Chronicle SOAR

Hitting Send on SOC Efficiency

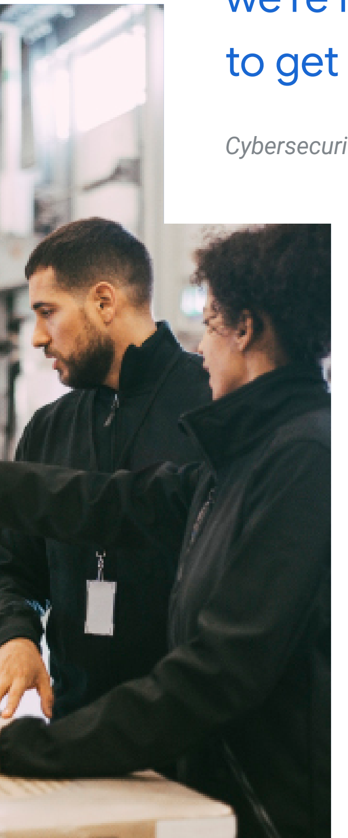
How one of the world's largest shipping companies turned to SOAR to shrink threat response times and demonstrate security value to stakeholders.

Not uncommon among large corporations, this multinational delivery services organization had alerts coming in from disparate sources and lacked the context required for analysts to accurately assess certain threats within a reasonable timeframe.

As a result, the organization needed a product that consolidated and delivered alerts with greater context and enrichment, while the executive team sought productivity metrics to determine how efficiently the security team is mitigating potentially costly incidents.

> Now, I have a single place where all of my learning comes in and I can document accurately and provide metrics from a performance standpoint to say, 'Here's how fast we're getting to threats and how quickly we're remediating them and how efficiently the analysts are working to get from the different phases of their investigation.."

Cybersecurity Command Center Manager, Delivery Services Organization



Challenges

Receiving alerts from disparate detection systems was wreaking havoc on the organization's security team when it came to detecting threats and accurately prioritizing their severity. Analysts were forced to manually tap into different tools to obtain the context they needed to apply to each alert. The environment was challenging and not efficient.

On top of that, managing a large multi-vendor security stack made it difficult to consolidate data and make sense of it. Without having visibility into potential process bottlenecks, the security team was unable to determine which investments could deliver improvement.

Alert Overload
Flood of alerts from increasing number of detection technologies

Tool Expansion
Disparate tools across the SOC that rarely work

Visibility
Slow, inconsistent process for incident response with little to no productivity metrics

Chronicle SOAR

Solutions

Knowing it needed a solution that would help its analysts first and foremost, the organization focused on tools that would increase efficiency in the SOC while maintaining its large security stack.

Now, alerts arrive with adequate context and enrichment to enable rapid triage, allowing threats to be escalated based on their possible impact to mission-critical assets. Automated playbooks are initiated to ensure repeatable processes are in place when responding to specific use cases like phishing, malware or ransomware.

The shipping organization identified Chronicle SOAR as a way to ensure analysts are getting the help they needed by consolidating all relevant information into a single workbench and delivering robust reporting to senior leaders.

Wins

The organization's analysts are now managing alerts that arrive with the fidelity required for them to reach mitigation quickly. A fully integrated security tech stack allows analysts to easily access information across domains, while displaying the metrics the executive team cares about. Their SOC can now continuously communicate and document its risks and responses.

> “I really wanted to choose a product that had the analyst in mind and was analyst driven.”
>
> *Cybersecurity Command Center Manager, Delivery Services Organization*

Automation is a force multiplier

Analysts now receive alerts with the context that it would have taken them 30 to 45 minutes to acquire previously.

The glue that binds the security stack

The SOC can now continuously communicate and document risks and responses.

Machine learning prioritizes the important stuff

The security team can close critical cases faster.

Improved ability to capture metrics

Alerting is now collected, and response actions are executed from a single product.