splunk>

CASE STUDY

City of Los Angeles Integrates Real-Time Security Intelligence Sharing Across 40+ City Agencies

Executive summary

To protect its digital infrastructure, the City of Los Angeles requires situational awareness of its security posture and threat intelligence for its departments and stakeholders. In the past, the city's more than 40 agencies had disparate security measures, complicating the consolidation and analysis of data. Los Angeles sought a scalable SaaS security information and event management (SIEM) solution to identify, prioritize and mitigate threats, gain visibility into suspicious activities and assess citywide risks. Since deploying Splunk Cloud and Splunk Enterprise Security (ES), the city has seen benefits including:

- Creation of citywide security operations center (SOC)
- Real-time threat intelligence
- Reduced operational costs

Why Splunk

Los Angeles is a vast metropolis with critical infrastructure like airports, seaports, and water and power, as well as 35,000 employees and over 100,000 endpoints generating 14 million security events daily. Its departments had their own security tools, requiring the city to gather and manually correlate logs from each agency for broad views of its network security. This process was cumbersome, imprecise and slow to address threats.

"Our mayor issued an executive directive to improve cybersecurity," says Timothy Lee, chief information security officer for Los Angeles. "This meant collecting and evaluating all of our logs in real time. We needed a scalable SIEM to drive an integrated, citywide SOC." Mindful of the city's budget, Lee wanted a cloud-based SIEM to avoid the administrative burdens of onsite platforms. After considering available solutions, Los Angeles chose Splunk Cloud and Splunk Enterprise Security. Splunk Cloud offers extraordinary scalability and a 100 percent uptime SLA. According to Lee, "Splunk Cloud was fast to deploy and easy to tailor, whereas customizing competing products required two full-time employees."

Splunk Cloud also resolved two concerns: data security and bandwidth consumption. Splunk forwarders encrypt and compress all data before

Industry

- City government

Splunk Use Cases

- Security

Challenges

- Disparate logs from over 40 departments were difficult to aggregate
- Inadequate situational awareness of security events
- Limited threat intelligence
- Slow responses to security incidents
- Modest IT resources

Business Impact

- Real-time, citywide, 24/7 network surveillance
- Stronger protection of digital assets and infrastructure
- Proactive network safeguards
- Shared threat intelligence with federal agencies
- Reduced headcount and lower operational costs
- Preservation of public trust

Data Sources

- Firewall logs
- FireEye Threat Prevention Platform
- Intrusion prevention/detection systems
- External threat intelligence feeds
- Switches and routers

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security

it leaves the enterprise, rendering information secure in transit and bandwidth consumption negligible.

Real-time situational awareness

Splunk Cloud provides Los Angeles with holistic views of its security posture. Splunk forwarders send raw logs and other data from the city's departments to Splunk Cloud, where they are normalized and returned to the integrated SOC, and then analyzed and visualized in Splunk dashboards.

Using pre-built, easily customizable dashboards in Splunk ES, executives and analysts have always-available, real-time situational awareness of security events across the city's networking infrastructure. With all security data in one continuously updated database, Lee's team views and compares any machine-generated data, including disparate logs and both structured and unstructured data, to extract all-inclusive, actionable security intelligence.

Analysts can monitor for malware and identify the top attackers and their targets within the infrastructure. Splunk dashboards alert for security events, enabling prompt responses to intrusions that threaten public services or assets. Analysts conduct searches and forensic investigations, drilling down to track hazards anywhere in the enterprise.

"By using the Splunk platform to gain visibility into questionable network activities, we assess risks, prioritize and mitigate threats, and proactively address vulnerabilities," says Lee. "Our Splunk SIEM is like having video cameras on every block; it provides visibility into what's happening on the network, which is foundational to safety."

Timely threat intelligence

The city's integrated SOC does more than collect information; it also provides information. It translates data from Splunk Cloud into timely threat intelligence. The city shares its findings with its agencies as well as external stakeholders like the FBI, the Department of Homeland Security, the Secret Service and other law enforcement agencies. With this information, the city collaborates with federal agencies to identify risks and develop strategies for deterring future network intrusions.

"By deploying the Splunk SIEM solution, we enhance our detection and response capabilities to protect the City's critical assets from all manner of cyberthreats and intrusions. By utilizing a cloud solution, our security team can focus on security events rather than deploying and maintaining infrastructure."

Timothy Lee
Chief Information Security Officer
City of Los Angeles

"With situational awareness, we know ourselves," says Lee. "But with threat intelligence, we know our enemy. We're now operating an integrated threat intelligence program and our Splunk SIEM is one of the key solutions for a centralized information management platform that we deploy at our Integrated Security Operations Center (ISOC)."

Locking down the city's digital assets

By anchoring its integrated SOC with the rich SIEM functionalities of Splunk Cloud and ES, Los Angeles met its mayor's directive by transforming its patchwork of security measures into a cohesive, all-encompassing cybersecurity strategy. "As the number and sophistication of risks increase, our cloud-based Splunk solution levels the playing field by making our security team more effective," concludes Lee. "With both holistic and granular views of our digital assets, we have the awareness and knowledge to counter the threats that imperil Los Angeles and other cities. For municipalities that are decentralized into many departments, the Splunk platform is a comprehensive yet cost-effective security solution."

splunk> sales@splunk.com www.splunk.com