

# US City Gets Better and Faster at Finding and Fixing Security Threats

## Case Study



## Overview

### Safeguarding city and citizen data

The administration of one of the largest US cities, with a burgeoning population, found that its existing legacy security solution was inadequate to ensure public safety and security — now and in the future. And it needed to fix the situation.

#### Zensar's brief:

- Perform a complete assessment of the existing infrastructure.
- Design and deliver a proactive solution for existing and future requirements.
- Configure log sources, alerts, reports, and playbooks in SIEM (security information and event management) and SOAR (security orchestration, automation, and response) platforms for greater visibility.
- Build the library for advanced threat detection, hunting, and response.

## Beyond the brief:

We supported the client with an end-to-end partnership to implement a transformative security solution with advanced capabilities and lay the foundation for future scalability and resilience.



## Challenges

---

### Poorly equipped to manage evolving threats

The city's IT organization was grappling with poor management and visibility of an ever-expanding security infrastructure, alert fatigue with a high number of false-positive alerts, and the use of MITRE modeling with massive manual efforts and without effective use of SIEM and SOAR tools.



## Solution

---

### Transforming the data management landscape

We transformed the client's legacy security landscape with a future-ready solution, with these key services:

- **Assessment** of existing infrastructure and the security operations center's (SOC) program management.
- **Transition** spanning across four weeks, followed by eight weeks of transformation and two weeks of the shadow state.
- **Implementation** of zero trust network with an identity management and multi-factor authentication (MFA) solution.
- **Development and optimization** of use cases.
- **Automation** of incident and task management.
- **Deployment of proactive strategies** for 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 security management** — across the web, network, and endpoints.
- **16x5 security content development** (L2 and L3).

# Solution highlights

---

- End-to-end support for the city's GCP cloud infrastructure, covering all support levels and cloud services.
- Ownership of daily operational requirements and enhancements as well as new solution requirements.
- Implementation of a private connection between the city's GCP cloud environment and the on-premises infrastructure.
- Implementation of redundant connectivity, for private connection through site-to-site VPN, to which traffic is automatically routed when the private connection becomes unavailable.
- Deployment of a GCP cloud storage solution to address rising storage needs.
- Installation of a Palo Alto firewall on the city's GCP environment to enhance internet access security.
- Collaboration with Google to lay the foundation for deploying AI chatbots.
- Definition of a GCP cloud cost reporting tool and process.



## Impact

Better, faster, and cost-effective threat response

According to internal benchmarks, these results were delivered:

- 90 percent reduction of false positives
- 70 percent faster incident handling
- 30 percent reduction in operating expenses due to effort optimization

**Business outcomes:** The solution enabled better visibility and utilization of resources, as well as greater preparedness for mitigating future threats.

**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](mailto:info@zensar.com) | [www.zensar.com](http://www.zensar.com)