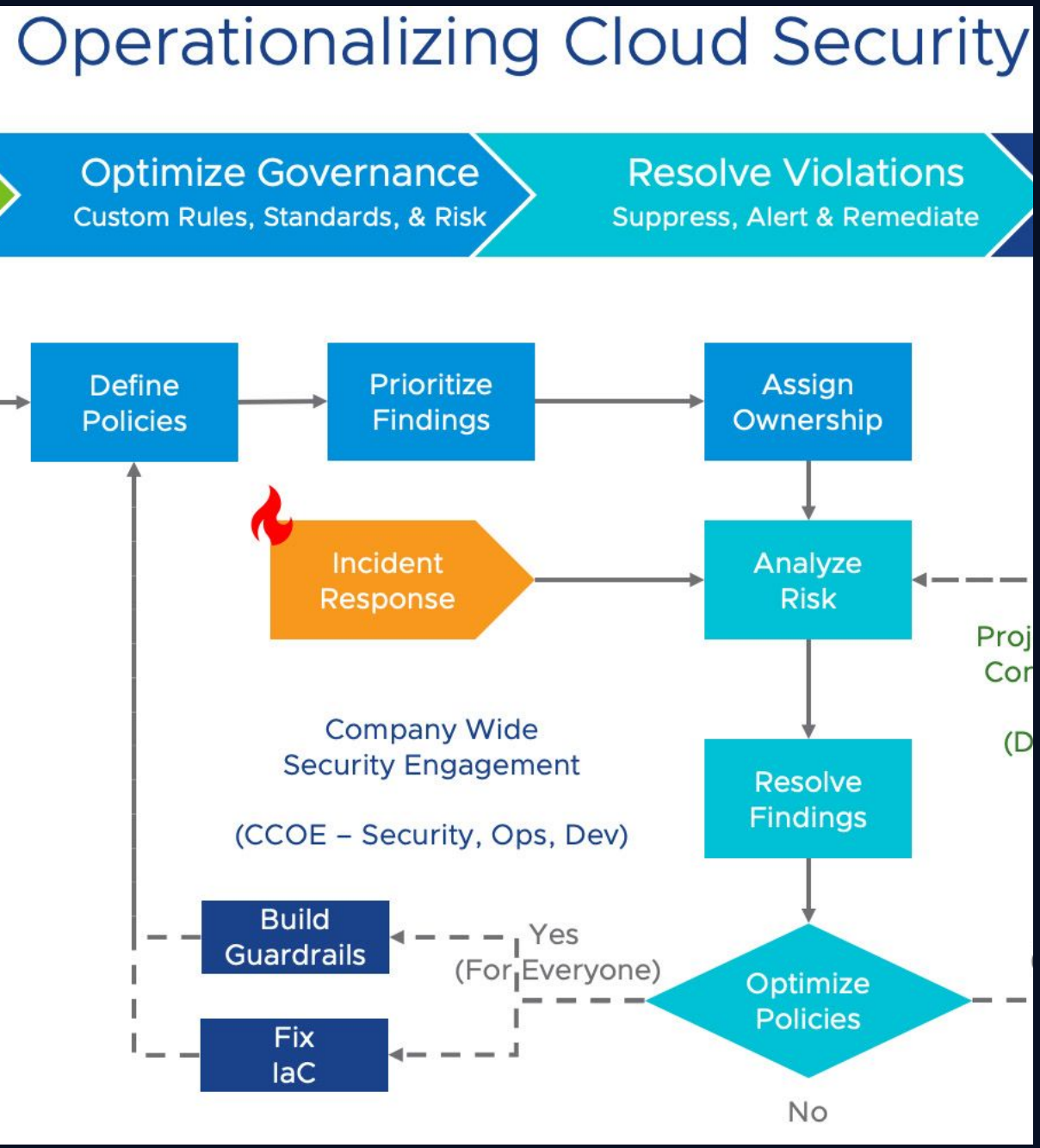


BEYOND LOGS: ENHANCING CLOUD SECURITY THROUGH POSTURE MANAGEMENT

This slide introduces the topic of cloud security posture management, which extends beyond traditional logging and event monitoring to proactively evaluate the security state of cloud infrastructure, applications, and resources.

INTRODUCTION TO CLOUD SECURITY POSTURE MANAGEMENT

Beyond Traditional Logging

Cloud security extends beyond traditional logging and event monitoring by incorporating Cloud Security Posture Management (CSPM).

Maintain Security Configurations

CSPM focuses on maintaining security configurations, identifying risks, and ensuring compliance across cloud environments.

Proactive Risk Identification

CSPM takes a proactive approach by continuously evaluating the security state of cloud infrastructure, applications, and resources.

Automated Remediation

Cloud-native tools enable security teams to assess vulnerabilities, detect anomalous behavior, and automate remediation workflows.

By incorporating Cloud Security Posture Management, organizations can enhance their cloud security beyond traditional logging and monitoring, focusing on maintaining secure configurations, identifying risks, and ensuring compliance across cloud environments.

MANAGEMENT PLANE LOGS

- ## Cloud Resource Governance

  The management plane governs how cloud resources are created, modified, and accessed, unlike the data plane which deals with actual data processing.

- ## Identify Policy Violations

  Management plane logs provide insight into how security policies are enforced, allowing organizations to identify non-compliant configurations or policy violations.

- ## Detect Unauthorized Access

  Monitoring management plane logs is essential for detecting unauthorized access, such as suspicious API calls or unexpected user activities.

- ## Prevent Privilege Escalations

  By tracking management plane events, security teams can detect privilege escalation attempts and proactively prevent unauthorized access to critical cloud resources.

SERVICE & APPLICATION LOGS

- ## Capture Runtime Events

  Service and application logs provide detailed information about the execution of cloud-based applications, including events such as function invocations, database queries, and API calls.

- ## Monitor API Requests

  Logs track all API interactions, allowing security teams to detect unauthorized access attempts, suspicious API usage patterns, and potential integration vulnerabilities.

- ## Analyze User Interactions

  Application logs capture user activities, authentication failures, and other user-related events, enabling the detection of anomalous user behavior and potential security breaches.

- ## Detect Security Anomalies

  By analyzing service and application logs, organizations can identify security threats, such as malware infections, data exfiltration attempts, and unauthorized access to sensitive resources.

- ## Identify Performance Issues

  Logs provide insights into application performance, helping organizations identify bottlenecks, resource exhaustion, and other operational issues that could impact the availability and reliability of cloud-based services.

RESOURCE LOGS

- ## Compute Logs

  Capture information about virtual machine activity, instance reboots, and software updates. Monitoring compute logs helps detect unauthorized access to cloud instances and potential malware infections.

- ## Storage Logs

  Record file access attempts, modifications, and deletion events, allowing organizations to identify data exfiltration risks or misconfigured permissions.

- ## Database Logs

  Provide insight into SQL query executions, failed login attempts, and privilege changes. These logs are essential for detecting suspicious database queries, unauthorized schema modifications, and potential SQL injection attacks.

- ## Network Logs

  Capture information about traffic patterns, firewall rule enforcement, and connectivity issues, helping security teams identify denial-of-service (DoS) attacks, lateral movement attempts, and insecure network configurations.

CLOUD-NATIVE TOOLS

Automated Risk Assessment

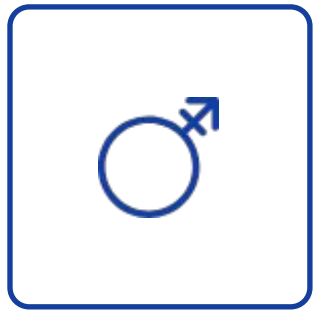
Cloud-native tools continuously scan cloud configurations to identify security vulnerabilities, misconfigurations, and compliance gaps.

Real-time Remediation

These tools enable automated remediation workflows to fix security issues and enforce best practices across cloud environments.

Integrated Monitoring

Cloud-native security solutions integrate with logging, monitoring, and compliance frameworks to provide a unified view of the security posture.



Centralized Visibility

Tools like AWS Security Hub, Azure Security Center, and Google Security Command Center offer a centralized dashboard for managing cloud security risks.

Cloud-native security tools empower organizations to proactively manage their cloud security posture, detect and remediate risks, and ensure compliance in real-time.

EVENTS TO MONITOR

- ## IAM and Access Management Events

  Track privilege escalations, unauthorized API calls, and suspicious login attempts to detect unauthorized modifications to IAM policies or excessive permission grants.

- ## Network Security Events

  Monitor firewall rule changes, anomalous outbound traffic, and failed VPN authentication attempts to detect potential cyber threats such as DDoS attacks, malicious IP connections, and unauthorized data transfers.

- ## Storage and Data Access Events

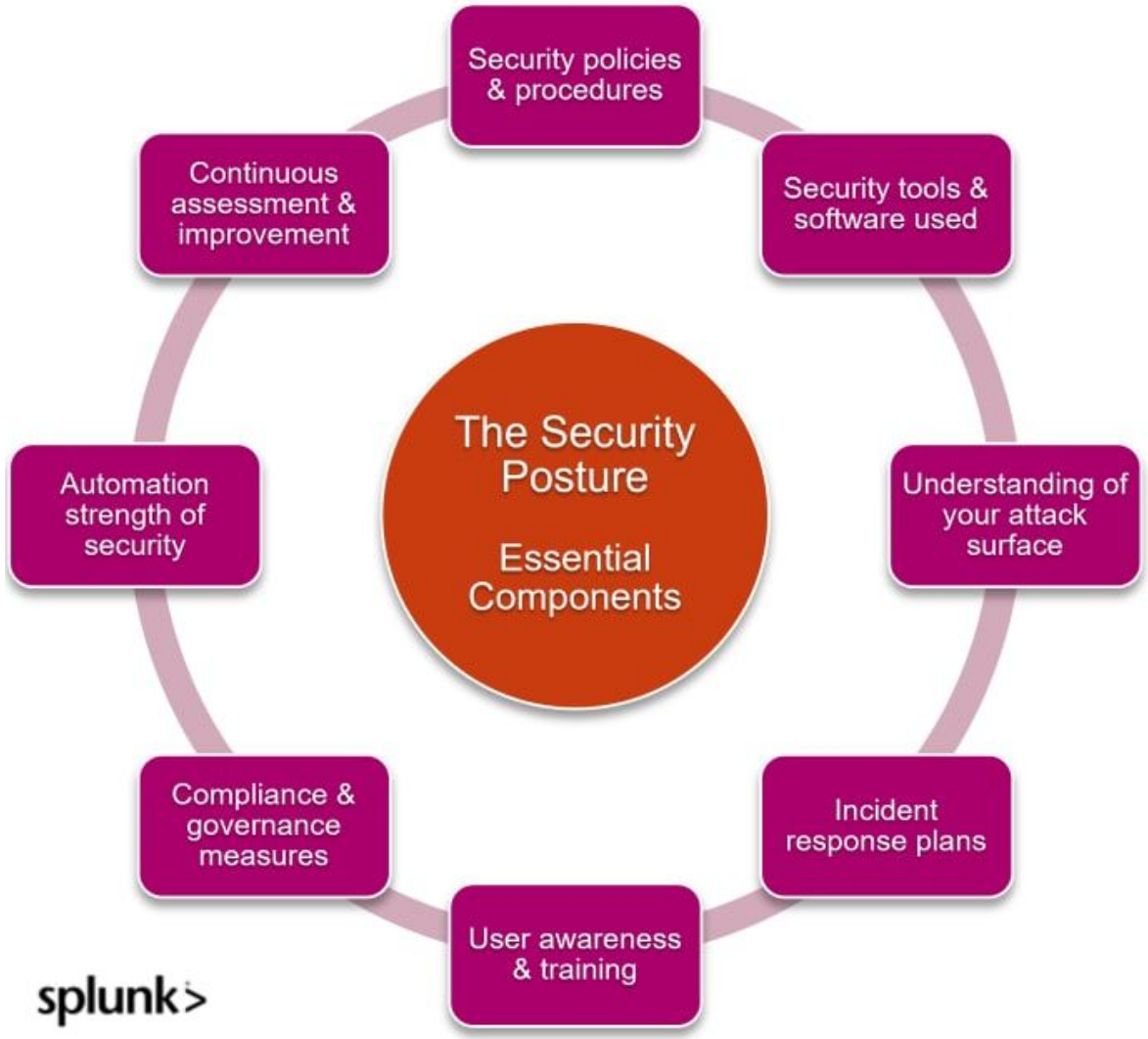
  Analyze cloud storage logs to detect file modifications, mass data downloads, and attempts to access restricted storage locations, which could indicate ransomware activity, data exfiltration, or insider threats.

- ## Compute and Infrastructure Changes

  Track unexpected instance terminations, unauthorized container deployments, and high CPU utilization spikes to detect potential cryptojacking, unauthorized software installations, or resource hijacking.

- ## Compliance and Policy Violations

  Monitor for non-compliant configurations, unencrypted data storage, and insecure IAM roles to enforce regulatory standards such as GDPR, HIPAA, and ISO 27001.



CASE STUDY: STRENGTHENING CLOUD SECURITY POSTURE

A multinational technology firm operating across AWS, Azure, and Google Cloud required real-time visibility into cloud security risks, automated compliance enforcement, and proactive posture management. The firm deployed AWS Security Hub and Azure Security Center to assess security vulnerabilities and detect non-compliant configurations.

OUTCOMES

Reduced Risk of Cloud Misconfigurations

The organization implemented cloud-native security posture management tools to continuously assess their cloud environments, identify security vulnerabilities, and automatically remediate misconfigurations, reducing the risk of security incidents caused by misconfigured cloud resources.

Ensured Compliance with Regulatory Frameworks

The automated compliance monitoring and enforcement capabilities provided by the cloud-native security tools enabled the organization to consistently maintain compliance with industry regulations such as GDPR, HIPAA, and ISO 27001, reducing the risk of costly fines and penalties.

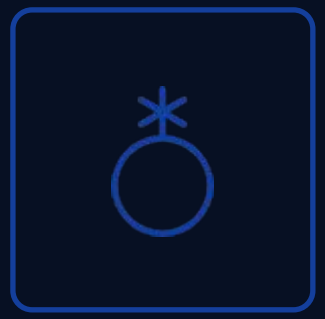
Improved Threat Detection Capabilities

By integrating the cloud-native security tools with their SIEM platform, the organization gained real-time visibility into security events, anomalous activity, and potential threats across their multi-cloud infrastructure, allowing them to respond quickly and mitigate the impact of security incidents.

Automated Posture Assessment and Event Monitoring

The continuous monitoring and automated remediation workflows of the cloud-native security tools enabled the organization's security teams to respond to security incidents in real-time, minimizing the impact of potential attacks and reducing the organization's overall risk exposure.

ADDITIONAL RESOURCES



AWS Security Hub Documentation

Comprehensive guide to AWS's security posture management service, including features, configuration, and best practices.

Azure Security Center Overview

Detailed overview of Microsoft's cloud security posture management solution, highlighting key capabilities and integrations.

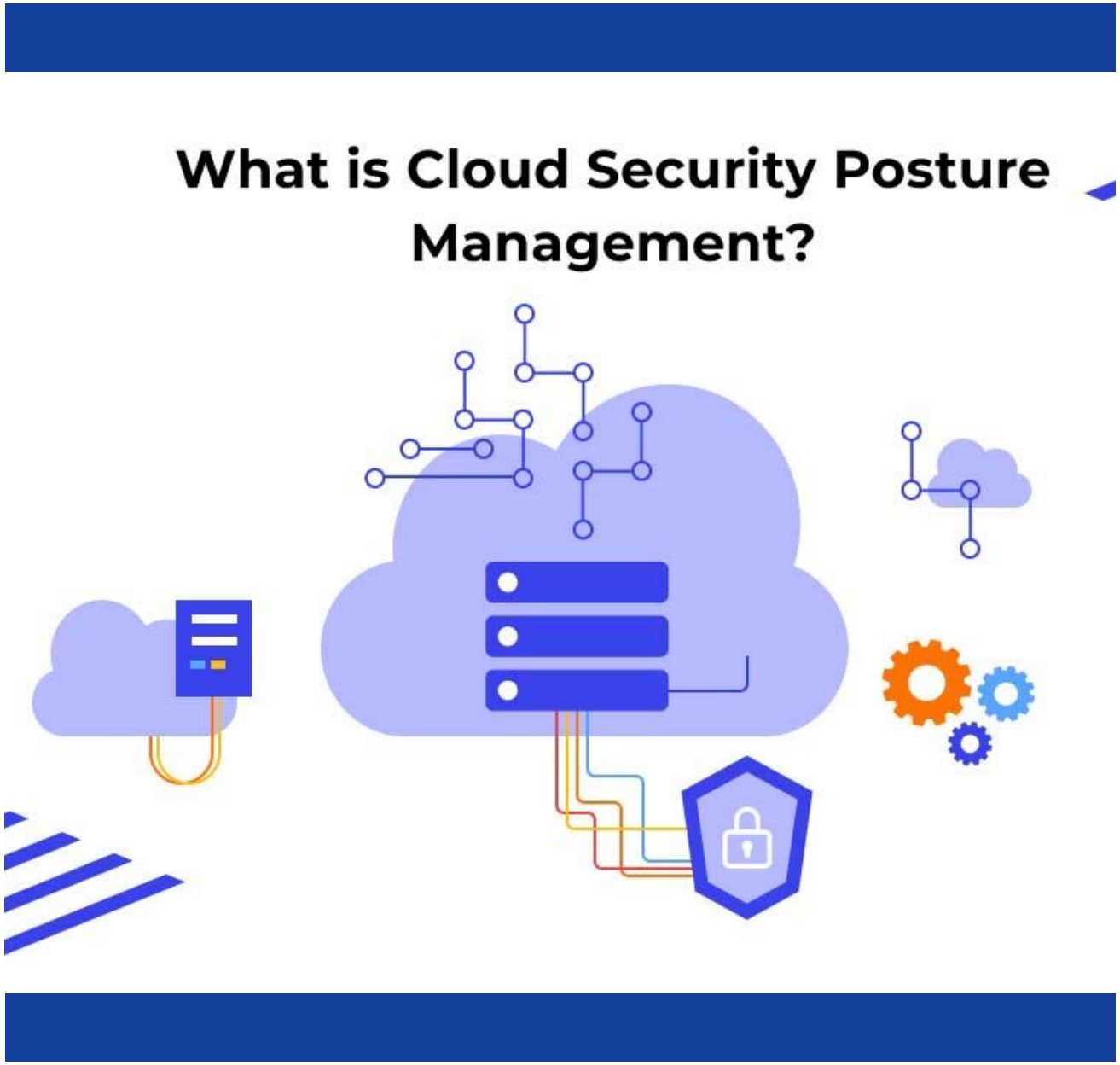
Google Security Command Center

In-depth information about Google's security posture management tool, featuring security assessment, threat detection, and remediation.

These resources provide detailed guidance and insights on implementing cloud security posture management across major cloud platforms, enabling organizations to enhance their cloud security and compliance.

CONCLUSION

Cloud security posture management is a critical component of modern cloud security strategies. It extends beyond traditional log-based monitoring by automating the detection of security risks, enforcing security policies, and proactively preventing security incidents across cloud environments.



KEY TAKEAWAYS

CSPM focuses on security configurations, risks, and compliance

Cloud Security Posture Management (CSPM) continuously evaluates the security state of cloud infrastructure, applications, and resources to maintain best practices, detect misconfigurations, and ensure compliance across cloud environments.

Monitoring management plane, service & application, and resource logs

Tracking API calls, user activities, runtime events, and resource access/modifications provides visibility into potential security threats, policy violations, and misconfigured settings.

Adopting a comprehensive cloud security posture management approach, leveraging cloud-native tools, and continuously monitoring critical events are essential to maintaining robust security and compliance in the cloud.

KEY TAKEAWAYS

Cloud-native tools for automated posture management

Integrated security solutions like AWS Security Hub, Azure Security Center, and Google Security Command Center enable real-time risk detection, security baseline enforcement, and automated remediation workflows.

Continuous monitoring of critical security events

Tracking IAM modifications, network anomalies, storage access, and infrastructure changes helps prevent data breaches, unauthorized access, and security incidents.

Adopting a comprehensive cloud security posture management approach, leveraging cloud-native tools, and continuously monitoring critical events are essential to maintaining robust security and compliance in the cloud.

"EMBRACE CLOUD SECURITY POSTURE MANAGEMENT TO STRENGTHEN YOUR ORGANIZATION'S CLOUD SECURITY AND MAINTAIN COMPLIANCE IN THE FACE OF EVOLVING THREATS. LEVERAGE CLOUD-NATIVE TOOLS AND AUTOMATED MONITORING TO PROACTIVELY IDENTIFY AND MITIGATE SECURITY RISKS."