esri

CASE STUDY

How Esri reduced its alert barrage, increased productivity, and reduced risk with Cortex XSOAR

paloalto NETWORKS

IN BRIEF

Customer
Esri

Country
United States

Industry
Software and geographic information systems

Challenges

- Overcome "alert fatigue" (more than 10,000 per week).
- Make up for the shortage of skilled SOC analysts (only five).
- Identify and remove duplicates and related incidents.
- Simplify a complex and distributed threat indicator management processes.

Requirements

- Decrease weekly alert volume, increase analyst productivity, and reduce organizational risk.

Solution

Esri used Cortex XSOAR to:

- Get faster closure and false positive detection with automated playbooks.
- Leverage historical cross-correlation for duplicate detection.
- Combine analyst knowledge with a collaboration window for joint investigations.

INTRODUCTION

Esri is a global organization that helps more than 350,000 customers worldwide solve challenging problems through advanced geospatial technology. With over 75% of Fortune 500 companies deploying Esri software to meet business goals, Esri needed to maintain a security posture that would protect its—and its customers'—diverse digital assets.

CHALLENGE

Esri's vast customer base and digital nature led to multiple security challenges. Over 10,000 alerts per week caused significant fatigue for five security operations analysts. Esri sought to streamline threat indicator management processes, which were distributed, complex, and not conducive to lean threat-hunting exercises. Detecting false positives and duplicate incidents amid countless attacks was one particular concern.

Suboptimal responses to these issues increased Esri's business risk, wasting resources and making managing the security operations center (SOC) more difficult.

SOLUTION

To meet these challenges head-on, Esri deployed Cortex XSOAR for security orchestration, automation, and response, in addition to its existing security information and event management (SIEM) and network monitoring solutions. To speed up incident triage and response, the team used custom playbooks that interweaved automated and manual tasks. These playbooks also codified analyst knowledge, facilitating a standardized response to specific attacks.

Cortex XSOAR enabled Esri to cut weekly alert volume by 95%, increase analyst productivity, and reduce organizational risk.

For false positive and duplicate detection, Esri used historical cross-correlation capabilities in Cortex XSOAR for false positive and duplicate detection. By quickly highlighting common artifacts and indicators across incidents, Esri analysts could spot and close duplicate attacks without spending too much time on redundant investigations.

To enhance analyst productivity and learning, Esri used the Cortex XSOAR War Room to conduct joint investigations and help cross-pollinate its analysts' skill sets. Now, able to work on complex incidents together, pull in security actions from other tools, and document results in the same window, Esri's analysts could restructure their task loads to focus on more interesting challenges.

RESULTS

Esri's application of orchestration, automation, and collaboration led to both objective and subjective improvements. Alerts went from 10,000 per week to roughly 500—a staggering 95% reduction stemming largely from swift resolution of false positives and duplicate incidents, thanks to automated playbooks and historical cross-correlation.

Moreover, Esri used Cortex XSOAR as the central hub to ingest all alerts, removing the need for analysts to visit multiple systems to find relevant information. Including ticket management in the team's incident response platform alongside automation and orchestration meant no alert could slip through the cracks at Esri to cause potential business risk.

Automation freed up the analysts' time, letting them focus on strategic tasks and continuous process improvements rather than being mired in day-to-day firefighting. Playbooks allowed them to scale their efforts effectively, enabling Esri to leverage resources more effectively to find and retain skilled analysts.

The Cortex XSOAR War Room led to increased analyst satisfaction. By automatically documenting all analyst actions, improving each other's skill sets, and giving machine learning-powered insights, the War Room empowers analysts to do more of what they do best—solve complex problems—without drowning in the documentation and menial tasks.

About Cortex XSOAR

Cortex® XSOAR™ supercharges incident response across your SOC. Reduce time spent on incidents by 90%,* eliminate busy work, speed investigations, and orchestrate across your SOC. Cortex XSOAR enriches data, improves alert triage, and automates repetitive tasks to reduce investigation time from hours to minutes.

Learn more at https://www.paloaltonetworks.com/cortex/cortex-xsoar.

*Reported time savings from aggregated customer use cases, including Palo Alto Networks SOC.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com