Recorded Future®

CASE STUDY

City of Los Angeles Stays One Step Ahead with Intelligence from Recorded Future®

The L.A. Information Technology Agency (ITA) works with agencies and departments across the city of Los Angeles to develop world-class IT infrastructure and keep the digital assets secure.

LOS ANGELES

USE CASE
- SOC alert triage and IOC prioritization

CHALLENGE

Too many alerts; not enough resources
- 3 Security Operations Centers
- 1 billion security-related events per day
- 4 million attempted intrusions per day

SOLUTION
- Security Intelligence integrated into SIEM and SOAR solutions

OUTCOMES

Improved analyst efficiency
- Accelerated alert triage
- Faster incident resolution

Too Many Alerts, Too Little Context

Timothy Lee, the city's chief information security officer, leads a team responsible for managing the daily operations of the Integrated Security Operations Center (ISOC), which maintains the overall cybersecurity posture of more than 40 departments. Tasked with investigating and responding to over one billion security-related events flowing from three integrated security operations centers, as well as more than four million attempted intrusions into City networks, per day, the team's resources were stretched thin and the work was inefficient.

"We were using a mix of open source and paid intelligence feeds, but didn't have the ability to dig deep into external threat indicators or groups," recalls security operations manager Ryan Norwall. "We were spending a lot of time weeding through feeds, ruling out false positives, and manually researching IOCs and threat actors — we needed our threat intelligence to be more actionable."

They knew that staying a step ahead of threat actors requires real-time context around the City's internal security environment and its relation to external threats and trends. Until recently, this was difficult to come by.

> "We were impressed by the flexibility and affordability of the Recorded Future platform, but what sealed the deal was its ability to integrate with our SIEM and SOAR systems.
>
> *Daniel Clark Lee*
> *Cybersecurity Threat Analyst*

Intelligence Integrated in SIEM and SOAR

After consulting industry peers and independent analysts and considering a number of solutions, the ITA selected Recorded Future Security Intelligence. The solution was selected for its rich context and ability to put real-time security intelligence directly into the City's existing security operations technology infrastructure.

Says cybersecurity threat analyst Daniel Clark Lee, "We were impressed by the flexibility and affordability of the Recorded Future platform, but **what sealed the deal was its ability to integrate with our SIEM and SOAR systems**."

These integrations enable the team to interact with rich external information and threat indicators from across the open and dark web, all correlated with their internal log data, resulting in:

- Accelerated alert triage and investigations with real-time context
- Prioritization of IOCs and faster incident resolution

"We see more than a billion events per day," says Norwall. "Recorded Future gives us the ability to enrich this data and gain additional insights into TTPs, social media handles, dark web forums, special access groups and more that we didn't previously have access to."

For example, the team has been able to zero in on specific conversations happening on social media and quickly validate claims such as, "I just hacked the City of L.A." "With Recorded Future, we understand the context behind the actor — who this person is, what they have been tweeting about, and if they've made similar claims in the past," says Norwall.

Security intelligence also empowers the City of L.A. to defend against common attacks, such as typosquatting. "Just seeing an alert that a domain has been registered doesn't tell you the full story," explains Norwall. "Recorded Future takes it to the next level by showing us the progression: when a site is registered, when certificates start getting registered to it, and when reports emerge that it's being used for malicious content."

> "We don't want our analysts to have to keep 20 different tabs open during the day in order to do their jobs. Recorded Future provides a single-pane-of-glass view and is easy to use within analysts' existing workflows.
>
> *Daniel Clark Lee*
> *Cybersecurity Threat Analyst*

With more than 50,000 City employees, the ability to find data leaks fast is also critical. Norwall continues, "Many other tools focus solely on paste sites. Recorded Future allows us to get more granular by filtering out places like dark forums and credit card sites where we can look for specific people trying to sell credentials and access."

Automated Processes and More Efficient Analysts

"**We've improved the efficiency of our analysts with Recorded Future**," says Norwall.

"And by integrating with our SIEM and SOAR, we're enriching and automating processes across our Integrated Security Operations Center."

Lee adds, "We don't want our analysts to have to keep 20 different tabs open during the day in order to do their jobs. **Recorded Future provides a single-pane-of-glass view and is easy to use within analysts' existing workflows**."

In a time when government agencies are being asked to do more with less, the team considers security intelligence to be critical in strengthening the City's cybersecurity posture, as well as protecting citizens' online safety and privacy.