Navigating Rough Seas

How Esri reduced their alert barrage with Demisto

CASE STUDY: SOFTWARE

Industry

- Software/Geographic Information Systems

Integrations

- Demisto on-premise platform
- SIEM
- Network Monitoring

Challenges

- Alert fatigue (>10,000 alerts per week)
- Shortage of skilled analysts (only 5 SOC analysts)
- Detection of duplicates and related incidents
- Complex and distributed Threat Indicator Management

Solution

- Automated playbooks for faster closure and false positive detection
- Historical cross-correlation for duplicate detection
- Collaboration window for joint investigations, combining analyst knowledge

Results

- 95% reduction in weekly alert volume
- Increased analyst productivity
- Reduced organizational risk

The Customer

Esri is a global organization that helps more than 350,000 customers around the world solve tough problems through advanced geospatial technology. With more than 75% of Fortune 500 companies deploying Esri to meet business goals, it was critical for them to maintain a security posture that would protect the diverse digital assets of both the company and its customers.

The Problem

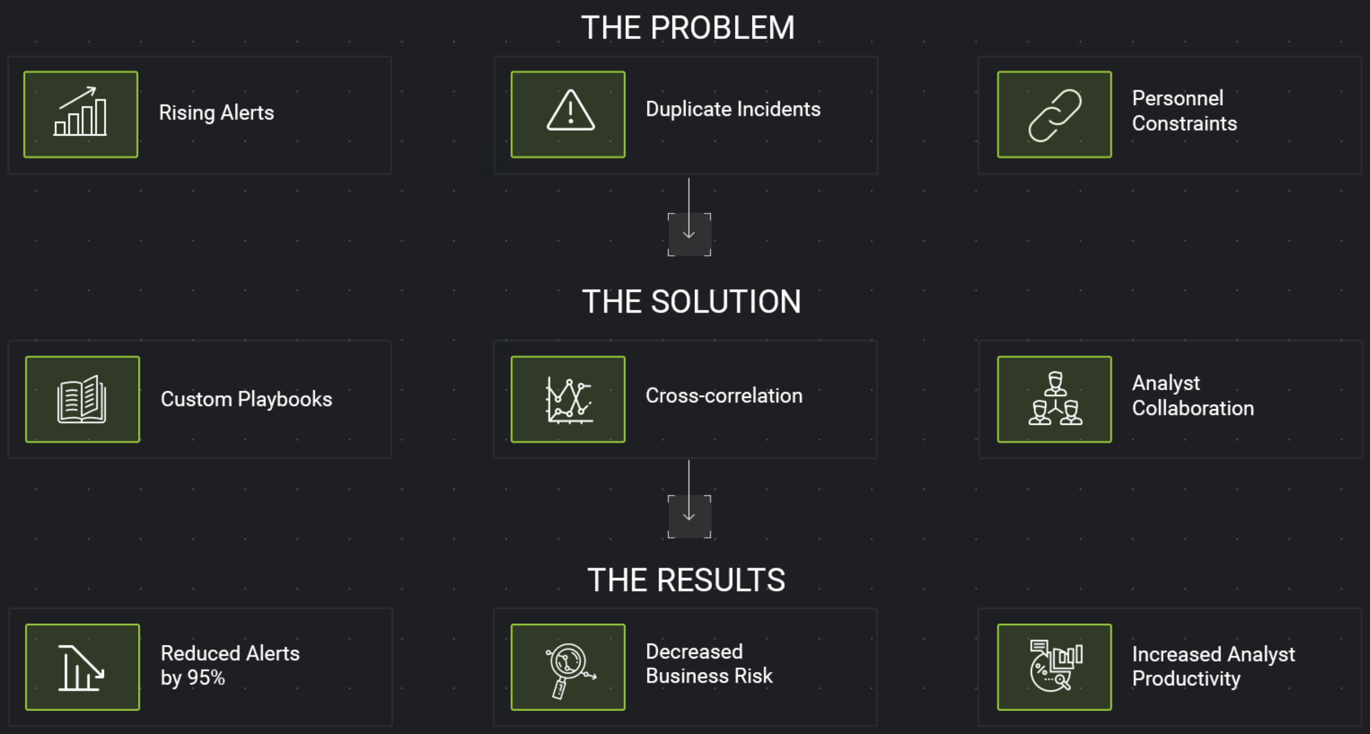
Esri's vast customer base and digital nature led to multiple security challenges. An alert volume of greater than 10,000 per week caused significant fatigue among their team of 5 SOC analysts. Detecting false positives and duplicate incidents from this host of high-quantity attacks was a specific concern that wasn't being addressed. Esri was also looking to streamline their threat indicator management processes, which were currently distributed, complex, and not conducive to lean threat hunting exercises.

Sub-optimal responses to these challenges were not only leading to an increased business risk, but were also resulting in improper optimization of current resources and SOC management.

The Solution

To meet these challenges head on, Esri deployed Demisto Enterprise in addition to existing SIEM and Network Monitoring solutions. For quickening triage of and response to high-volume incidents, they actioned custom playbooks that interweaved automated and manual tasks. These playbooks also codified analyst knowledge, enabling a standardized response to specific attacks.

For false positive and duplicate detection, Esri utilized Demisto's historical cross-correlation capabilities. By quickly highlighting common artifacts and indicators across incidents, Esri analysts were able to spot and close duplicate attacks without spending too much time on redundant investigations.



THE PROBLEM

Rising Alerts

Duplicate Incidents

Personnel Constraints

THE SOLUTION

Custom Playbooks

Cross-correlation

Analyst Collaboration

THE RESULTS

Reduced Alerts by 95%

Decreased Business Risk

Increased Analyst Productivity

For enhancing analyst productivity and learning, Esri also used Demisto's War Room for conducting joint investigations and aiding cross-pollination of analyst skill-sets. With analysts working on complex incidents together, pulling in security actions from other tools, and documenting results in the same window, their task loads were restructured to focus on the cerebral over the trivial.

The Results

Esri's application of orchestration, automation, and collaboration led to both objective and subjective improvements. Alert numbers reduced from a high of 10,000 per week to roughly 500 per week – **a staggering 95% decrease**! This decrease stemmed largely from speedy resolution of false positives and duplicate incidents due to automated playbooks and historical cross-correlation.

Moreover, Esri now used Demisto as the central hub to ingest all alerts, precluding analysts from visiting multiple systems to get relevant information. Including ticket management in their IR platform, in addition to automation and orchestration,meant that NO alert slipped through the cracks at Esri and caused potential business risk.

The automation also freed up analyst time; they could now focus on strategic tasks and continuous process improvements rather than be mired in day-to-day firefighting. The playbooks also allowed them to scale their efforts effectively, enabling Esri to leverage the toughest resource to find and retain – skilled analysts.

Demisto's War Room led to increased analyst satisfaction. By automatically documenting all analyst actions, allowing them to improve each other's skillsets, and giving machine learning powered insights, the War Room lets analysts do more of what they enjoy – solving problems without drowning in documentation and menial tasks.

"The automation infused into our security infrastructure by Demisto complements our existing SIEM, allowing our SOC team to realize greater efficiencies. Automating these mundane tasks allows our analysts to focus on decision making."

Sean Kohlmeier,

Incident Response Lead, Esri