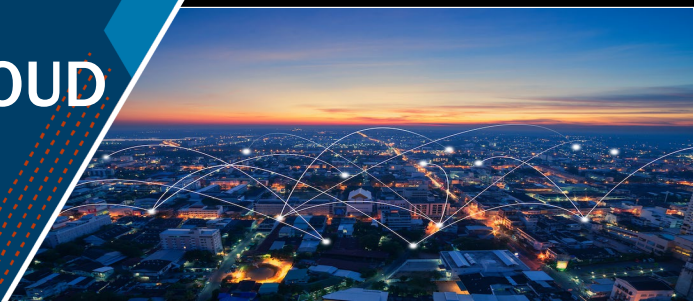
FREE TOOLS FOR CLOUD ENVIRONMENTS



OVERVIEW

This factsheet was developed for the purpose of aiding businesses transitioning into a cloud environment in identifying the proper tools and techniques needed for data security and protecting critical assets. This factsheet provides network defenders and incident response/analysts open-source tools, methods, and guidance for identifying, detecting, and mitigating cyber threats, known vulnerabilities, and anomalies while operating a cloud or hybrid environment.

Malicious cyber actors target organizations, on-premises, and cloud environments, who do not possess the proper resources for defending against cyber threats. As organizations continue to advance into operations associated with cloud and cloud computing, this factsheet provides tools and guidance that can be used to help mitigate the risk of information theft, data encryption and extortion, and information exposure. These tools assist in hardening network environments/infrastructure, preventing malicious compromise, detecting malicious activity, mapping potential threat vectors, and identifying malicious activity post compromise.

RESOURCE INTRODUCTION

Asset assessment and management is crucial when evaluating an organization's security posture. In hybrid cloud operations, it is likely that the organization and its cloud service provider (CSP) share the responsibility of securing critical assets. It is important for businesses to develop practices that evaluate industrial control systems (ICS) and IT security practices that best fit your organization before using cloud services.

With the development of cloud service platforms, CSPs have developed built-in security capabilities for organizations to use and enhance security capabilities while operating in cloud environments. Organizations should use these built-in security features from CSPs and take advantage of free CISA- and partner-developed tools/applications to fill security gaps and complement existing security features. All organizations should create a design phase aligned with Secure-by-Design concepts and strategies to architect the solutions required, forecasting security needs, and using free tools fitting with the organization.

Many open-source tools are available to investigate adversary activity in cloud environments. They can detect unusual activity, service principles, and cloud business application environments. Some open-source tools can help network defenders map threat actor behavior to MITRE ATT&CK® framework.

Organizations can use various open-source tools to evaluate their security posture, providing step-by-step processes that evaluate IT networks and security practices. For example, publicly available PowerShell tools exist that allow network defenders to investigate and aid an organization's security posture, including:

- The Cybersecurity Evaluation Tool (CSET) (CISA)
- SCuBAGear (CISA)
- The Untitled Goose Tool (CISA)
- Decider (CISA)
- Memory Forensic on Cloud (JPCERT/CC)

Note: These open-source tools are highlighted and explained to assist with on-site investigation and remediation in cloud environments but are not all-encompassing. Paid tools/services can complement open source. Most CSPs offer their own platform-specific monitoring and analysis tools, which typically allow network defenders to perform custom queries and write custom detection.

CISA TOOLS

The Cyber Security Evaluation Tool

CISA developed the Cyber Security Evaluation Tool (CSET) using industry-recognized standards, frameworks, and recommendations to assist organizations in evaluating their enterprise and asset cybersecurity posture. CSET asks detailed questions about organizations' system components, architectures, and operational policies and procedures. CSET uses provided answers to generate a report highlighting strengths and weaknesses and offering prioritized recommendations for optimizing an organization's cybersecurity posture.

As of CSET version 11.5, the tool includes a Cross-Sector Cyber Performance Goals (CPG) assessment intended to help organizations determine the extent to which they have implemented CISA's CPGs. The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), provide a minimum set of best practices and protection guidance that CISA and NIST recommend all organizations follow. CPGs are derived from existing cybersecurity frameworks and guidance to protect against the most common and impactful TTPs.

Network administrators of all organizations to include hybrid environments can use CSET to identify gaps and areas for future investment.

See CISA's CSET GitHub page for directions on downloading and using CSET.

SCuBAGear M365 Secure Configuration Baseline Assessment Tool

SCuBAGear is a CISA-created automation script for comparing Federal Civilian Executive Branch (FCEB) agency tenant configurations against CISA M365 baseline recommendations. SCuBAGear is part of CISA's Secure Cloud Business Applications (SCuBA) project, which provides guidance for FCEB agencies securing their cloud business application environments and protecting federal information created, accessed, shared, and stored in those environments. Although tailored to FCEB agencies, the project provides security guidance applicable to all organizations with cloud environments. CISA created the SCuBA program in response to the SolarWinds Orion software supply chain compromise. During the SolarWinds Orion supply chain compromise, threat actors changed domain federation trust settings using Azure Active Directory (AAD) administrative permissions; the threat actors configured the domain to accept authorization tokens signed using their own security assertion markup language (SAML) signing certificate. The actors used these tokens to access resources in hosted environments, such as email, for data exfiltration via an authorized application programmable interface (API). As part of SCuBA, CISA developed multiple documents that collectively provide guidance on cloud security and hardening:

- The SCuBA Technical Reference Architecture (TRA) – describes essential components of security services and capabilities to secure and harden cloud business applications, including the platforms hosting the applications. These security services and capabilities prevent and mitigate vulnerabilities and threats from affecting the cloud business applications during implementation, configuration, and administration. The scope of the TRA includes cloud business applications, delivered through a Software-as-a-Service (SaaS) model to users, and the security services used to secure and monitor these applications.
- The draft Hybrid Identity Solutions Architecture – presents potential approaches for addressing identity management in a hybrid environment.
- M365 security configuration baseline (SCB) guides – provide minimum viable secure configuration baselines for Microsoft Defender for Office 365, Azure Active Directory, Exchange Online, OneDrive for Business, Power BI, Power Platform, SharePoint Online, and Teams.

The SCuBAGear M365 SCB Assessment Tool verifies an organization's M365 tenant configuration conforms to the minimum viable security configurations described in the M365 SCB guides. The tool creates an HTML report highlighting policies that deviate from the SCB guides. Network administrators of all organizations with M365 tenant(s) can use the tool to quickly identify and address configuration gaps.

See CISA's SCuBAGear GitHub page for directions on installing and using the tool.

Untitled Goose Tool

CISA, together with Sandia National Laboratories, developed the Untitled Goose Tool to assist network defenders with hunt and incident response activities in Microsoft Azure, AAD, and M365 environments. This tool allows network defenders to query, export, and investigate audit logs, Unified Audit Logs (UALs), Azure activity logs, and Microsoft Defender for Endpoint (MDE) data. Untitled Goose Tool can support incident response teams by exporting cloud artifacts; this can be especially useful for environments that do not ingest logs into a security information and event management (SIEM) tool or other long-term solutions for log storage after an incident.

CISA developed the Untitled Goose Tool to fill a gap in PowerShell tools, which lacked data collection capacity for Azure, AAD, and M365 investigations. Many tools available prior to Untitled Goose Tool had the same overlaps (e.g., pulled the same data) but missed large amounts of critical data. Additionally, many tools could not extract the UAL in a timely fashion. Even when the tools extracted the data in a timely fashion, the logs were usually cut short due to PowerShell's restriction on number of log entries returned from a query (5000).

Untitled Goose Tool uses novel data-gathering methods via bespoke mechanisms to analyze and gather large M365 data sets via the UAL. This allows network defenders to:

1. Extract cloud artifacts from Microsoft's AAD, Azure, and M365 environments.
2. Perform time bounding of the UAL with goosey graze.
3. Extract data within those time bounds with goosey honk.
4. Collect data using time-bounding capabilities for MDE data.

See CISA's Untitled Goose Tool GitHub Repository for directions on installing and using the tool.

Decider Tool

For CISA, understanding malicious behavior is often the first step to protecting networks and data. Understanding malicious behavior can also improve network defenders' success in detecting and mitigating malicious cyber operations. CISA consistently encourages incident responders and analysts to leverage the MITRE ATT&CK framework in mapping observed threat actor activity to defined tactics and techniques.

MITRE ATT&CK is a free knowledge-based repository of cyber actors' tactics and techniques based on real-world observations. These tactics and techniques include known exploits used on cloud systems, such as Create Account: Cloud Account [T1136.003] and Cloud Infrastructure Discovery [T1580]. Understanding the techniques cyber threat actors use to compromise cloud environments can help defenders better target detections and mitigations to those techniques. This understanding can also assist network defenders in identifying tailored defenses. This framework provides an abundance of information for organizations of any size to leverage in their respective organizations.

Network defenders can leverage ATT&CK to identify defensive gaps, assess security tool capabilities, organize detections, hunt for threats, engage in red team activities, or validate mitigation controls.

On March 1, 2023, CISA, together with the Homeland Security Systems Engineering and Design Institute (HSSEDI), operated by the MITRE Corporation, released Decider. Decider assists incident responders and analysts in mapping observed activity to the MITRE ATT&CK framework. The tool makes mapping to ATT&CK easier by providing step-by-step guidance, including techniques used against cloud systems.

Decider starts with a series of questions to help network defenders properly identify adversary tactics, techniques, or sub-techniques. With Decider, users can filter queries relevant to user analysis to determine the best possible identification method. After gaining proper mapping accuracy, users are then able to:

- Export results to tables, such as ATT&CK Navigator heatmaps.
- Publish threat intelligence reports.

- Identify and execute mitigation and/or detection procedures.
- Prevent exploitation from occurring by identifying threats early.

For guidance on how to properly use Decider, see CISA's Decider Fact Sheet, video, and blog. CISA encourages analysts and incident responders to use the tool in conjunction with the recently updated Best Practices for MITRE ATT&CK® Mapping guide.

Note: This factsheet provides examples of tools for informational purposes only. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services does not constitute or imply their endorsement, recommendation, or favoring by CISA.

JAPAN COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER (JPCERT/CC)

Memory Forensic on Cloud

Memory Forensic on Cloud, developed by JPCERT/CC, is a tool for building a memory forensic environment on Amazon Web Services (AWS). This tool enables Windows operating system memory image analysis on AWS using Volatility 3.

Fileless malware is currently a popular attack vector. Analysts often must examine Windows memory images during incident response engagements, usually requiring machines with high specifications along with the time and resources to prepare sufficient analysis environment in a timely manner. This tool helps setting up a memory image analysis environment on AWS, which can also be expanded depending on need.

ACKNOWLEDGEMENTS

CISA would like to thank the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) for their contributions to this advisory.

RESOURCES

- CISA's Cloud Security Technical Reference Architecture Version 2
- CISA's Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)
- CISA's Secure Cloud Business Applications (SCuBA) Hybrid Identity Solutions Architecture
    - Security Guidance for 5G Cloud Infrastructures: Prevent and Detect Lateral Movement (Part I)
    - Security Guidance for 5G Cloud Infrastructures: Securely Isolate Network Resources (Part II)
    - Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services.
- See CISA's Trusted Internet Connections 3.0 Cloud Use Case for information on how network and multi-boundary security should be applied in cloud environments. TIC, originally established in 2007, is a federal cybersecurity initiative intended to enhance network and boundary security across the Federal Government. Although tailored to FCEB organizations, non-federal organizations may derive value from the documents as programs, strategies, and approaches are being considered to address multi-boundary or perimeter security needs.

CSA-published products about cloud:

- Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- Security Guidance for 5G Cloud Infrastructures: Prevent and Detect Lateral Movement (Part I)
- Security Guidance for 5G Cloud Infrastructures: Securely Isolate Network Resources (Part II)
- Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services