DEMISTO

Cutting Through the Noise

How telecom company used Demisto for automated malware analysis and response

CASE STUDY: TELECOM

Industry

- Cellular/Telecommunications

Integrations

- SIEM
- Threat Intelligence
- Email Listener
- Behavioral Analytics

Challenges

- Lack of defined SOC team
- High weekly alerts
- Connecting disparate teams (production, security, development)
- Open tickets, long response times

Solution

- Playbook for automated malware analysis and response
- Ingestion of security intelligence across sources for centralized context
- War Room for team collaboration and information visibility

Results

- Faster response times through automation of repeatable tasks
- Cross-team coordination and improved team accountability
- Increased response efficiency through single-console investigations

The Customer

A leading telecommunications company that provides cellular, internet, and OTT TV services as well as infrastructure hosting services for businesses. With the data of over 2.8 million subscribers at stake, it was critical for the customer to protect their digital and infrastructure assets from compromise.

The Situation

Because of the customer's broad range of services, security was (and continues to be) a multi-team effort. It was a challenge to coordinate between security, development, and production teams, both for regular security operations and incident response. This situation was exacerbated by the lack of a defined SOC team, resulting in high daily alerts (around 100) and 'dead time' during incident handoffs.

The customer's security teams also had a variety of ingestion and detection sources to deal with. While they had a SIEM to aggregate logs and machine data into alerts, some incidents also flowed in via mailboxes where employees forwarded suspected phishing emails. This resulted in the lack of a single console to view alerts and execute response at scale.

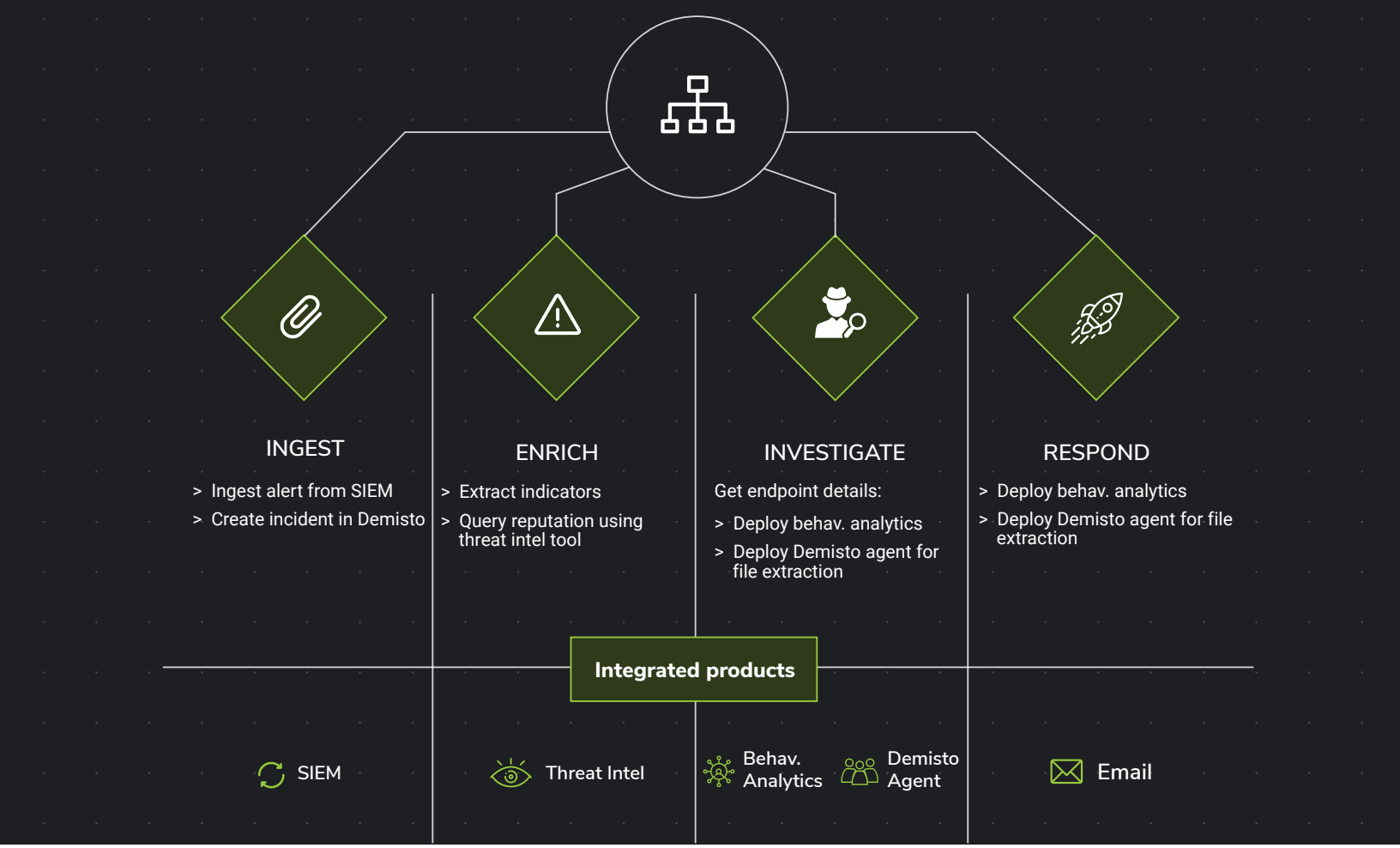
The Solution

The customer solved these challenges by deploying Demisto Enterprise in addition to their existing SIEM, threat intelligence, email, and behavioral analysis solutions.

Ingestion across sources: Since Demisto's orchestration allowed for ingestion of alerts across sources, the customer was able to direct alerts both from its SIEM and mailboxes into Demisto's console for single-window visibility, triage, and response.

Malware enrichment and response playbook: The customer deployed a custom playbook that coordinated across a range of products for automated malware enrichment and response.

The playbook receives alerts from the SIEM and runs initial threat intelligence actions to get IOC reputation. It then retrieves endpoint details using integrations with relevant tools, runs both behavioral analytics using a customer-owned custom tool, and deploys Demisto's dissolvable agent on infected endpoints. These actions help extract a wealth of data from the endpoint – such as file details and memory dumps – and bring it to Demisto for the security team's perusal.



Team coordination: To address team coordination, the customer utilized Demisto's 'War Room' to great effect. The War Room provided a platform where cross-functional teams could view playbook task results, collaborate on plans of action, and run security commands in real-time.

The Results

No SOC team, no problem: Playbooks – such as the malware enrichment case discussed in this document – helped automate hitherto time-consuming tasks and freed up analyst time by providing them with rich information for problem-solving. Codifying a sequence of steps helped the entire team stick to a response quality benchmark and onboard to use cases quickly.

Cross-team collaboration: Using the War Room for incident investigations improved team coordination and productivity, preventing the need to maintain disparate threads of communication across emails, tickets, and so on. Moreover, since participants worked on a common window, it was easy to impart visibility and assign accountability when required.

Faster response: Demisto provided the central console where incidents from multiple sources could be ingested. Multiple attacks belonging to common campaigns could be identified as related incidents within Demisto, further sanitizing and enriching the alert queue so that security teams can respond to incidents faster.

"We've been using Demisto for almost two years now. The platform has threaded together our security systems, enabled different teams to collaborate, and continuously onboarded new features to help us resolve incidents faster."

– CSO, Telecom Customer