zensar

Delivering a Cognitive Security Operations Center for a Global Mobility Leader

Case Study

Overview

Identifying and mitigating threats before they cause harm

A global mobility company, operating in 150 countries worldwide, helps businesses and individuals navigate the complexities of cross-border work with a wide range of services, including tax planning, immigration services, business travel management, remote work compliance, and compensation and rewards management. It decided to transform its risk management strategy in response to the evolving threat landscape.

Zensar's brief:

Deploy a comprehensive vulnerability management solution to address key cybersecurity goals:

- Enable proactive threat identification to address security weaknesses before they can be exploited by malicious actors.

- Ensure compliance with regulations and industry standards that mandate regular security assessments.
- Strengthen the company's overall security posture with remediation measures to mitigate the fallout of cyberattacks.

Beyond the brief:
We accelerated the path toward realizing a cognitive security operations center (SOC), leveraging our IP, advanced tools, and capabilities that cover these key security aspects:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- Identity and access management (IAM)
- Web application firewalls (WAFs)
- Vulnerability assessment and penetration testing (VAPT)

Challenges

Addressing multiple concerns with a transformative approach

The organization's IT department needed a technology consultant to explore a transformative approach to deal with a whole gamut of concerns:

- **High dwell time:** Prolonged periods between initial compromise and threat detection were leading to significant damage.
- **Alert fatigue:** Security operations teams were often overwhelmed by the sheer volume of alerts, many of which turned out to be false positives.
- **Complex security infrastructure:** As integrating various security tools and solutions was complex and time-consuming, achieving a unified view of security incidents was proving to be difficult.
- **Manual processes:** Reliance on manual processes for threat detection and incident response was inefficient and slow, leading to delayed responses to security incidents.
- **Regulatory compliance:** Ensuring compliance with regulatory requirements and maintaining historical data for audits was often challenging, especially when transitioning from older security solutions.
- **Resource constraints:** Limited in-house resources and expertise made it difficult to effectively manage and respond to security threats.

Solution

Migrating SIEM from IBM QRadar to Azure Sentinel

Working closely with the client's IT department, we delivered end-to-end vulnerability management, covering initiation and scoping, reconnaissance, vulnerability assessment, penetration testing, remediation and management, and continuous verification and monitoring.

Assessing and designing the security architecture: We started with a detailed assessment of the capabilities and gaps between IBM QRadar and Azure Sentinel. Based on this analysis, we designed and implemented the Azure Sentinel architecture, integrating critical infrastructure, security solutions, and custom logs for comprehensive event correlation and detection of malicious activities.

Configuring security use cases and automating: We configured security use cases according to the MITRE ATT&CK framework and integrated Azure Sentinel with the organization's ticketing tool for automated SLA management. This setup was designed to reduce manual intervention, minimize alert fatigue, decrease false positive alerts, and enhance overall SecOps efficiency.

Delivering custom dashboards and real-time insights: We developed custom dashboards to monitor SecOps efficiency, traffic, and cost utilization. We leveraged Azure Sentinel to provide a unified view of security incidents from all devices, enabling real-time dashboards with threat insights, expediting incident response, and improving decision-making.

Enabling enterprise-wide threat hunting and compliance: We enabled enterprise-wide threat hunting to proactively search for threat actors and ensured data archival from the old solution for regulatory compliance. Drawing on Azure Sentinel's built-in threat hunting, threat intelligence, and user and entity behavior analytics (UEBA) services, we enhanced the organization's security posture.

Leveraging cloud and community support: With Azure Sentinel, we harnessed the scale of the cloud SIEM and AI capabilities to offer advanced threat detection and response. Moreover, support from the SIEM community and Microsoft security experts enabled continuous information sharing and robust protection against emerging threats.

Solution enablers

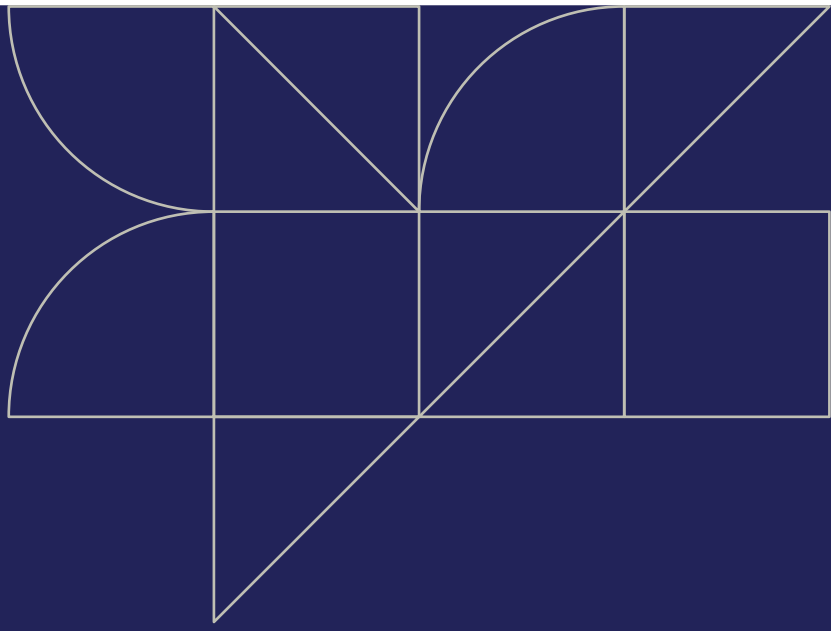
- **Azure Cloud** was used for its scalable, AI-driven threat detection and response capabilities, ensuring robust protection and operational efficiency.
- **Azure Active** Directory was used to enable seamless integration, robust identity management, and enhanced security, ensuring secure access and compliance.
- **Azure Sentinel** was used for its advanced threat detection and automated response features, ensuring comprehensive and efficient security management.
- **Azure Lighthouse Connectivity** was used to enable scalable, secure, and efficient management of multi-tenant environments, enhancing visibility and control across resources.

Impact

Enhanced efficiency and resiliency

- **Reliable foundation:** Established an effective correlation layer for basic security events monitoring.
- **Advanced analytics:** Defined security operations with proactive threat detection, visibility, and hunting.
- **Powerful accelerators:** Enabled integrated and well-orchestrated operations by leveraging SIEM and SOAR tools.
- **Future-ready approach:** Set up the environment with autonomous threat-hunting capabilities to quickly detect and respond to threats, minimizing the time attackers can operate undetected.

Business outcomes: Bringing together advanced analytics, proven accelerators, and a proactive and adaptive security approach, the solution fueled the global mobility leader's mission to create a connected and empowered global workforce.



zensar

An RPG Company

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145 leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: **info@zensar.com | www.zensar.com**