CyberProof®
A UST Company

The SecOps Guide to Multi-Cloud Environments

Optimizing multi-cloud infrastructures by leveraging GenAI capabilities

cyberproof.com

Table Of Contents

About this report

As more organizations move their infrastructure and IT services to the cloud, it is common to adopt services from more than one cloud platform provider, such as Microsoft Azure, Google Chronicle and Amazon AWS. This provides much more flexibility than working with only one cloud platform, allows organizations to better manage costs and avoid vendor lock in, and improves resiliency. Research shows that over 90% of large organizations already use a multi-cloud model, meaning they rely on apps and infrastructure from multiple cloud providers.

However, this opens up new attack surfaces and cyber risks requiring security operations teams to adapt their practices to those required for detecting and responding to security threats in their cloud environments.

This report aims to guide security teams in how to best apply threat detection and response to multi-cloud environments.

Gaining visibility

The proliferation of DevOps and increasing control at the employee level means new cloud applications are being created all the time, whether sanctioned or unsanctioned by corporate IT. This challenge is referred to as Shadow IT, covering anything from enterprise SaaS services to cloud storage or collaboration suites.

Shadow IT is not a new topic. In fact, most organizations think they have this issue under control. However, they are often surprised at the thousands of SaaS applications being used that were previously unknown. According to Gartner, 41% of employees acquired, modified, or created technology outside of IT's visibility in 2022. Gartner expects that number to climb to 75% by 2027. If your employee is working from home or on their own personal device, you must approach security differently than the traditional approaches of endpoint software or firewalls.

Security teams must be able to gain visibility into such applications to maintain robust defenses while assessing whether they're configured according to security best practices. Cloud Access Security Broker (CASB) solutions provide visibility into both sanctioned and unsanctioned cloud services.

These solutions enable you to discover what cloud applications are being used to identify risks and compliance status, set policies, and provide continuous visibility of threats. CASB solutions enable you to carry out three main functions:

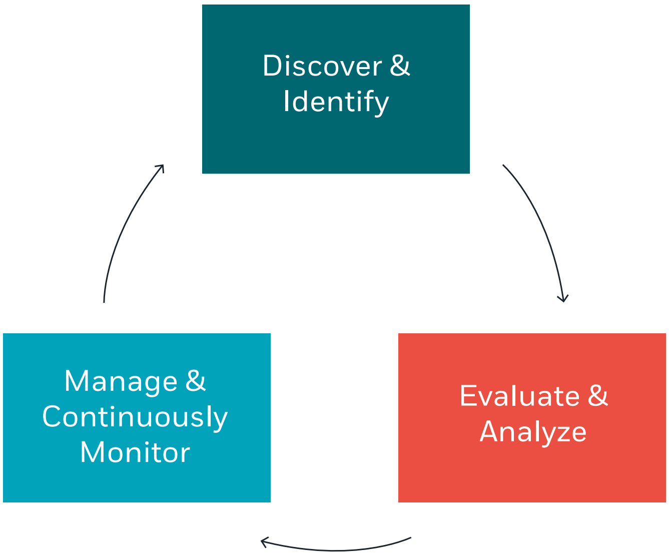
Discover & identify – Identifying the cloud applications used by your organization, as well as understanding any associated risks.

Evaluate & Analyze – Creating tailored reporting to evaluate whether cloud services are compliant against standards such as GDPR, HIPAA, COBIT, ISO27001. Questions you should be seeking to answer include:

- Who is accessing our cloud services?
- What files are being shared publicly?
- What activity is happening in this cloud service right now?
- Are there any connected third-party apps to my environment?
- What cloud services are being used?

Manage & Continuously Monitor – Focusing on governance and monitoring for threats. Governance can include activities such as reviewing policy violations and managing the usage of your cloud services by taking appropriate action, such as blocking access to unsanctioned apps when connected to Microsoft Defender for Endpoint. Security teams need to be able to monitor threat actor activity as well as governance, which is why detections and alerts should be configured in line with the MITRE ATT&CK framework.

Microsoft Defender for Cloud Apps is a CASB solution that provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all Microsoft and third-party cloud services. It supports various deployment modes including log collection, API connectors, and reverse proxy. This solution can also be integrated with Microsoft Sentinel to enable centralized monitoring of alerts and SIEM discovery data. You can run Snapshot reports, which provide ad-hoc visibility on a specific set of traffic logs, or continuous reports, which automatically forward all logs and identify anomalous use.



Sample Use Cases

Detecting and remediating malware in cloud apps

Challenge

Attackers can take advantage of an unknown vulnerability in software or operating systems by creating malware that's purpose-built to exploit and attack critical systems.

Solution

CASB solutions can detect malicious zero-day exploit behavior by running suspicious files through a sandbox, allowing security teams to quickly react. You can also leverage session controls to prevent the upload and infiltration of known malware in real time across all of your apps.

Detecting threats from privileged accounts

Challenge

Attackers try to take over privileged accounts that have the keys to critical assets and systems by using techniques such as phishing, password spray, and breach replay.

Solution

CASB solutions alert you to various activities indicating that a privileged account may have been compromised. Relevant alerts include privilege escalation, mass impersonation by a single user, and login from a new country with an admin account.

Multi-cloud infrastructure

Migrating from on-premises to cloud infrastructure environments requires organizations to take more responsibility for security processes that cloud providers previously operated within SaaS environments. Monitoring the security posture of your Infrastructure as a Service (IaaS) environments means having effective processes and controls for collecting and analyzing data from various cloud workloads across hybrid and multi-cloud environments, including:

- Server Virtual Machines
- Containers
- SQL/Storage
- Network
- Internet of Things (IoT)

Using a technology solution that combines Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) like Defender for Cloud can help you to assess weaknesses in your cloud resources running across Azure, AWS, and GCP. You can also configure Defender for Cloud to provide you with alerts about suspicious activities and vulnerabilities across workloads running in those environments such as Virtual Machines, containers, storage, and app services, depending on your plans. For example, you can enable Defender for Containers to provide an alert in response to hardening recommendations.

Sample Use Cases

Identifying misconfigurations in cloud infrastructure

Challenge

Misconfigurations in cloud infrastructure can lead to the exposure of data to cyber attackers, which consequently results in loss of customer trust and legal liability.

Solution

A CSPM can compare your cloud configurations against industry standards and discover misconfigurations in real time. By aggregating all scan results and providing a risk score, CSPM tools enable you to prioritize remediation.

Detecting vulnerabilities that an attacker could exploit

Challenge

Organizations are responsible for securing the workloads they run in the cloud, be it Virtual Machines, containers, or applications. But due to the elasticity of cloud-native technology, workloads such as containers can come and go as they are needed, making it incredibly difficult to monitor for threats and vulnerabilities.

Solution

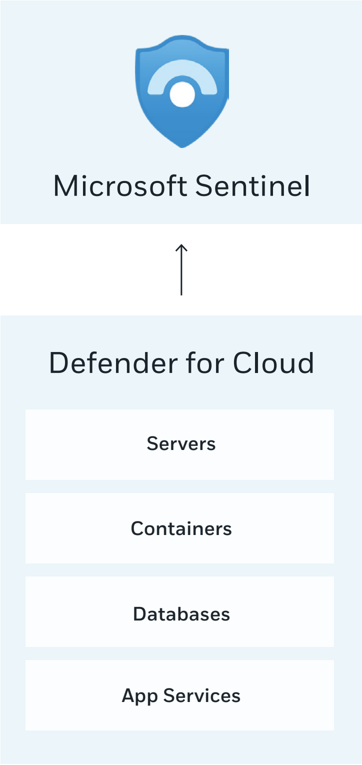
Cloud Workload Protection Platform (CWPP) solutions provide visibility into malicious activity across continuous integration/continuous delivery (CI/CD) workflows. The solution can perform a vulnerability assessment to identify any potentially exploitable security issues with the workload based on defined security policies and known vulnerabilities while recommending timely security controls or remediation actions.

Connecting to your cloud SIEM

A single pane of glass

To maintain an efficient security monitoring infrastructure, you should have a single view of all cloud security activity, to the extent possible. A cloud-native SIEM can be used to aggregate and prioritize alerts from multiple cloud sources.

It's important to configure the detection of both the cloud applications (SaaS) and infrastructure (IaaS). This requires implementing agents on specific cloud resources across these planes. Microsoft Defender offers a suite of integrated security solutions that deploy agents across these areas and acts as a source for generating alerts in Microsoft Sentinel.



Leveraging machine learning

Sentinel is a cloud-native SIEM that provides security data correlation, advanced analysis, and hunting of large volumes of events from hybrid environments to obtain high-context alerts.

Sentinel uses machine learning (ML) to proactively find anomalies hidden within acceptable user behavior and generate alerts. It natively incorporates other foundational Azure services such as Azure Logic Apps to help build playbooks and connectors, enabling you to automate workflows and integrate with third-party services.

Sentinel log ingestion methodologies

Azure monitoring agent

Azure Monitor Agents (AMA) collect monitoring data from the guest operating systems of Azure and hybrid virtual machines and deliver them to Azure Monitor for use by features, insights, and other services, such as Microsoft Sentinel and Microsoft Defender for Cloud.

Sentinel native connector and API

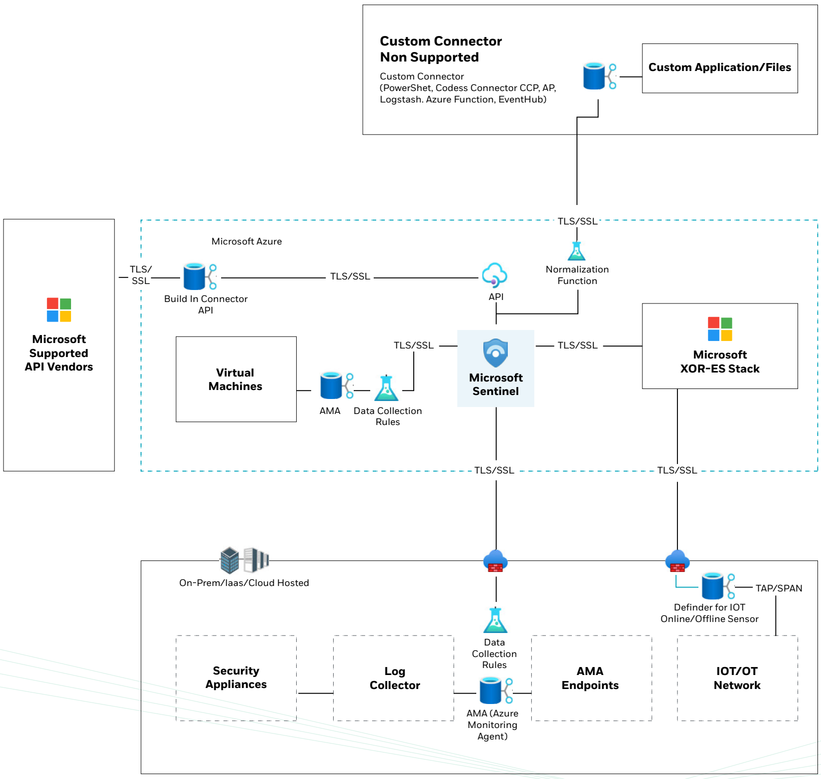
Native connectors work at the click of a button with most of the Azure Products like Microsoft Defender, Defender for Identity, etc. Many security technologies provide a set of APIs for retrieving log files, and some data sources can use those APIs to connect to Microsoft Sentinel. Data connectors that use APIs either integrate from the provider side or integrate using Azure Functions.

Data collection rules (DCRs)

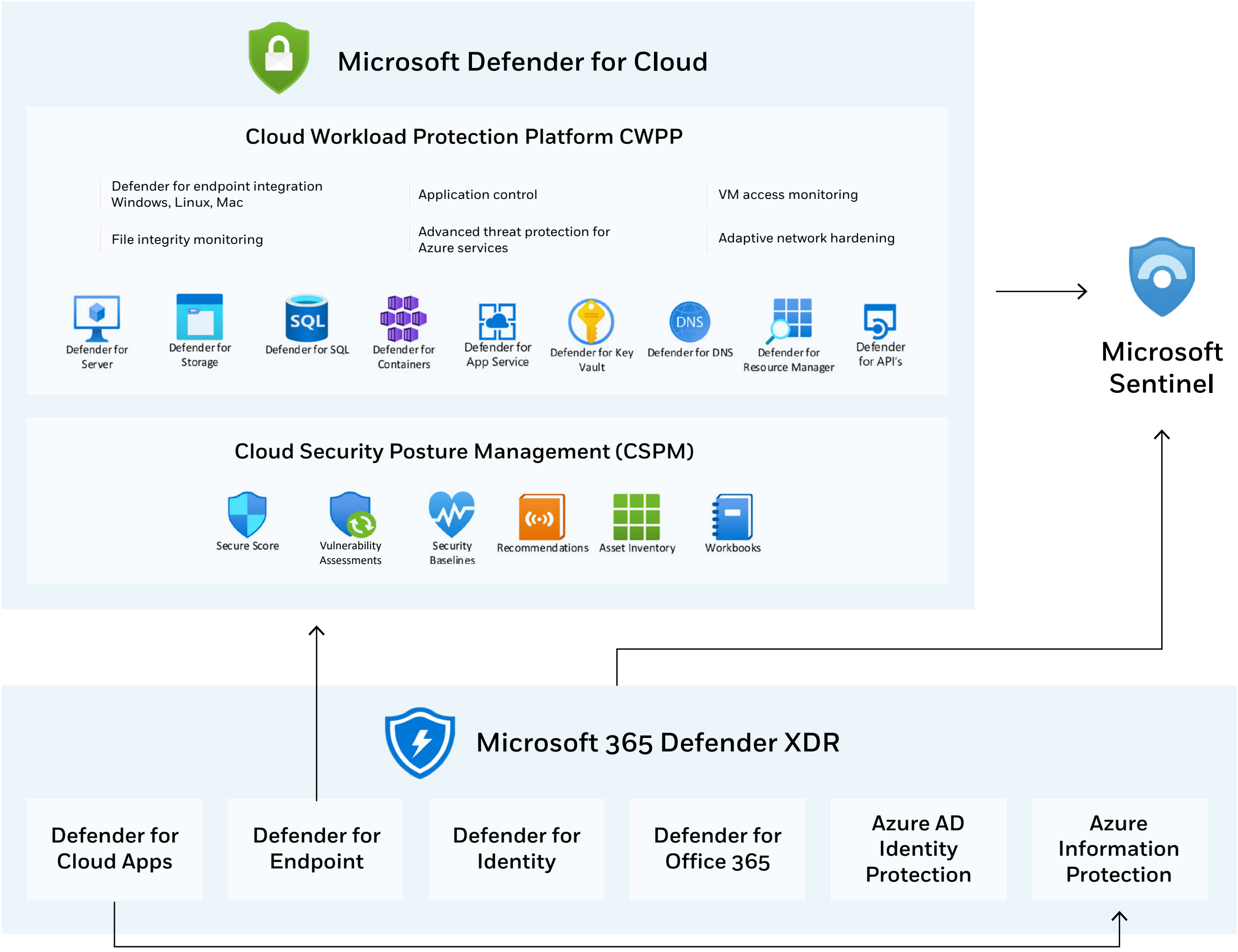
DCRs define the data collection process in Azure Monitoring Agent. They specify what data should be collected, how to transform that data, and where to send that data. Some DCRs are created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.

Custom connector

This is a combination of functionalities including PowerShell, Codeless Connector Platform (CCP) API, Logstash, and Azure Functions to configure the onboarding of custom log sources into Sentinel.



Sentinel log ingestion methodologies

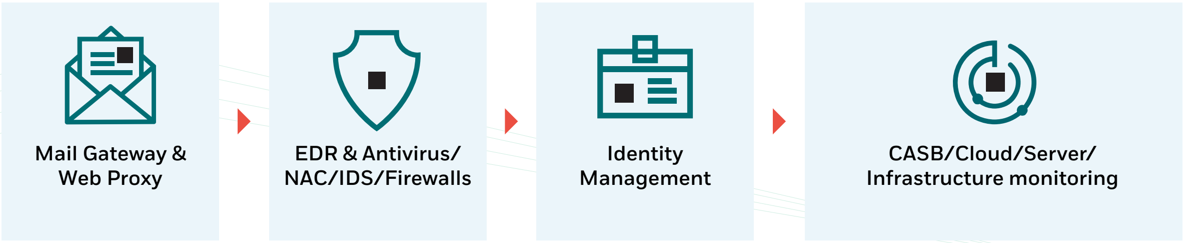

Microsoft Defender for Cloud
Cloud Workload Protection Platform CWPP
Defender for endpoint integration Windows, Linux, Mac
Application control
VM access monitoring
File integrity monitoring
Advanced threat protection for Azure services
Adaptive network hardening
Defender for Server
Defender for Storage
Defender for SQL
Defender for Containers
Defender for App Service
Defender for Key Vault
Defender for DNS
Defender for Resource Manager
Defender for API's
Cloud Security Posture Management (CSPM)
Secure Score
Vulnerability Assessments
Security Baselines
Recommendations
Asset Inventory
Workbooks
Microsoft Sentinel
Microsoft 365 Defender XDR
Defender for Cloud Apps
Defender for Endpoint
Defender for Identity
Defender for Office 365
Azure AD Identity Protection
Azure Information Protection

Defender for cloud and cloud apps in the cyber kill chain

With the E5 cloud-native security stack, CyberProof can support enterprises to optimize protection against potential attacks along the entire cybersecurity kill chain. Defender for Office 365 deals with potential malicious mail and browsing activity control macros of sent files.

Defender for Cloud, with Defender for Endpoint, protects virtual assets as well as on-prem. assets and should be correlated with Firewall and IPS logs to be even more efficient. Defender for Identity and Identity Protection should both be rolled out as much as possible, as they are key to detecting lateral movement and account compromise in on-prem. and cloud environments. They are a big enrichment source for Defender for Endpoint and Defender for Office 365.

Defender for Cloud Apps acts as a CASB solution, protecting - with Azure AD Identity Protection and Azure Information protection - potential exfiltration and tampering of data in the cloud.


Mail Gateway & Web Proxy
EDR & Antivirus/ NAC/IDS/Firewalls
Identity Management
CASB/Cloud/Server/ Infrastructure monitoring

Optimizing cost and complexity

Ingesting data from multiple cloud environments using a cloud-native security monitoring technology like Sentinel adds scalability, flexibility, and speed to monitoring efforts - but it can considerably ramp up the cost and complexity of data, too. When adopting a cloud-native approach, consider the following questions:

Should you collect all logs?

How can you normalize data as it is being ingested?

How can you ensure compliance with data residency requirements and regulations such as GDPR?

This aligns with a broader challenge in the security analytics/SIEM market in terms of maximizing the investment in this technology, to reduce alert fatigue and prioritize based on risk. To address these issues, organizations need to solve the data collection and processing layer – a foundational layer of security analytics that often goes unnoticed.

Understanding data collection architecture

Data collection architecture consists of three components:

- Collection
- Storage
- Classification

Collection

There are two types of collectors:

Native

These are built-in connectors supported by Sentinel which can bring in logs from third-party cloud sources such as AWS CloudTrail, Google Cloud Platform, Oracle Cloud Infrastructure, Cisco Umbrella, and others.

Non-native

These data sources are not supported by default by Microsoft Sentinel and require custom collectors that can parse and filter the data so it can be understood by the SIEM. Without finding a way to collect data from sources that aren't covered natively by Microsoft Sentinel, you are essentially leaving out blind spots that attackers can use to hide in your network undetected.

Non-native sources are not covered or supported, both for an enterprise organization that is about to migrate or in the future as new applications, services, and systems are adopted during your digital transformation. These new assets generate data and events in different formats that aren't supported and this inevitably slows down threat detection efforts.

Without finding a way to collect data from sources that aren't covered natively by Sentinel, you're essentially leaving out blind spots that attackers can use to hide in your network undetected.

Solving this involves developing a continuous process for collecting new formats of data through non-native collection methodologies. If you have data scientists on your team, we recommend leveraging their experience in coding and data engineering. Data scientists can leverage PowerShell scripts and tools such as LogStash to create custom parsers to filter unstructured data, identify relevant fields, and converge on a common format.

Storage

As you collect data from multiple cloud sources, it's important to have a scalable cloud data lake that can ingest and manage large volumes of structured, semi-structured, and unstructured data. Platforms such as Azure Data Explorer (ADX) provide this capability. Just as importantly, they share the same querying language as Sentinel, which means data being stored on ADX can be used for hunting activities across large datasets.

Classification

Classifying data as it is being ingested improves data security, compliance, and search capabilities. This is done by applying metadata tags to fields at the time of collection. The tags are used to determine who can access the data, how long it should be retained, and how it can most efficiently be retrieved through search queries and dashboards.

Leveraging the CyberProof Log Collector

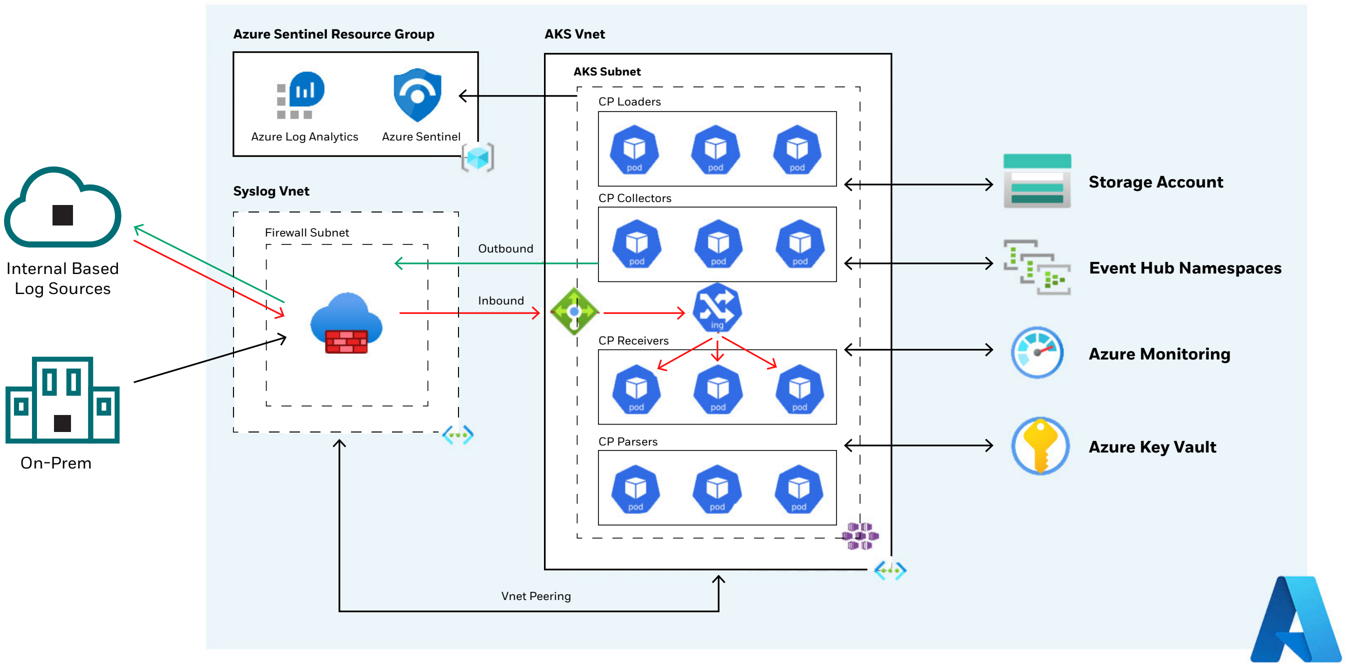
At CyberProof, we developed a tool based on a microservices architecture, which plays a key role in helping clients transition to multi-cloud security monitoring.

The CyberProof Log Collector (CLC) is purpose-built to collect all data types, from any source. It can take any log and handle the parsing, tagging, cleaning, and aggregation of the data before it is ingested into Sentinel.

The CLC works with all languages, so that it does not matter whether an integration is written in Python, PowerShell, .NET, or another programming language.

It improves the flow and handling of data, augmenting Sentinel's predefined rules and capabilities to provide customers with automated and dynamically updated threat detection. Costs are reduced by more than 50% due to the filtering of log data and routing of less relevant data into a cost-effective, cloud-native storage solution.

CyberProof Log Collection Topology



A DevOps approach to automation

Leveraging an Infrastructure as Code (IaC) model allows organizations to maintain the agility necessary to respond continuously to the changing threat landscape. IaC allows security content and infrastructure to be managed as code.

Similarly, in the development life cycle of a cloud application, security teams can use DevOps environments and Continuous Deployment/Continuous Improvement (CI/CD) pipelines to develop, test, deploy, and update content such as detection rules, playbooks, reports, automation rules, and hunting queries across multiple workspaces.

With Sentinel acting as the single security analytics platform for multi-cloud environments, Azure DevOps repositories can be leveraged to deploy infrastructure and content updates to monitor, detect, and respond to cloud threat activity.

Automating the infrastructure includes:

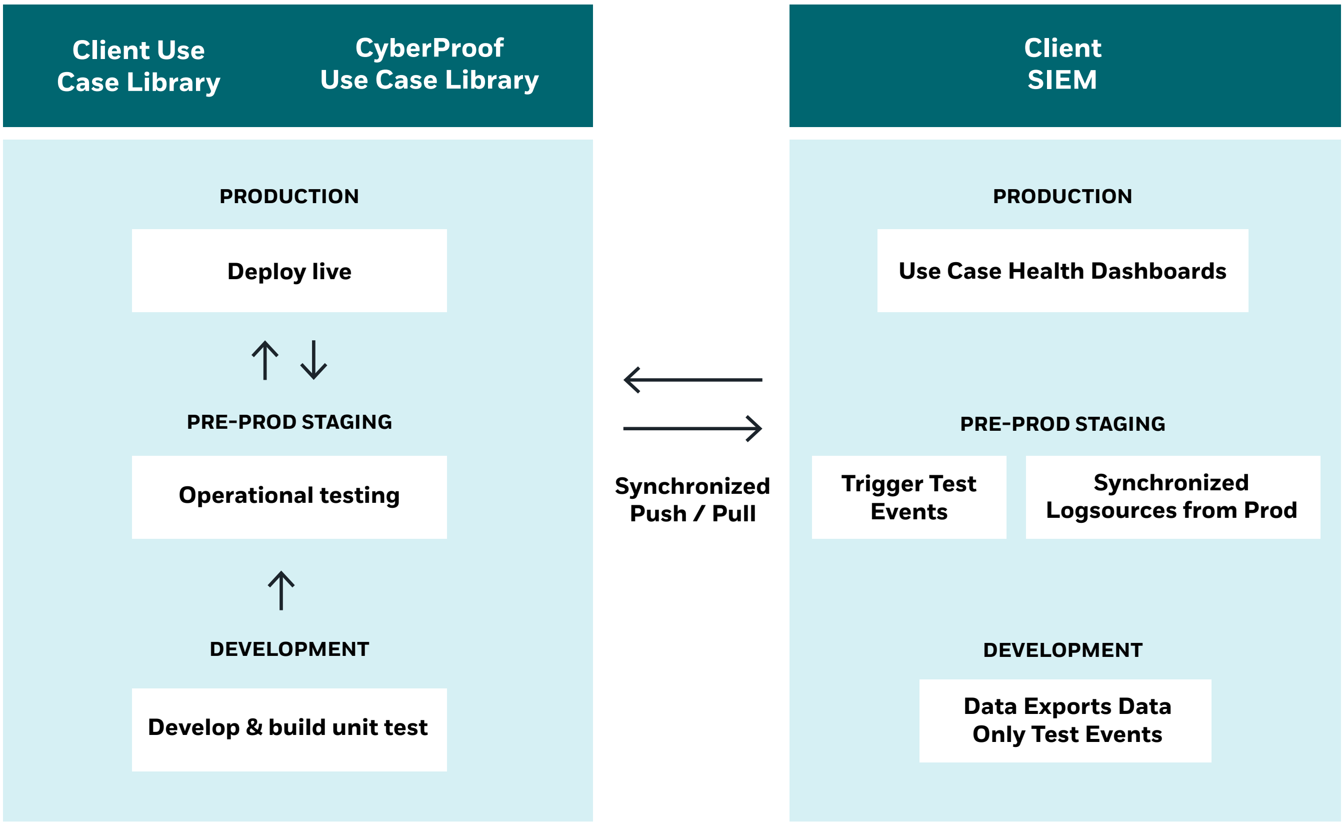
- **Resource groups –** A container that holds related resources for an Azure solution
- **Log analytics –** A service that helps you collect and analyze data generated by resources in your cloud and on-premises environments
- **Sentinel –** A cloud-native security analytics platform

Automating the content includes:

- **Hunting queries –** Helping you find suspicious activity in your environment
- **Alert rules –** Queries that trigger alerts when security incidents happen in your environment
- **Playbooks –** Using Azure Logic Apps to respond to incidents automatically. Logic Apps are a native resource in Azure
- **Workbooks –** Visualizing and monitoring the data and providing versatility in creating custom dashboards

The added benefit of using the IaC model is immutability – i.e., any time code for security content or infrastructure is changed or added, the change or addition is applied automatically to all Sentinel workspaces.

Needless to say, you need to have DevOps specialists that know how to manage this process. At CyberProof, our DevOps specialists use the IaC model for deploying Sentinel infrastructure and content as part of our Managed Detection and Response service.



An example of CyberProof's Use Case Management staging in a client environment

Benefits

- Fail-safe approval process
- Instant revert back
- Easy access for our clients
- Traceability of changes
- Automatic documentation
- False positive checks
- Coding guidelines to ensure quality
- Support portal for use case requests

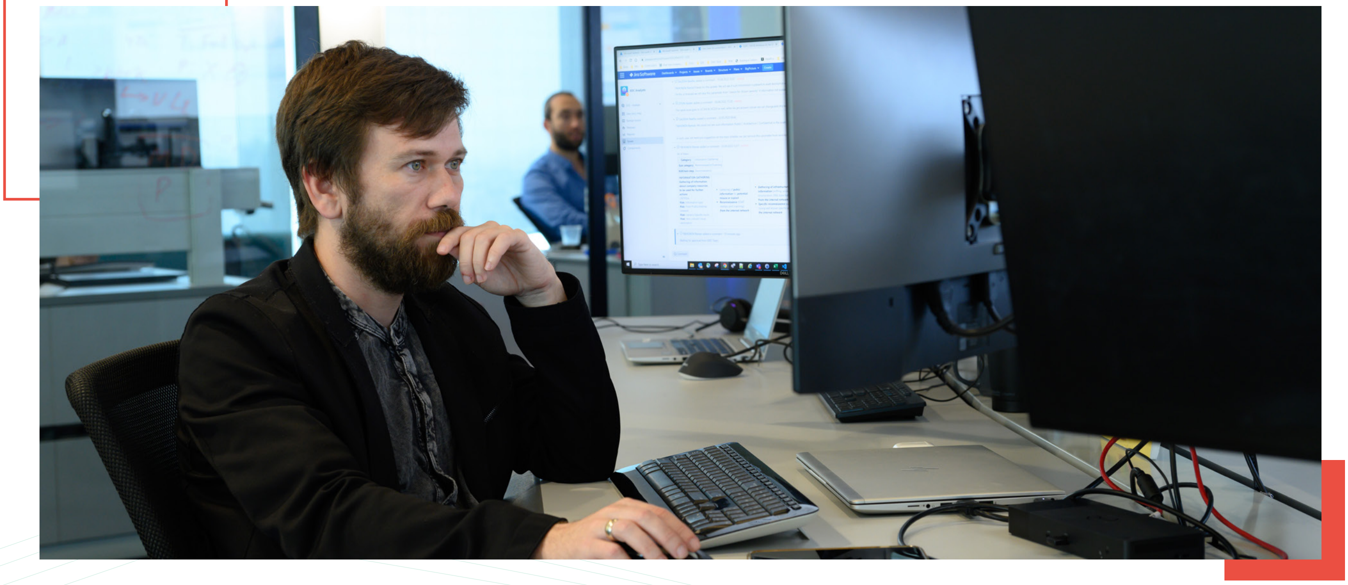
Use case management – handling threats proactively

You cannot detect a threat if you can't define it. Developing use cases is a way of defining not only which types of threats to monitor, but also how to respond to them. This is particularly important when onboarding new cloud sources that provide new attack surfaces. Use cases also help you evaluate which log sources from a legacy SIEM should be transitioned over to Sentinel.

To define a use case:

1. Identify the attack scenario you'd like to monitor. The most common example of an attack that exploits multi-cloud environments is driven by misconfigured cloud resources such as publicly-exposed databases or over-privileged users.
2. Identify which attacker techniques could be used to exploit these misconfigurations, for example:
   - Exfiltration of sensitive data from an AWS bucket
   - Modification of cloud compute infrastructure
3. Identify the right data sources for generating alerts. Conversely, if you were to start by monitoring all data sources without first defining the attacker scenario and techniques, you would be overloaded with events to monitor and with determining which were false positives.

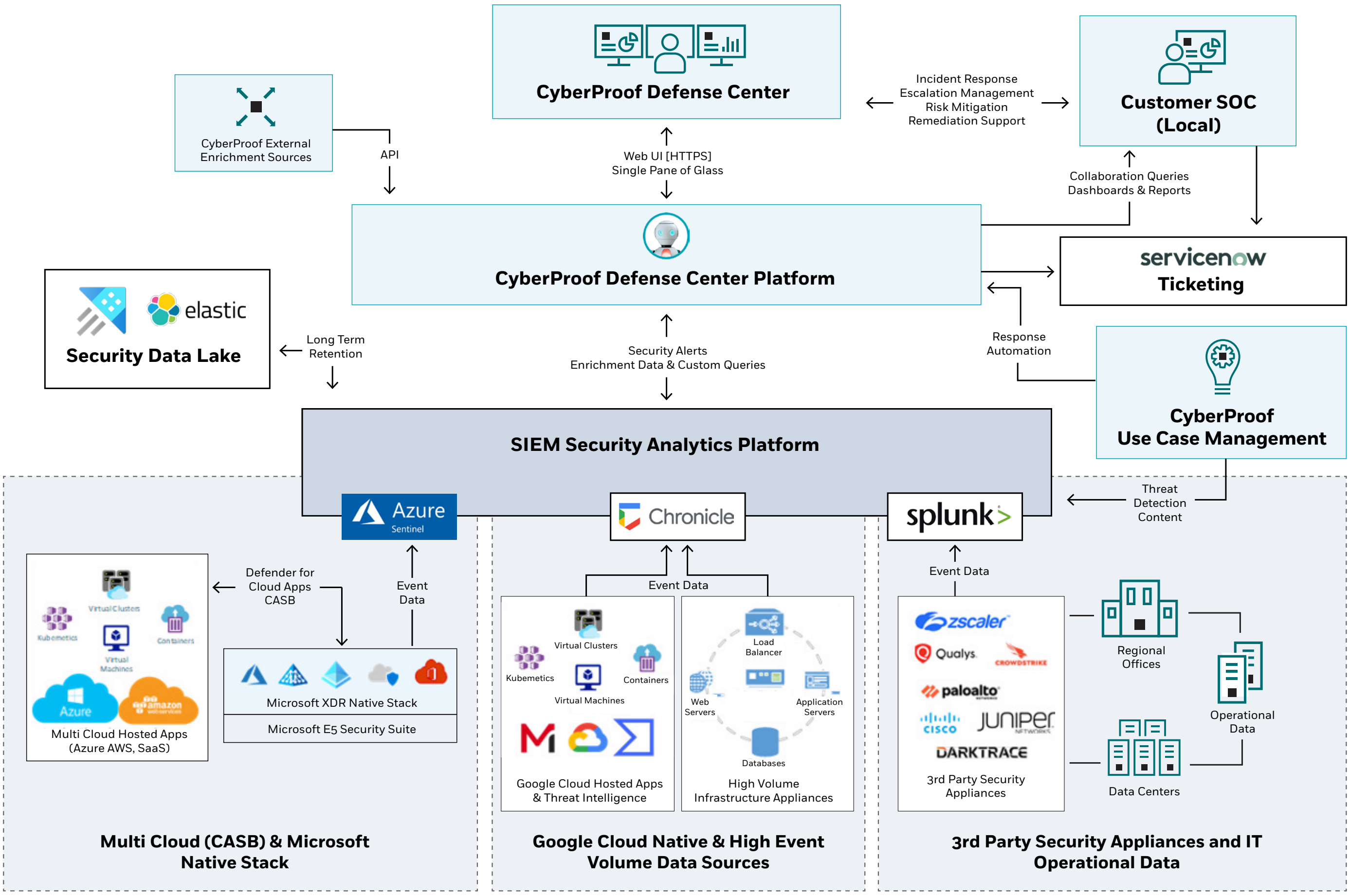
For example, assuming the technique "Modification of cloud compute infrastructure" is a likely attack vector for your enterprise, you could look at ingesting logs from AWS CloudTrail, Azure Monitor Log Data, and Google Admin Activity audit logs that indicate an attacker is creating a copy of an existing Virtual Machine (VM) to bypass defenses.



This information alone won't provide enough context to investigate the activity further. Hence, enriching this with other internal data such as user information or vulnerability intelligence, combined with threat intelligence, could reveal attack campaigns that conduct the same behavior and therefore help predict where the attack will move next within your estate. Ultimately, this can also help facilitate the right response to limit the spread of infection.

Supporting multi-cloud security operations

A seamless SOC operation requires a modern platform that provides holistic visibility.



Challenge

In the Cloud, security is a joint responsibility. Cloud providers (including AWS, Google, and Azure) produce huge amounts of event logs that need to be correlated with all cloud native and on-prem. applications. These provide a holistic picture of what is happening in the environment. Often the providers have their own proprietary security solutions including CASB, SIEM, and EDRs, and bringing everything into a single pane of glass is challenging.

Solution

There are advantages to using some of the integrated security solutions offered by cloud providers because they are stronger at understanding their individual data sets. In this example (see the diagram), an enterprise is using Multiple SIEMs.

- **Microsoft Sentinel:** Sentinel is strong at understanding the Microsoft Azure Cloud data set and brings a strong CASB solution to monitor multi-cloud environments (including Azure, AWS, and SaaS applications).
- **Google Chronicle:** Chronicle is optimized for the Google Cloud Applications data set and provides additional threat intelligence capabilities with Mandiant and VirusTotal. Additional data ingestion is cheaper in Google. Therefore, it makes sense to ingest high-volume data such as network-related sources: network, routers, switches, web applications, load balancers etc.
- **Splunk:** Splunk efficiently brings Security and IT operational data sources together. The data models can correlate firewalls, EDRs, IDS, antivirus, and IT operational data from data centers together.

A single pane of glass view is essential to bring everything together in a SOC operations platform. CyberProof's CDC platform allows security teams to support advanced correlation and algorithms to understand how security alerts from different solutions are grouped into security incidents. Grouping algorithms and a high level of automation and enrichment is important to not overwhelm SOC analysts with alert fatigue and false-positive blindness.

Leveraging GenAI for security operations

Generative AI has the potential to significantly influence security operations in the cloud – in both positive and negative ways.

Benefits

Threat detection and analysis:
Generative AI can enhance threat detection by analyzing large volumes of data and identifying patterns that might indicate malicious activities. It can assist in detecting new and evolving threats that traditional, rule-based systems might miss. For example, generative AI models could help identify previously unseen attack vectors or create realistic simulations of potential attack scenarios to test defenses.

Anomaly detection:
Generative AI can be used to establish baselines of normal behavior in a cloud environment and identify anomalies that deviate from these patterns. This is particularly useful in detecting insider threats, unauthorized access, or unusual resource consumption that might signal a breach.

Phishing and social engineering mitigation:
Attackers often use social engineering techniques to deceive users into revealing sensitive information. Generative AI can aid in the creation of realistic simulated phishing attacks to train users to recognize and respond to such threats effectively.

Automated incident response:
Generative AI can assist in automating incident response by generating incident reports, analyzing data to determine the scope and impact of an incident, and recommending appropriate remediation steps. This can help security teams respond faster and more accurately to incidents.

Data protection and privacy:
Generative AI can play a role in data anonymization and privacy protection. It can help generate synthetic data for testing and development purposes, reducing the risk of exposing real user data.

Cybersecurity training and simulation:
Generative AI can be used to create realistic simulations for training security professionals in various scenarios, from defending the organization from sophisticated attacks to testing incident response procedures.

Risks

Adversarial attacks:
Just as generative AI can be used for security purposes, it can also be misused by attackers to create convincing phishing emails, spoofed content, or other malicious artifacts that might bypass traditional defenses.

Bias and ethical concerns:
Generative models can inadvertently learn biases present in the training data, leading to the generation of content that perpetuates these biases. This could impact decision-making processes in security operations.

False positives and negatives:
Overreliance on generative AI can lead to both false positives (legitimate activities flagged as threats) and false negatives (actual threats not detected). Fine-tuning and continuous monitoring are crucial to strike the right balance.

Resource consumption:
The use of generative AI for security operations might require substantial computational resources, potentially affecting the overall performance and cost of cloud services.

While generative AI holds promise in enhancing various aspects of security operations in the cloud, it is essential to approach its implementation with caution – addressing ethical concerns, biases, and potential limitations to maximize benefits and minimize risks. Until now, the positives overweigh the challenging aspects of GenAI use. It is advisable to monitor the development constantly, create POCs, and try out new applications to leverage new possibilities.

Microsoft Security Co-Pilot

Open AI-based language support helps detect hidden patterns, harden defenses, and respond to incidents faster, with generative AI.

Incident Response:

Identify an ongoing attack, assess its scale, and get instructions to begin remediation - based on proven tactics from real-world security incidents.

You can ask questions like: "Can you summarize the response to incident 538090?"

or "Summarize the Log4j vulnerability."

Threat Hunting:

Discover whether your organization is susceptible to known vulnerabilities and exploits. Examine your environment one asset at a time for evidence of a breach.

You can ask: "Show me who sent and received mails with an exploit link or attachment around the incident 538090."

Reporting:

Summarize any event, incident, or threat in minutes and prepare the information in a ready-to-share, customizable report for your desired audience.

You can ask: "Create a single PowerPoint slide outlining the Incident 538090 attack chain."

Microsoft XDR-E5 Stack

- Azure Active Directory
- Azure Activity
- AD Identiy Protection
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Defender for Endpoints
- Defender for Office 365
- Defender for IOT

65 trillion signals from the Microsoft XDR E5 stack Security Telemetry data go into the language model.

There are reverse engineering functions as well as feedback reporting that help to improve the results even further.

Microsoft promises your data is protected by the most comprehensive compliance and security controls in the industry. They are committed to an AI-driven methodology with ethical principles.

Fairness

Focuses on how an AI system can allocate opportunities, resources, or information in ways that are fair to the humans who use it

Reliability and safety

Focuses on how an AI system can function well for people across different use conditions and contexts, including ones it was not originally intended for

Privacy and security

Focuses on how an AI system can be designed to support privacy and security

Inclusiveness

Focuses on how an AI system can be designed to be inclusive of people of all abilities

Transparency

Focuses on how an AI system used by people could be misunderstood or misused, or could incorrectly estimate the capabilities of the system

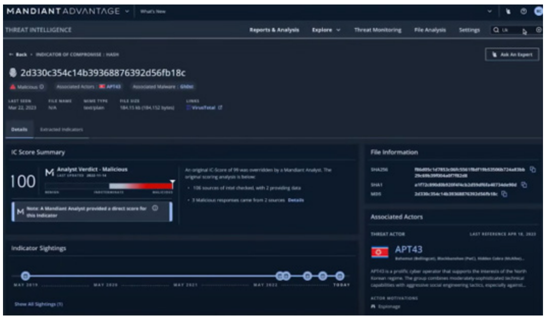
Accountability

Focuses on how an AI system could create oversight so that humans can be accountable and in control

It is a positive sign for the future of AI that a lot of their focus and research is spent on responsible AI learning methods. Microsoft established a team called Aether, an internal AI and ethics committee, which performs research and provides recommendations on responsible AI issues. Aether organizes working groups focused on issues, analysis, and development of the six above-mentioned responsible AI principles.

Google Cloud Security AI Workbench

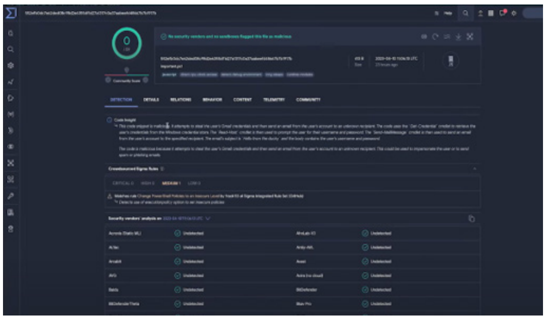
Vertex AI, a Google Cloud Security AI Workbench, gives defenders more natural, creative, and effective ways to keep their organizations safe.



Mandiant Threat Intelligence:

Mandiant Threat Intelligence gives security practitioners unparalleled visibility and expertise into threats that matter to their business.

↓



VirusTotal Malware Research:

VirusTotal aggregates many antivirus products and online scan engines called Contributors. VirusTotal allows a user to check for viruses that the user's own antivirus software may have missed, or to verify against any false positives.

↓

Google Cloud Security AI Workbench could be an industry-first extensible platform powered by a specialized, security LLM, Sec-PaLM.

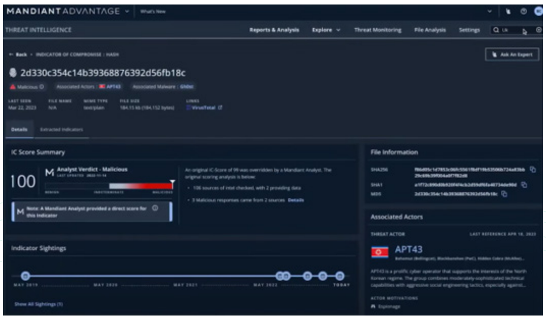
The workbench will be fine-tuned for security use cases, incorporating intelligence into the threat landscape from Google and Mandiant.

Chronicle

The Workbench will feature an extensible, plug-in architecture that allows customers and partners to build on top of the platform while helping to keep control and isolation over their data.

With Google Security Workbench, clients can combine threat intelligence with real time incident analyses with novel AI-based detections and analytics to identify and contain initial infections and help prevent them from spreading.

↓



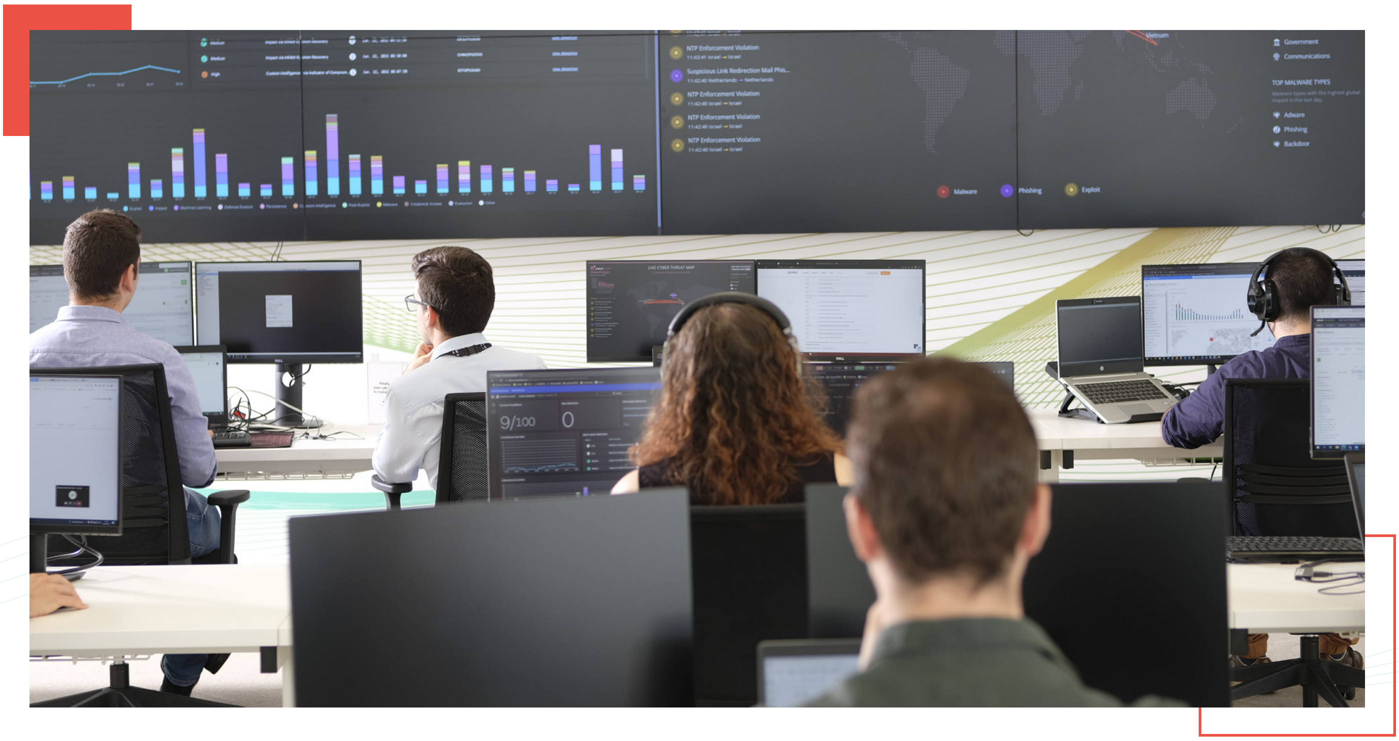
Google Security Workbench

When Google releases this generative AI Security Workbench, it has the potential to profoundly change how practitioners across different skill levels "do" security. AI assistive features summarize complex threats, assess risk, and enable natural language search and investigation to help usher in a new era of effectiveness.

Chronicle Cloud enables clients to search security events and interact conversationally with results, ask follow-up questions, and quickly generate detections.

Key Takeaways

- **GenAI:** Keep track of the potential that GenAI brings to cloud security operations. Big vendors will invest heavily in technologies that will provide them with differentiation on the market. For security practitioners, GenAI can enhance threat detection, supporting the analysis of large volumes of data and identification of patterns that might indicate threat actor activity in the environment.
- **What to monitor:** Monitoring the security of your multi-cloud estate requires not just the aggregation of data from different cloud providers but also of cloud assets, including virtual machines, containers, applications, and others.
- **Single aggregation point:** Make sure you have a level of individual controls that allow you to monitor the threat activity of individual assets. It can become overwhelming to connect the dots across these assets so that you're seeing correlated activity, which paints a picture of what an attacker could be doing in your cloud environments. Ensure that you have a single aggregation point, via a cloud-SIEM like Sentinel, that can centralize the detection of all activity.
- **Cost**: As you start ingesting more data from your cloud environments, the costs will rise exponentially if they are not controlled. It's critical to filter data before it enters your detection systems.
- **Use case governance:** Determine what type of threats you should be looking for that involve multi-cloud scenarios, so you can focus your detection efforts and minimize alert fatigue. Having a Use Case Governance framework enables you to prioritize and fill threat coverage gaps.
- **Working with experts:** Invest in the right human resources that know how to continuously detect, investigate, and respond to these kinds of threats, use a combination of tools, and recommend the right action for remediating appropriately.



CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts.

Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics.

Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com

Locations

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum