DEMISTO
A PALO ALTO NETWORKS® COMPANY

Keeping the SOC Lights On

How an Electric Utility company used Demisto to optimize their security analyst team.

CASE STUDY: ENERGY CUSTOMER

Industry

- Energy/Electric Utilities

Integrations

- SIEM
- Forensics & Malware Analysis
- Ticketing
- Data Analytics

Challenges

- High volume of alerts
- Detection of duplicates and related incidents
- Case management/ticketing tasks a time-sink

Solution

- Automate duplicate alert detection and consolidation
- Orchestrate workflows across products on one platform
- Correlate threat intel from multiple sources including open source tools
- Detect similarities between cases for better insights and training opportunities
- Accelerate case management reporting

Results

- 30% reduction in case volume resulting in approx 1 analyst FTE time savings
- Deploy aggressive detection without negatively impacting analyst workload
- Case management information in one place speeds monthly risk audit reporting

The Customer

One of the largest Electric Utility Companies providing energy related services to the US. Aggressive detection was a priority for this company's SOC team but they also wanted to ensure their security analysts were not spending inordinate amounts of time investigating duplicate alerts.

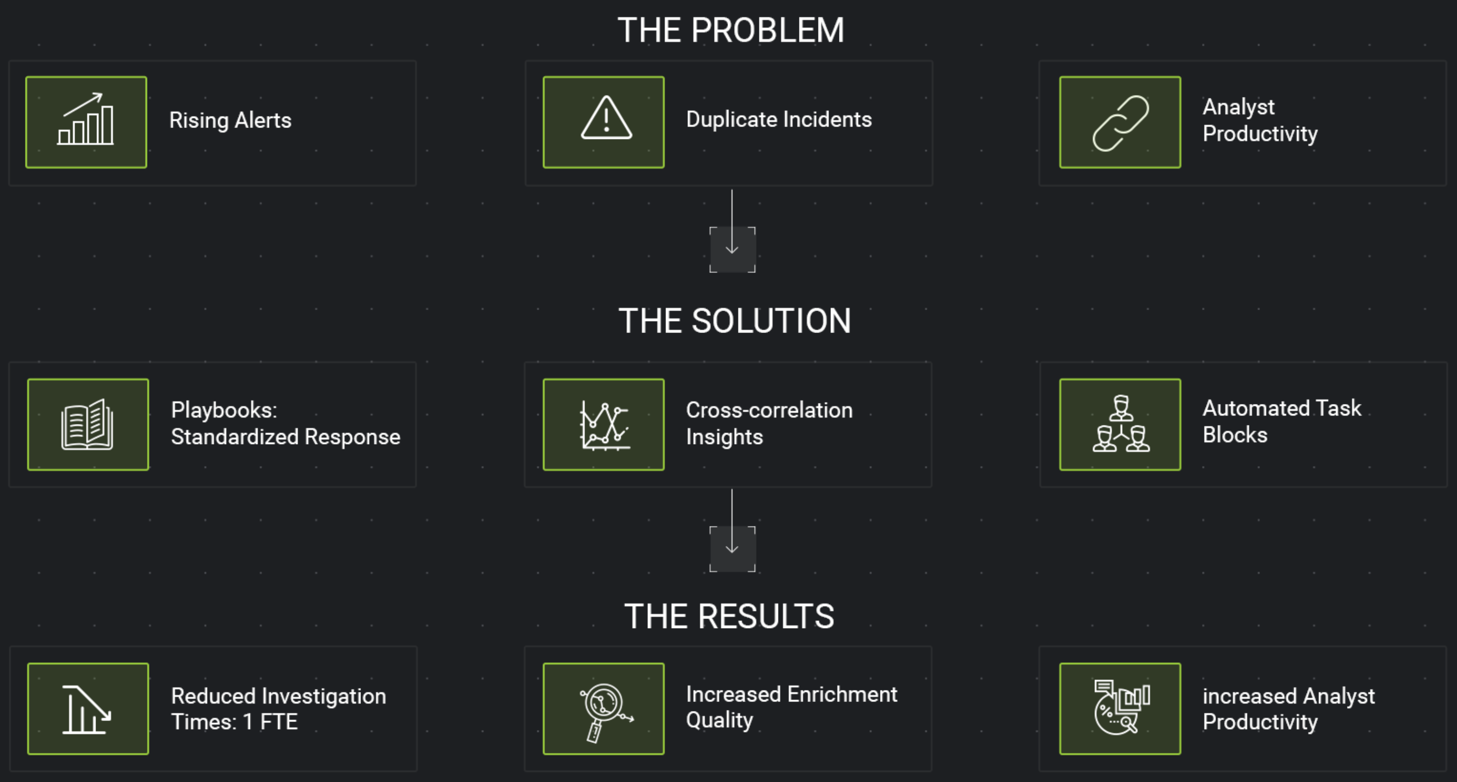
The Problem

The SOC team also had a mix of ingestion and detection sources to deal with, ranging from security vendor products and open source platforms to in-house tools and proprietary solutions. While they had a SIEM to aggregate logs, their analysts were frustrated because they spent a great deal of time investigating duplicate alerts instead of hunting threats. Case management was also bogged down with the need to pivot between multiple screens, often resulting in the analysts cutting and pasting information manually. In addition, there was a lot of chasing down of analysts at the end of each month to get case details for case management reports. These low level tasks prevented analysts from focusing on interpretation of data and problem solving, which ultimately led to longer resolution times and decreased productivity.

The Solution

The SOC team first deployed Demisto playbooks to identify and remove duplicate alerts generated by their cybersecurity tools. The team also leveraged Demisto to automate case metrics tracking and reporting. With the expanded visibility across cases, the team was able to derive similarities and surface trends that were available before to them. As analysts tracked their actions within Demisto, this facilitated monthly risk audit reporting since case data and analyst actions were now archived and easily retrievable from one location. This common knowledge repository provided smoother transition of knowledge between analyst shift changes and served as a training resource for lower level analysts.

The case management lifecycle managed within Demisto includes ticketing. By automating and integrating the ticketing process, the SOC managers hope to free up analysts from doing "stupid stuff" such as manual transcription (copy and pasting) of information from one system to another, so they can focus on threat hunting and decision-making.



THE PROBLEM

Rising Alerts

Duplicate Incidents

Analyst Productivity

THE SOLUTION

Playbooks: Standardized Response

Cross-correlation Insights

Automated Task Blocks

THE RESULTS

Reduced Investigation Times: 1 FTE

Increased Enrichment Quality

increased Analyst Productivity

As the SOC team is very focused on metric data-driven decisions, there are plans to integrate Demisto with their in-house visualization platforms for advanced reporting and insights.

The Results

Demisto enabled the SOC team to be as aggressive as they needed to be in their alert settings without worrying about impacting analyst workload. As a result of automating deduplication efforts, the SOC team was able to realize alert reduction of 30% within the first month of operation. This netted out to a full analyst FTE in time savings.

An added benefit from using Demisto was in the area of metrics. As a user of SIEM knows, the process of extracting metrics from a SIEM to identify similarities across cases can be onerous. The SOC team was able to leverage Demisto playbooks to automate some of these tasks to gain previously undetected insights into problem areas related to people, processes, and technology.

For example, they were able to discover multiple malware cases associated with a specific machine or user account. This was an unexpected benefit with the expanded visibility into their case related metrics. As the SOC team builds out their automation efforts, the goal is to map alerts and threat behavior to the MITRE ATT&CK framework to better understand security risk against adversarial threat behavior, to aid in planning better defenses and verifying the effectiveness of existing defenses.

> *“We are very aggressive in prioritizing alerts. A shortfall of SIEMs is when you get too granular with alerting, you also get the volume that is too taxing to handle manually. With Demisto, we were able to gain value for being aggressive but don’t lose value for being aggressive because Demisto helps you manage it.”*