BSides Munich 2025

Cloud Incident Response

A Rapid Guide for Amazon Web Services Microsoft Azure & Google Cloud Platform

Erblind Morina - IBM X-Force

Agenda

- Intro
- Threat Landscape
- About Logging Problems
- Cloud IR Cheat Sheet
- AWSACS – Cloud IR Preparedness
- Q&A

$whoami

IBM X-Force Principal Incident Response Consultant
EMEA Cloud Incident Response Lead

- 7+ years of experience in Security Operations with a focus on Incident Response and Threat Intelligence.
- Extensive experience in the banking sector, having served as an Incident Responder, Detection Engineer, and SOC Manager within a global Security Operations Center.
- Successfully handled multiple high-impact security incidents, including APT-level investigations.
- Led efforts in building IR capabilities, developing TI platforms, and delivering technical training.

- Certifications
  - GIAC Cyber Threat Intelligence (GCTI)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Cloud Forensics Responder (GCFR)

- Education
  - Bachelor’s Degree in Security Studies
  - Master in Cybersecurity
  - Chevening Fellow – UK Defence Academy

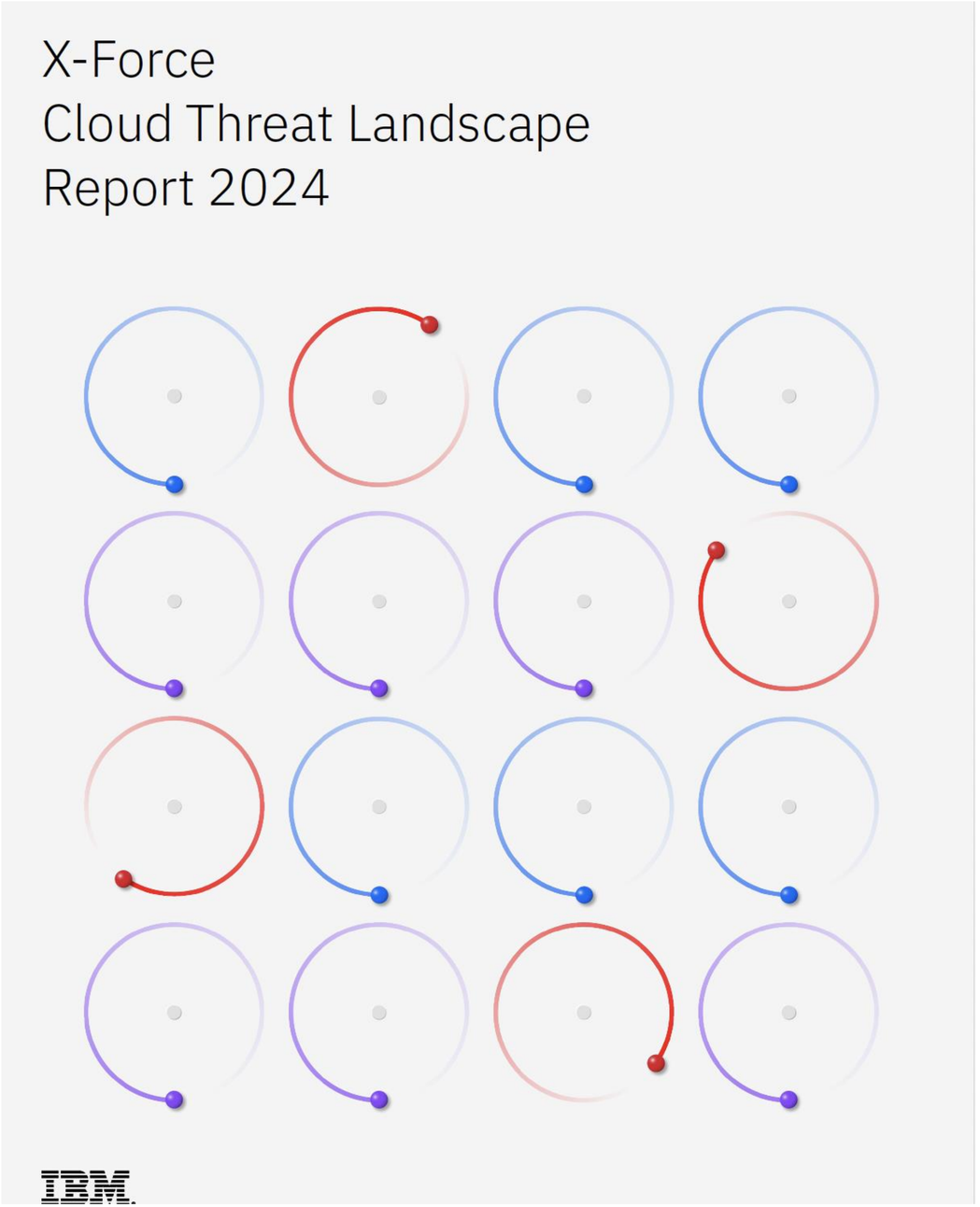
Cloud Threat Landscape

- 5th annual report
- Aid clients and the broader community with their cloud security strategy

To produce this report, X-Force reviewed data compiled between June 2022 through June 2024 and gleaned from the following sources:

- IBM X-Force Threat Intelligence
- IBM X-Force Red engagements (pen testing, adversary simulation)
- IBM X-Force incident response (IR) engagements
- Red Hat Insights
- Dark web analysis by IBM X-Force and data provided by report contributor Cybersixgill.

Our findings reveal the various ways we've observed threat actors compromising cloud environments and what types of malicious activity are pursued once they're inside.



Key Findings

Phishing and exploitation of vulnerabilities are top initial access vectors for attackers. Top CVE impacts include cross-site scripting, obtaining information, and gaining access

Phishing accounted for 33% of all cloud-related incidents X-Force responded to over the past 2 years, with attackers often using phishing to harvest credentials.

Exploitation of legitimate credentials was the second most common initial access vector - with the cost of credentials going down.

X-Force observed a steady decrease in the average price per cloud access credentials on the dark web from USD 11.74 in 2022 to USD 10.68 in 2023 and USD 10.23 in 2024

Percentage of cloud-related incidents involving the use of legitimate credentials to get into victim environments.

The most common action on objective is business email compromise.

Business email compromise activities accounted for 39% of IR engagements over the last 2 years.

More specifically, threat actors are frequently leveraging Adversary-In-The-Middle (AITM) phishing tactics to bypass user multi-factor authentication (MFA).

Increased use of trusted cloud-based file hosting services for malicious activities

Threat actors are increasingly leveraging trusted cloud-based services, such as Dropbox, OneDrive and Google Drive, for command-and-control communications and malware distribution.

Recommendations

Conduct comprehensive preparation and testing

A proactive, holistic security approach is paramount in the cloud landscape.

Integrate security throughout development through secure DevOps, threat modeling and rigorous testing to build resilience.

Automation minimizes human error and helps ensure continuous compliance, enabling organizations to navigate evolving threats with confidence.

Build a stronger identity security posture

A streamlined identity management strategy is no longer a luxury, but a necessity.

Simplify identity policies to strike a balance between robust security and user-friendly experiences.

Embrace modern authentication methods, such as MFA, and explore passwordless options, such as a QR code or FIDO2 authentication, to fortify defenses against unauthorized access.

Strengthen incident response capabilities

A swift and effective incident response can make all the difference. Leverage security threat intelligence to understand attacker motivations and respond more rapidly.

During investigations, preserving forensic evidence by redeploying affected machines, rather than reimaging them, helps ensure critical data is retained.

Regular testing of disaster recovery and backup procedures is also essential for business continuity and resilience.

Design secure AI strategies to stay ahead of cloud threats

Organizations must proactively manage risks associated with shadow AI and unsanctioned use of AI tools in the workplace, helping ensure transparency and control over AI initiatives. Additionally, organizations should prepare for the potential impact quantum-enabled threats could have on the long-term security of AI projects.

Why the Cloud Is Insecure by Default

Ease of Adoption Over Security

Cloud providers design services for fast onboarding and usability, as they want users to adopt their platforms easily. Default configurations often prioritize convenience, not protection.

Usability vs. Security

Providers tend to optimize for usability and scalability rather than strict security controls. This leads to systems that are functionally ready but not securely hardened.

Defaults = Open and Accessible

Many services start with public endpoints, open ports, or broad IAM permissions.

Security features (encryption, logging, network restrictions) are often **off by default** and must be manually enabled.

Shared Responsibility Confusion

The shared responsibility model is frequently misunderstood. Users assume providers handle more security than they do.

Misconfigured storage buckets, weak IAM policies, and unmonitored assets are common results.

Default Logging Problem and Visibility during IR

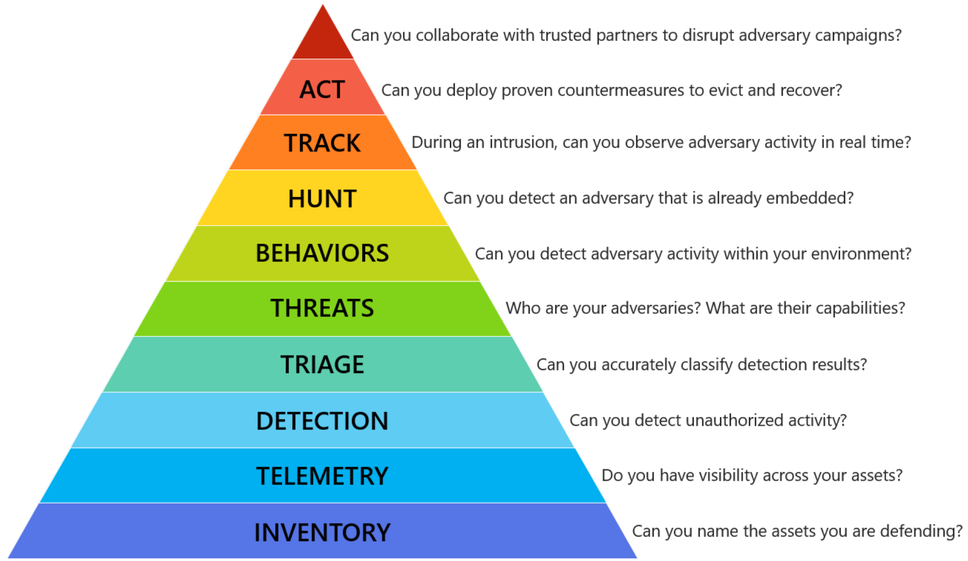
Lack of Logging = Limited Evidence

Investigators lose context, making it difficult to determine what happened, when, and who was involved.

Vertical visibility vs **Horizontal visibility**

- Real-time remediation depends on visibility + context
  - missing logs delay containment and increase potential damage.
- Enable baseline logging by default and centralize log collection.
- Define retention and monitoring policies to ensure both proactive detection and efficient post-incident investigation.

Incident Response Hierarchy of Needs:
https://github.com/swannman/ircapabilities



Cloud IR Cheat Sheet

Amazon Web Services Cloud Incident Response Cheat Sheet

The following table outlines key logs by category and highlights which are most critical during an IR. While services like CloudTrail and CloudWatch can capture a wide scope of activity, in less mature environments, logging might not be fully enabled by default - this can limit visibility during an investigation.

For example, if ELB is used the source IP address of an attacker is only visible in ELB logs and are not enabled by default. For more info about techniques used by threat actors check Threat Technique Catalog for AWS.

In case the client don't have logs enabled, Assisted Log Enabler help to find AWS resources that are not logging, and turn them on.

Category	Logs	Scenarios and related TTPs
Management Plane (On by Default) All actions via API in Console (GUI) or CLI go through management plane and are logged by CloudTrail, including read and write operations. Note: *Unlike Azure, AWS logs both management and read activities by default.*	• CloudTrail – *Tenant audit logs* • CloudTrail Insights – *API usage outside of baseline* • GuardDuty – *Anomaly detection* • CloudWatch Logs – *Forwarded logs from applications and endpoints*	• T1078 - Valid Accounts • T1078.A002 - Account Root User • T1078.A001 - IAM Users • T1087.004 - Cloud Account • T1531 - Account Access Removal • T1562.008 - Disable Cloud Logs • T1562.A001 - Disable or Modify GuardDuty
Network VPC Flow Logs capture network traffic for detecting suspicious communication and lateral movement.	• VPC flow logs – *NetFlow logs* • VPC Traffic Mirroring – *PCAP files* • Route 53 – *DNS Resolver Logs* • Load Balancer Logs	• T1190.A016 - EC2 Hosted App Compromise • T1491.A001 - Subdomain Takeover
Compute EC2, Lambda, ECS logs (via CloudWatch) help track system and app events during incidents.	• AWS Config - *Tracks resource changes* • CloudWatch Logs agent - *Collects system/app logs* • GuardDuty – *Anomaly detection*	• T1496.A008 – EC2 Hijacking • T1552.005 - Cloud Instance Metadata API • T1578.001 - Create Snapshot
Application Cloud-hosted web apps such IIS, Apache, also ELB, API Gateway, CloudFront access logs requests, client IPs, and request details.	• CloudWatch Logs - *Web app logs* • Load Balancer Logs - *Proxied web requests*	• T1562.008 - Invoking Lambda • T1496.A006 – EC2 Hijacking
Data S3 access logs track data reads and writes for detecting data breaches.	• CloudTrail Data Events • S3 Server Access Logs	• T1530.A001 - S3 Object Collection • T1619.A001 - S3 Object and Bucket Enumeration • T1485.A003 - S3 Object and Bucket Deletion
Cloud Security Services GuardDuty, Security Hub, Inspector generate alerts and findings are very helpful in threat detection and IR.	• GuardDuty • Amazon Inspector • AWS Config	• T1562.A001 - Disable or Modify GuardDuty • T1562.008 - Disable Cloud Logs

Microsoft Azure Cloud Incident Response Cheat Sheet

The following table outlines key logs by category and highlights which are most critical during an IR. While services like Azure Activity Logs can capture a wide scope of activity, in less mature environments, logging might not be fully enabled by default—this can significantly limit visibility during an investigation.

The Azure Threat Matrix is a very helpful resource for mapping detections to MITRE ATT&CK techniques, helping prioritize relevant logs during IR and to identify malicious activity.

Category	Types of Logs	Scenarios and related TTPs
Management Plane (On by Default) All actions via Azure Portal (GUI), CLI, or API go through the management plane and are logged by Azure Activity Logs. Note: *Unlike AWS, Azure does not log read activities by default.*	• Signin logs – *Entra ID* • Managed-identity signin logs • Non-interactive user signin logs • Service principal signin logs • Auditlogs - *App registration, service principal changes* • Activity Logs - *Tracks API calls*	• AZT202 - Password Spraying • AZT203 - Malicious Application Consent • AZT502 - Account Creation • AZT704 - Soft-Delete Recovery • AZT501 - Account Manipulation
Network NSG Flow Logs capture network traffic, DNS, Load Balancer logs which can help to detect suspicious communication.	• NGS flow logs – *NetFlow logs* • Azure Packet Capture – *PCAP files* • Traffic Analytics • Azure DNS Logs – *DNS Resolver Logs* • Load Balancer Logs/Azure Front	• AZT101 - Port Mapping • AZT102 - IP Discovery • AZT301 - Virtual Machine Scripting • AZT503.3 - Runbook Webhook
Compute Logs from Azure Virtual Machines (VMs) or Azure Functions (via Azure Monitor or Log Analytics) help get system/security logs.	• Azure Monitor Agent - *Logs from VMs* • WAD Logs - *system-level events* • LinuxSyslogVer2v0 – *for Linux* • Azure Functions Logs • Container Insights - *AKS and containers logs*	• AZT301 - Virtual Machine Scripting • AZT301.1 – RunCommand • AZT701.1 - VM Disk SAS URI
Application Logs from cloud-hosted web apps such as IIS, Apache, or Azure App Services, as well as logs from Application Gateway, Azure Front Door, and Azure Load Balancer.	• Application Insights - *Tracks web app performance and logs* • Azure Application Gateway Logs - *Tracks web traffic routing*	• AZT105 - Gather Application Information • AZT203 - Malicious Application Consent • AZT405 - Azure AD Application
Data Azure Storage Account Logs including read/write operations to detect potential data breaches.	• Azure Storage Account Logs • Azure Blob Storage Access Logs • Storager Read	• AZT701 - SAS URI Generation • AZT701.2 - Storage Account File Share SAS
Cloud Security Services Microsoft Defender for Cloud, Azure Security Center, and Azure Policy generate alerts and findings are very helpful in threat detection and IR.	• Microsoft Defender for Cloud • Log Analytics • Azure Policy - *Tracks compliance and resource changes*	

Google Cloud Platform Cloud Incident Response Cheat Sheet

The following table outlines key logs by category and highlights which are most critical during an IR. While services like Cloud Logging can capture a wide scope of activity, in less mature environments, logging might not be fully enabled by default—this can significantly limit visibility during an investigation.

Category	Logs	Scenarios and related TTPs
Management Plane (On by Default) All actions via the Google Cloud Console (GUI), CLI, or API go through the management plane and are logged by Cloud Audit Logs. 'Policy denied' bucket logs access attempts denied by IAM policies.	• Admin Activity Logs - *Tracks administrative actions* • System Event Logs - *Logs of VM and system changes* • Enterprise Group Audit Logs - *Tracks Google Workspace group activity* • Login Audit Logs - *authentication* • Platform Audit Logs	• T1078 - Valid Accounts • T1531 - Account Access Removal • T1189 - Drive-by Compromise • T1136 - Create Account • T1110 - Brute Force
Network VPC Flow Logs capture network traffic, helping detect suspicious communication and lateral movement within VPC. Note: *GCP does not cover 100% of traffic; they focus only on sampling.*	• VPC Flow Logs - Captures network traffic for analysis • Packet Mirroring - *Captures full packet data (PCAP equivalent)* • VPC Firewall • Cloud Load Balancer Logs	• T1190 - Exploit Public-Facing Application
Compute Logs from Compute Engine VMs, Cloud Functions, and Google Kubernetes Engine (GKE) (via Cloud Logging) help track system and application events during incidents.	• Logging Agent - *Host VM logs* • Cloud Functions Logs - *Logs for serverless functions*	• T1496.A008 - Compute Hijacking - EC2 Use • T1552.005 - Cloud Instance Metadata API • T1578.001 - Create Snapshot
Application Logs from cloud-hosted web apps such as Apache, Nginx, or apps deployed on App Engine, as well as logs from Cloud Load Balancer, API Gateway, and Cloud CDN.	• Cloud Load Balancer Logs • API Gateway Logs: *Logs API traffic and requests*	• T1648: Abuse of Cloud Functions • T1496: Resource Hijacking
Data Azure Storage Account Logs track data read/write operations to detect potential data breaches.	• Storage Bucket Logs - *Web access to Storage Bucket*	• T1530 - Cloud Object Storage Discovery • T1619 - Cloud Storage Bucket Enumeration • T1485 - Data Destruction
Cloud Services Security Command Center, Cloud Logging, and Cloud Monitoring generate alerts and findings that are very helpful for threat detection and incident response.	• Security Command Centre • Cloud Monitoring - *Tracks resource performance and alerts on anomalies*	• T1562.008 - Disable Cloud Logs • T1556.005 - Cloud Credential Dumping • T1070.004 - Indicator Removal on Host: Cloud Logs

AWSACS – Cloud IR Preparedness

AWSACS – Cloud IR Preparedness

AWSACS checks AWS for **visibility** and **logging coverage**. It **reports gaps** that may hinder IR investigations or evidence collection.

Outputs

- Console: Real-time
- CSV: Detailed matrix saved to output/aws_logging_matrix.csv

Services Checked

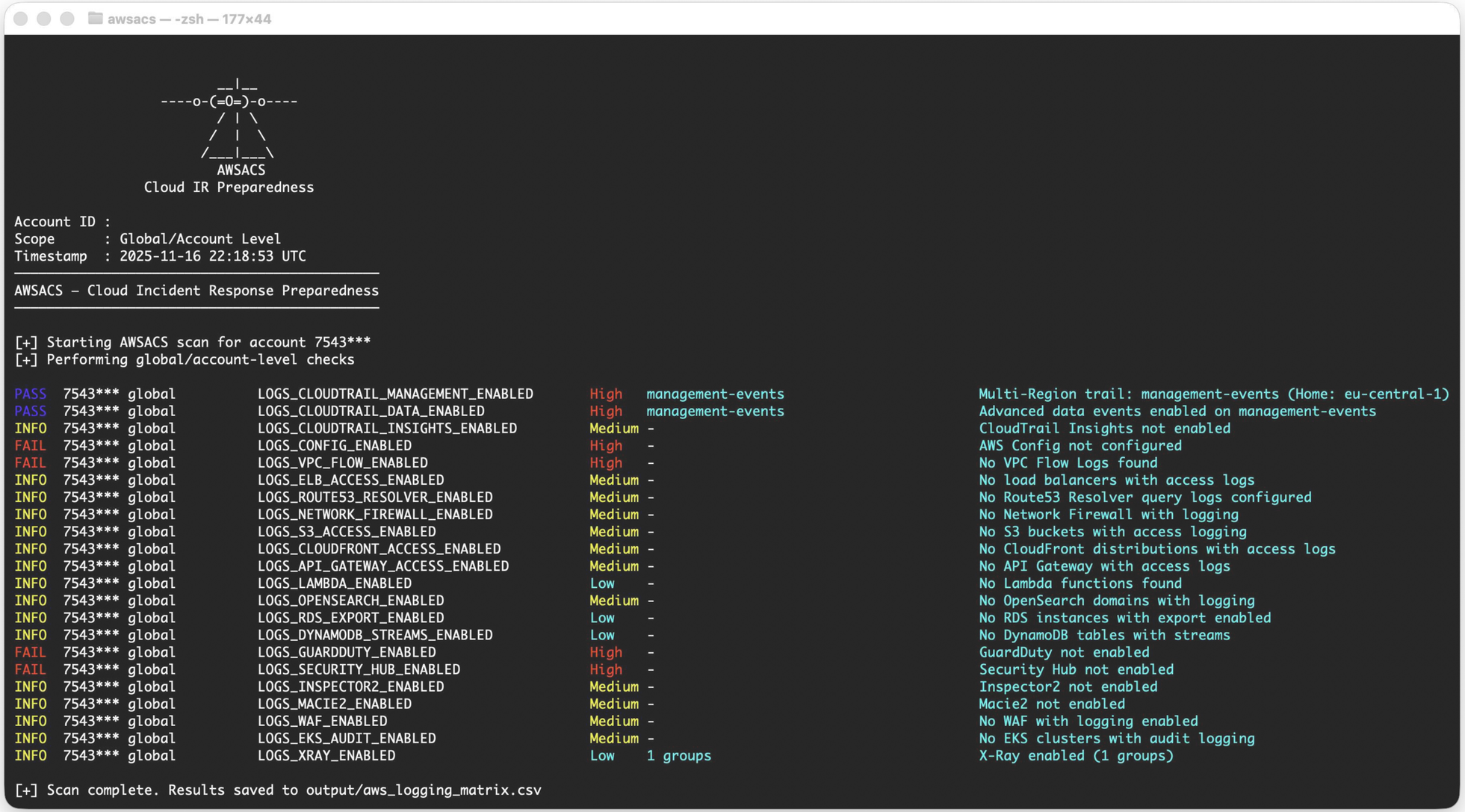
- CloudTrail (Management, Data Events, Insights)
- AWS Config
- VPC Flow Logs
- ELB/ALB Access Logs

Services Checked (Cont.)

- Route53 Resolver Query Logs
- Network Firewall Logs
- S3 Access Logs
- CloudFront Access Logs
- API Gateway Access Logs
- Lambda Logs
- OpenSearch Logs
- RDS Export Logs
- DynamoDB Streams
- GuardDuty
- Security Hub
- Inspector2
- Macie2
- WAF Logs
- EKS Audit Logs

GitHub:
https://github.com/erblind1/cloud-ir

AWSACS – Cloud IR Preparedness



Resources

Cloud Incident Response Cheat Sheet + AWSACS

Download cheat sheet for key logs and techniques for AWS, Azure, and GCP incident response.

Link: github.com/erblind1/cloud-ir

Cloud Threat Landscape Report

Read the detailed report for a deep-dive into the findings and recommendations for cloud.

Link: ibm.com/cloudthreats

MITRE ATT&CK® Cloud Matrix

Read about tactics and techniques representing by MITRE ATT&CK® for cloud platforms

Link: attack.mitre.org/cloud/

FOR509: Enterprise Cloud Forensics and Incident Response

Learn about Cloud forensics which covers major providers (Microsoft Azure, Amazon AWS and Google Cloud)

Link: sans.org/509

Threat Technique Catalog for AWS

Read about tactics and techniques representing by AWS

Link: github.io/threat-technique-catalog-for-aws

Relevant resources

SANS FOR509 GitHub
Azure Threat Research Matrix
Google Cloud Platform (GCP) to MITRE ATT&CK

Thank you.