October 2016. [Online]. Available: https://www.cnss.gov/CNSS/issuances/Policies.cfm.

[45] S. Lyngaas, "US government review faults Microsoft for ‘cascade’ of errors that allowed Chinese hackers to breach senior US officials’ emails," 02 April 2024. [Online]. Available: https://www.cnn.com/2024/04/02/tech/us-government-microsoft-hack/index.html.

[46] NSA, "Mitigating Cloud Vulnerabilities," January 2020. [Online]. Available: https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF.

[47] Cloud Security Alliance, "Top Threats to Cloud Computing: Pandemic 11 Deep Dive," 2023.

[48] IBM, "What is user and entity behavior analytics (UEBA)?," [Online]. Available: https://www.ibm.com/topics/ueba. [Accessed 5 July 2024].

[49] Microsoft, "Anomalies detected by the Microsoft Sentinel machine learning engine," 3 April 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/sentinel/anomalies-reference#ueba-anomalies.

[50] NSA, "Performing Out-of-Band Network Management," 2020. [Online]. Available: https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT20200911.PDF.

[51] NIST, "NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," December 2021. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-160v2r1.

[52] E. Laderman and K. Cox, "Resiliency Mitigations in Virtualized and Cloud Environments," The MITRE Corporation, 2016.

[53] P. Nicholas and K. Ciglic, "Advancing Cyber Resilience with Cloud Computing," 2017. [Online]. Available: https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-cyber-resilience-with-cloud-computing.

[54] A. Chaudhary, "Managing Cloud Misconfigurations Risks," Cloud Security Alliance, 14 August 2023. [Online]. Available: https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks.

[55] U.S. Congress, "National Artificial Intelligence Initiative Act of 2020 (enacted as Division E of the William M . (Mac) Thornberry National Defense Authorization Act for

Fiscal Year 2021 (Public Law 116-283), Section 5002(3)," 2021. [Online]. Available: https://www.congress.gov/bill/116th-congress/house-bill/6216/text#toc-H41B3DA72782B491EA6B81C74BB00E5C0.

[56] NIST, "NIST SPECIAL PUBLICATION 1800-19, Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments," April 2022. [Online]. Available: https://doi.org/10.6028/NIST.SP.1800-19.

[57] DoD CIO, "DevSecOps Continuous Authorization Implementation Guide," March 2024. [Online]. Available: https://dodcio.defense.gov/Library/.

[58] DoD CIO, "DoD Enterprise DevSecOps Fundamentals," September 2021. [Online]. Available: https://dodcio.defense.gov/Library/.

Appendix A. Resources

This appendix offers sources of adversarial techniques and countermeasures for these techniques.

MITRE ATT&CK® Adversarial Techniques

For a list of adversarial techniques, see MITRE ATT&CK®. ATT&CK is "a knowledge base of adversarial techniques based on real-world observations. ATT&CK focuses on how adversaries interact with systems during an operation, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target."

This free service is widely used in both the DoD and industry.

MITRE D3FEND™ Countermeasures

MITRE Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND™) is a knowledge graph of cybersecurity countermeasures. Each countermeasure is linked to ATT&CK adversarial techniques that they counter. This free service can be found here: MITRE D3FEND™.

CAVEaT™ Cloud Threat Model

Cloud Adversarial, Vectors, and Threats (CAVEaT™) is a joint effort between the Cloud Security Alliance (CSA) and MITRE. The intent is to "develop, curate, and host a cloud specific threat model to assist Cloud Security practitioners with threat-based analysis." It can be found here: CAVEaT™ | CSA.

OWASP® Top 10 Web Application Security Risks

Web applications should address the OWASP® Top 10 Web Application Security Risks. Briefly, these risks are:

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

Most of these are addressed in various plays in this Playbook. But some, such as Insecure Design, are specific to the application and out of scope for this document.

OWASP® API Security Top 10

The OWASP® API Security Top 10 for 2023 are listed below.

- API1:2023 - Broken Object Level Authorization – APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.
- API2:2023 - Broken Authentication – Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user compromises API security overall.
- API3:2023 - Broken Object Property Level Authorization – This category combines API3:2019 Excessive Data Exposure and API6:2019 - Mass Assignment, focusing on the root cause: the lack of or improper authorization validation at the object property level. This leads to information exposure or manipulation by unauthorized parties.

- API4:2023 - Unrestricted Resource Consumption – Satisfying API requests requires resources such as network bandwidth, Central Processing Unit (CPU), memory, and storage. Other resources such as emails/texts/phone calls or biometrics validation are made available by service providers via API integrations and paid for per request. Successful attacks can lead to Denial of Service or an increase in operational costs.
- API5:2023 - Broken Function Level Authorization – Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions.
- API6:2023 - Unrestricted Access to Sensitive Business Flows – APIs vulnerable to this risk expose a business flow - such as buying a ticket, or posting a comment - without compensating for how the functionality could harm the business if used excessively in an automated manner. This doesn't necessarily come from implementation bugs.
- API7:2023 - Server-Side Request Forgery – Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied Uniform Resource Identifier (URI). This enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.
- API8:2023 - Security Misconfiguration – APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Software and DevOps engineers can miss these configurations, or don't follow best security practices when it comes to configuration, opening the door for different types of attacks.
- API9:2023 - Improper Inventory Management – APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. A proper inventory of hosts and deployed API versions also are important to mitigate issues such as deprecated API versions and exposed debug endpoints.
- API10:2023 - Unsafe Consumption of APIs – Developers tend to trust data received from third-party APIs more than user input, and so tend to adopt weaker security standards. To compromise APIs, attackers go after integrated third-party services instead of trying to compromise the target API directly.

Cloud Misconfigurations

"Misconfiguration is a concern in cloud computing due to the complexity of multi-cloud settings and the difficulty of manually identifying and correcting errors. It occurs when settings, permissions, or access controls are not properly configured or are left at default values, which can expose sensitive information, grant excessive privileges, or create unintended security gaps. Misconfigurations can lead to unauthorized access, data breaches, service disruptions, or other security incidents." – *Managing Cloud Misconfigurations Risks* [54], which is the source for Table 3.

Table 3. Possible Cloud Misconfiguration Areas in Popular Environments

Types	AWS	Azure
Access Management	• IAM Overly Permissive Role Policies • Overly Permissive Customer-based inline policies • Common usage of Root user	• Azure AD Directory Access. • Guest Users in Azure AD • Mismanaged User roles
Serverless	• Lambda Functions are accessible globally • Using out-of-date runtime environments • Lack of encryption in the lambda runtime environment	• Hosting a website that contains vulnerabilities • The database doesn't have any encryption policies • Not configuring a Web Application Firewall (WAF) to manage & block traffic
Virtual Environment	• No Limits on OnDemand vCPU Instances • Instance IAM role limitless access • Custom ports are allowed	• No limits in VM Instances • VM AD Authentication Disabled • Custom Ports enabled
Networking	• IP Forwarding Enabled • Enabling Public Ingress & Egress in Security Groups • Public IP enabled on EC2	• IP Forwarding Enabled • Enabling Public Ingress & Egress in Network Security Groups • Public IP on Virtual Machine
Databases	• Table Backup Exists • No Encryption when implementing the Accelerator cluster • Rest Encryption Disabled	• Secure Sockets Layer (SSL) not enforced, and retention Period not set • Threat enable is not set • Publicly accessible database

Appendix B. Glossary

Term **Definition**

Artificial Intelligence (AI)

AI is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to

a) perceive real and virtual environments;
b) abstract such perceptions into models through analysis in an automated manner; and
c) use model inference to formulate options for information or action.

(Source: *National Artificial Intelligence Initiative Act of 2020 (Public Law 116-283) Section 5002(3)* [55]).

Cloud Service Offering (CSO)

A CSO is a service offered by a CSP. Each CSP provides many different CSOs.

Cloud Service Provider (CSP)

A CSP is an entity that offers one or more cloud services in one or more deployment models. Each CSP provides many CSOs. – (Source: *Cloud Service Provider (CSP) Security Requirements Guide (SRG)*, Version 1, Release 1, DISA,14 June 2024 [11].

Cloud workload

A logical bundle of software and data that is present in, and processed by, a cloud computing technology. (Source: NIST SP 1800-19 [56]).

Continuous Authorization to Operate (cATO)

Continuous Authorization to Operate (cATO) is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in their ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust information security continuous monitoring capabilities, active cyber defense, and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system’s cyber posture. (Source: *DevSecOps Continuous Authorization Implementation Guide* [57]).

DevSecOps pipeline

A collection of DevSecOps tools, upon which the DevSecOps process workflows can be created and executed. (Source: *DoD Enterprise DevSecOps Fundamentals* [58]).

DevSecOps Platform (DSOP)

The set of tools and automation that enables a software factory. It includes the ability to create DevSecOps pipelines with control gates, and to deploy software into development, test, and staging/pre-production environments. It may also deploy into production, depending on the production environment. (Source: *DevSecOps Continuous Authorization Implementation Guide* [57]).

Generative AI

AI that can generate new content, such as text, images or video. Large Language Models (LLMs) are an example of generative AI. (Source: *The near-term impact of AI on the cyber threat*, 2024 [3]).

Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (Source: NIST Glossary).

Large Language Model (LLM)

A large language model (LLM) is a specialized type of artificial intelligence (AI) that has been trained on vast amounts of text to understand existing content and generate original content. (Source: Gartner Glossary)

Machine Learning (ML)

Machine Learning is an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed. (Source: National Artificial Intelligence Initiative Act of 2020 (Public Law 116-283) Section 5002(3) [55]).

Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (Source: NIST Glossary)

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (Source: NIST Glossary).

Software Factory

A DSOP combined with the people and processes that support the DSOP, as well as a hosting environment such as a cloud; it includes at least development, test and staging/pre-production environments, and it may include a production environment, as well as other environments such as integration. (Source: *DevSecOps Continuous Authorization Implementation Guide* [57]).

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (Source: NIST Glossary).

Vulnerability

A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Source: NIST Glossary)

Appendix C. Acronyms

Acronym	Definition
3PAO	Third Party Assessment Organization
ACAS	Assured Compliance Assessment Solution
AD	Active Directory
AI	Artificial Intelligence
AO	Authorizing Official
API	Application Programming Interface
APT	Advanced Persistent Threat
AST	Application Security Testing
ATO	Authorization to Operate
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
AWS	Amazon Web Services
BCAP	Boundary Cloud Access Point
BCD	Boundary Cyberspace Defense
BOM	Bill of Materials
C-ITP	Cloud Information Technology Project
CAC	Common Access Card
CAO	Connection Approval Office
CAP	Cloud Access Point
CATC	Cloud Authorization to Connect
CAVEaT	Cloud Adversarial, Vectors, and Threats
CC	Cloud Computing
CC SRG	Cloud Computing Security Requirements Guide
CD	Continuous Delivery
CDR	Cloud Detection and Response
CERT	Computer Emergency Readiness Team
CI	Continuous Integration
CI/CD	Continuous Integration / Continuous Delivery
CIEM	Cloud Infrastructure Entitlement Management
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CNAP	Cloud Native Access Point
CNAPP	Cloud-Native Application Protection Platform
CNCF	Cloud Native Computing Foundation
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COA	Course of Action

Acronym	Definition
COI	Community of Interest
COOP	Continuity of Operations
CPTC	Cloud Permission to Connect
CPTs	Cyber Protection Teams
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRT	Continuous Risk Treatment
CS	Cybersecurity
CSA	Cloud Security Alliance
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
CSSP	Cybersecurity Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
CWP	Cloud Workload Protection
D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
DAST	Dynamic Application Security Testing
DB	database
DCAS	DoD Cloud Authorization Services
DCAT	DoD Cyber Assessment Team
DCD	DODIN Cyberspace Defense
DCO	Defensive Cyberspace Operations
DCRT	DoD Cyber Red Team
DevSecOps	Development Security Operations
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMZ	demilitarized zone
DoD	Department of Defense
DoDI	Department of Defense Instruction
DODIN	DoD Information Network
DR	Disaster Recovery
DSAWG	DOD Security/Cybersecurity Authorization Working Group
DSOP	DevSecOps Platform
DSS	DISN Subscription Service
DTM	Directive-type Memorandum
EaC	Everything as Code
EDR	Endpoint Detection and Response
eMASS	Enterprise Mission Assurance Support Service

Acronym	Definition
ESF	Enduring Security Framework
ETL	Extract, Transform, and Load
FE	Federated Entity
FedRAMP	Federal Risk and Authorization Management Program
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standard
HA	High Availability
HIDS	Host Intrusion Detection System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IAP	Internet Access Point
IAST	Interactive Application Security Testing
IATT	Interim Authorization to Test
ICAM	Identity, Credential, and Access Management
ID	Identification
IdAM	Identify and Access Management
IDM	Internal Defensive Measures
IDS	Intrusion Detection System
IE	Information Enterprise
IL	Impact Level
IMDS	Instance Metadata Service
IoT	Internet of Things
IP	Internet Protocol
I/PaaS	Infrastructure or Platform as a Service
IPS	Intrusion Prevention System
IT	Information Technology
JFHQ	Joint Force Headquarters
JIT	Just-in-Time
JWCC	Joint Warfighter Cloud Capability
KM	Key Management
KMS	Key Management System
LLM	Large Language Model
MCA	Malicious Cyber Actor
MCD	Mission Cyberspace Defense
MFA	Multi-Factor Authentication
ML	Machine Learning
MO	Mission Owner
MOSA	Modular Open System Approach

Acronym	Definition
MPE	Mission Partner Environment
mTLS	mutual Transport Layer Security
NCSC	National Cyber Security Centre
NIC	Network Information Center
NIDS	Network Intrusion Detection System
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security Systems
OCI	Open Container Initiative
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
OS	Operating System
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PA	Provisional Authorization
PaaS	Platform as a Service
PaC	Policy as Code
PAW	Privileged Access Workstation
PBAC	Pipeline-Based Access Controls
PE	Person Entity
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
PoLP	Principle of Least Privilege
PPE	Poisoned Pipeline Execution
RD	Reference Design
RME	Risk Management Executive
RMF	Risk Management Framework
SaaS	Software as a Service
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SCAP	Security Content Automation Protocol
SDN	Software Defined Network
SDP	Software Defined Perimeter
SIEM	Security Information and Event Management
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SNAP	System Network Approval Process

Acronym	Definition
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SP	Special Publication
SQL	Structured Query Language
SRG	Security Requirements Guide
SSC	Sidecar Security Container
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
SSRF	Server-Side Request Forgery
STIG	Security Technical Implementation Guide
TAG	Technical Advisory Group
TLS	Transport Layer Security
TTP	Tactics, Techniques, and Procedures
U.S.	United States
UEBA	User and Entity Behavior Analytics
URI	Uniform Resource Identifier
US	United States
US-CERT	United States - Computer Emergency Readiness Team
VDMS	Virtual Datacenter Managed Service
VDSS	Virtual Datacenter Security Stack
VM	Virtual Machine
VNet	Virtual Network
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection and Response
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access