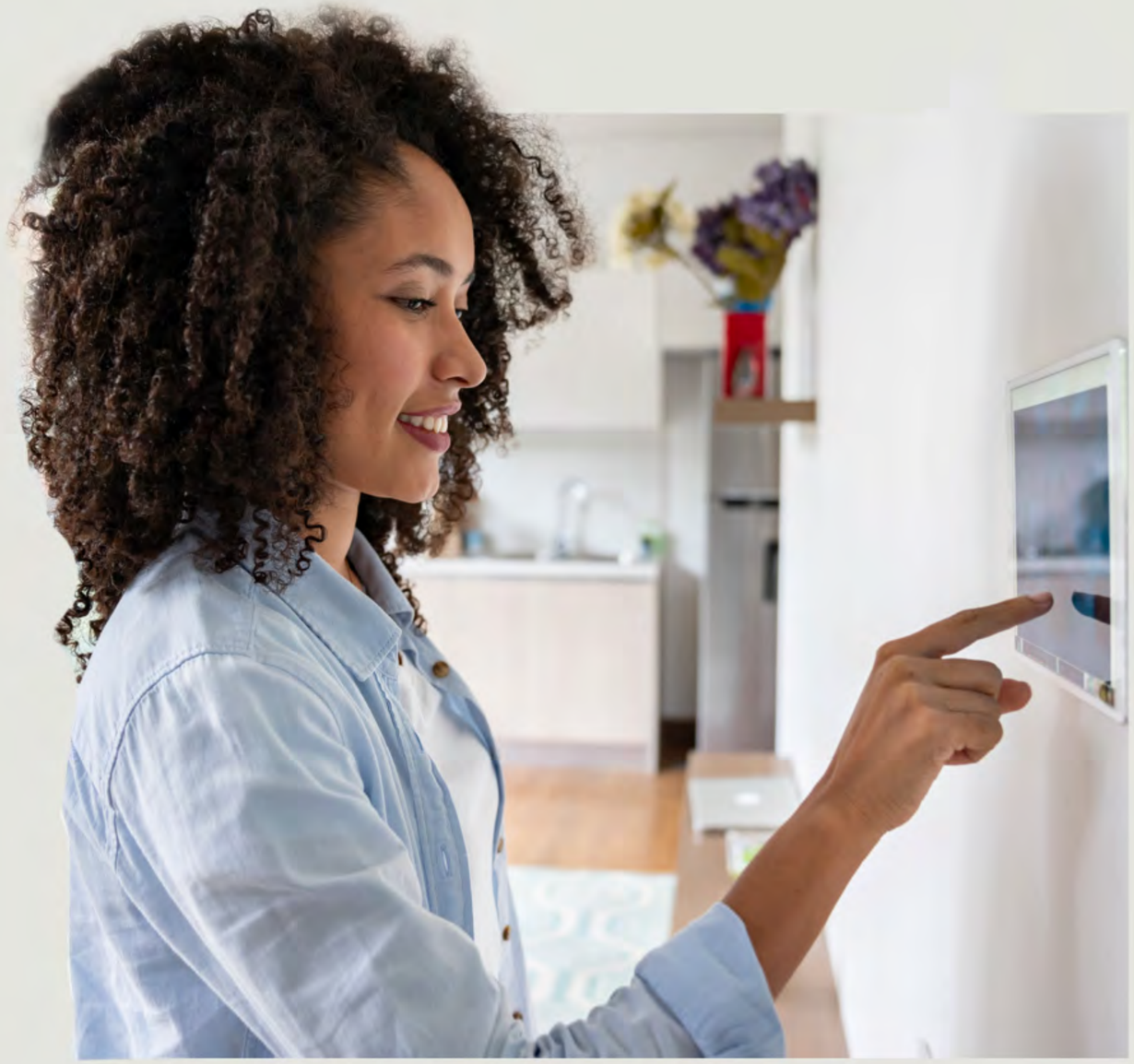
zensar



Transforming the legacy security of a large U.S. city with end-to-end threat detection, hunting, and response

Case study

Overview

The client is one of the largest cities in the United States. It needed transformation of its existing legacy security to end-to-end security with advanced capabilities to manage threats and risks in the future.

We provided a complete solution using the following tools in the client environment: Sumo Logic cloud security information and event management (SIEM), Demisto security orchestration, automation, and response (SOAR), FireEye, Palo Alto firewall, Palo Alto Prisma, Cisco Adaptive Security Appliance (ASA), Cisco Identity Services Engine (ISE), CrowdStrike endpoint detection and response (EDR), Netskope cloud access security broker (CASB), RSA multi-factor authentication (MFA), Sucuri web security, Cloudflare distributed denial-of-service (DDoS), public key infrastructure (PKI), hardware security module (HSM), Sectigo, F5 Application Security Manager™ (ASM), Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) cloud security.

Business objective

The key objective was to perform a complete assessment of the client's existing infrastructure, then design and manage a proactive solution for existing and future requirements.

We focused on configuring log sources, alerts, reports, and playbooks in SIEM and SOAR platforms for greater visibility and building the library for advanced threat detection, hunting, and response.

Challenges

- **Alert fatigue**
  with a high number of false-positive alerts
- **Management and visibility**
  with the security of an ever-expanding infrastructure
- **MITRE modeling**
  with massive manual efforts without effectively using SIEM and SOAR tools

Solution

- Assessment of existing infrastructure and the security operations center's (SOC) program management
- Four weeks of transition with eight weeks of transformation and two weeks of the shadow state
- Zero trust network with identity management and MFA solution
- Use cases development and optimization
- Automated incident and task management
- Proactive threat hunting, threat detection, logs monitoring, and incident response
- 24x7 security monitoring and platform support (L1, L2, and L3)
- Unified workflow. Example: problem, change, and configuration management framework
- 24x7 web, network, and endpoint security management
- 16x5 security content development (L2 and L3)

Impact

- 90% reduction of false positives
- 70% faster incident handling
- 30% reduction in operating expenses (OPEX) due to effort optimization
- Better visibility and utilization of resources

zensar

An RPG Company

We conceptualize, build, and manage digital products through experience design, data engineering, and advanced analytics for over 130 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile, and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,000+ associates work across 33 locations, including San Jose, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

For more information please contact: velocity@zensar.com | www.zensar.com