DEMISTO

Clearing Digital Battlefields

How a top tech company's investigation speed surged with Demisto

CASE STUDY: APPLICATION DEVELOPMENT

Industry

- Application Development

Integrations

- Demisto Enterprise
- Endpoint Monitoring
- Network Detection
- Log Collectors
- User Login Tools

Challenges

- Growing alert numbers
- Small IR team and fast-growing company
- Coordinating among multiple security products
- Growing no. of network sensors in remote locations

Solution

- Playbooks as single source of truth for investigations
- Playbook task-blocks to reduce need for cycling between screens and systems
- Repetitive task flows now handled by automated computing power

Results

- Reduced investigation times (from 4 hours to 10 minutes)
- Richer incident context at analyst fingertips
- Leaner security operations

The Customer

The customer is a technology company with worldwide operations spread across multiple spheres of application development. Juggling multiple business units, the customer must facilitate a high volume of users and maintain a security posture robust enough to guarantee the integrity of the users' personal and financial data.

The Situation

For the customer, fast business growth engendered a rise in security challenges. The incident response team faced a growing number of network sensors in remote locations that, coupled with limited personnel, resulted in a mushrooming of security alerts.

The analysts also found it time-consuming to repeat the same sequence of manual tasks for each incident – a sequence that usually involved straddling across screens and security products. These menial tasks prevented analysts from lending focus to interpretation of data and problem solving, which ultimately resulted in arduously long resolution times.

To meet and vanquish these challenges, the analysts needed a security operations toolkit in addition to traditional SIEM logging and event correlations.

The Solution

The customer deployed Demisto Enterprise as a connective security fabric for its products and teams. By using Demisto as a common layer across a host of tools such as user login, endpoint monitoring, network detection, and log collection, analysts were able to harmonize actions across platforms without needing to switch screens and chasing fragmented information.

By creating formalized playbooks and automating quantity-heavy action blocks, analysts ensured that there was a single source of truth for security investigations within the SOC. Automation also meant that hitherto laborious tasks – like scouring log sources for relevant entries – could be distilled into sub-playbooks that analysts could chain together with a few values and clicks.

The Results

The most tangible benefit was an exponential decrease in investigation times for analysts. One common incident type that took analysts 4 or more hours to get through before Demisto's deployment, now reduced to an average of 10 minutes – **a 95% decrease in investigation time!**

This decrease in time was accompanied by an increase in enrichment quality. By quickly gathering and cross-referencing data across a host of sources, Demisto playbooks provided rich context that analysts could use for faster resolution.

Demisto also helped the SOC extract maximal value from existing security products. By coordinating actions across products and automating repetitive task blocks, analysts could leverage the product stack without an increased rate of error, stress, or dead time.

Thus, Demisto freed up the analysts' time to focus on more mission-critical objectives, benefited SOC managers through increased workforce productivity, and helped security heads realize lower business risk and higher return on security investments.

"Demisto enables analysts to automate and string together security actions across our entire product stack in one workflow window. This eliminates dead time and provides us with the needed context for faster incident resolution."

– Senior Incident Response Engineer