Customer Story

Hunt & Hackett

Seeking Flexible NDR for an Advanced MDR Solution

Hunt & Hackett is a fast-growing Dutch security service provider based in The Hague, The Netherlands. Founded in 2020, Hunt & Hackett protects their customers against the specific threat landscape based on the needs of each organization and sector.

By deploying a managed detection and response (MDR) framework, Hunt & Hackett monitor the security assets of the client organization 24/7 to protect them from even the most advanced threat actors.

Their cloud-native MDR service delivers threat monitoring, detection, and automated response to organizations by using an in-house, Security Operations Center (SOC) where their security experts combine threat intelligence, data-driven analytics and human expertise for the strongest detection and response strategies.

Hunt & Hackett's SOC analysts combine cloud-based and on-premise operations to function as the organization's primary line of defense against digital threats.

SNAPSHOT

Organization type: Managed Security Service Provider

Location: The Hague, The Netherlands

Industries Served: Agriculture, Energy, Manufacturing, Maritime, Logistics

Top challenges: Introduce a flexible NDR into their security stack that is suitable for both IR and MDR-services and could easily integrate with their SOAR and SIEM, while also maintaining high-level support and management.

Solution: Stamus Security Platform (SSP)

They incorporate a broad range of data sources such as network, logs, cloud, and endpoint to adapt to an organization's existing security set-up and to provide the optimum visibility across their client's unique threat landscape. Their clients operate in critical industries – such as agriculture, (renewable) energy, maritime, manufacturing, logistics, and technology – that commonly face targeted attacks.

These organizations are typically not large enough to afford an in-house 24/7 SOC, and yet they still need effective cybersecurity practices. Despite a lack of in-house security resources, these clients must manage and mitigate cybersecurity risk.

In building its security tech stack from scratch, Hunt & Hackett selected Chronicle, a cloud-native security information and event management (SIEM) platform from Google in combination with the Cortex XSOAR from Palo Alto Networks, a security orchestration automation & response (SOAR) platform.

Together, these platforms enable Hunt & Hackett to consume and analyze high volumes of security telemetry data while scaling their workloads dynamically. Hunt & Hackett does not typically select the endpoint detection and response (EDR) technology, because most clients already deployed some form of endpoint technology.

TECH STACK

Cortex XSOAR from Palo Alto Networks

Chronicle SIEM from Google

Various honey pots

Endpoint detection and response (EDR) supplied by client

Network detection and response (NDR) by Stamus Networks

Additionally, the firm makes extensive use of honeypots and tokens in their MDR technology stack. Network monitoring is provided with technology from Stamus Networks and is typically deployed for organizations with significant on-premise IT, remote locations and/or with in-house data centers.

Hunt & Hackett had the unique opportunity to select every system in their MDR security technology stack.

With some of their key team-member's having a background pioneering SOC & NDR-solutions in Europe, they initially sought to create their own proprietary network detection and response (NDR) platform. But because the ongoing development and maintenance of these systems can become very expensive and time consuming, the team at Hunt & Hackett began to search for a commercial solution that would fit their unique requirements.

They needed an NDR platform that would integrate with Chronicle and Cortex XSOAR while also allowing them to customize detection and operational elements.

CHALLENGES

First and foremost, Hunt & Hackett needed an effective network-based threat detection system that would complement their other sources of detection. The team understood that an organization's network is a powerful resource for security operations, as nearly all cyber threats generate communications that can be observed on the network.

And with the right system in place, they could more completely uncover serious and imminent threats to their clients' organizations.

They required a network-based threat detection system that could seamlessly integrate into the new architecture that formed the foundation for their incident response (IR) and MDR services. This foundation includes a commitment to an infrastructure as code (IaC) automation process which helps H&H manage and provision their vast systems using machine-readable definition files, rather than the usual interactive configuration tools.

SUMMARY OF NEEDS

Needed a simple, seamless integration with tech stack

Preferred a Suricata-based system

NDR must be flexible enough to manage both on-prem and cloud appliances

Required rich API for integration

Needed special support and management considerations

Required flexibility in billing structure and true partnership with suppliers

Additionally, they preferred an NDR solution that was based on Suricata. Hunt & Hackett had familiarity with Suricata as a highly capable IDS solution, so searching for an NDR that used Suricata-based detection and signature syntax was a necessity.

The challenge was finding a Suricata-based NDR that would provide them with high-confidence notifications that could trigger an immediate response in their Cortex XSOAR system while automatically generating enriched IDS logs for their SIEM. The solution also needed to fit an infrastructure-as-code architecture so it can be rolled out in a largely automated fashion.

Because they needed seamless integration, a full-featured API was a requirement for the Hunt & Hackett team. The desire for application connectivity and fluid data transformation resulted from the need for systems to function as intended regardless of the deployment.

The API needed to accommodate custom rules from the Hunt & Hackett detection pipeline. With some appliances being on-premise, others in the cloud, and their SOC analysts often working on networks from remote locations, Hunt & Hackett needed to ensure that the communications between systems was always secure and reliable.

Another unique challenge Hunt & Hackett faced while searching for a NDR solution was the need for a partnership based on the unique needs of an MSSP/MDR service provider. Many large NDR vendors could not commit to a true working partnership with the Hunt & Hackett team. They needed an NDR partner who would work with them to understand their requirements and solve any issues that arose as the deployment evolved, allowing new clients to be on-boarded quickly.

SOLUTION

Hunt & Hackett chose the Stamus Security Platform (SSP) as the network security solution for their services. The platform from Stamus Networks is an advanced network-based threat detection and response (NDR) solution that exposes critical threats against an organization by analyzing network traffic using multiple detection engines and providing response-ready and high-fidelity threat detection.

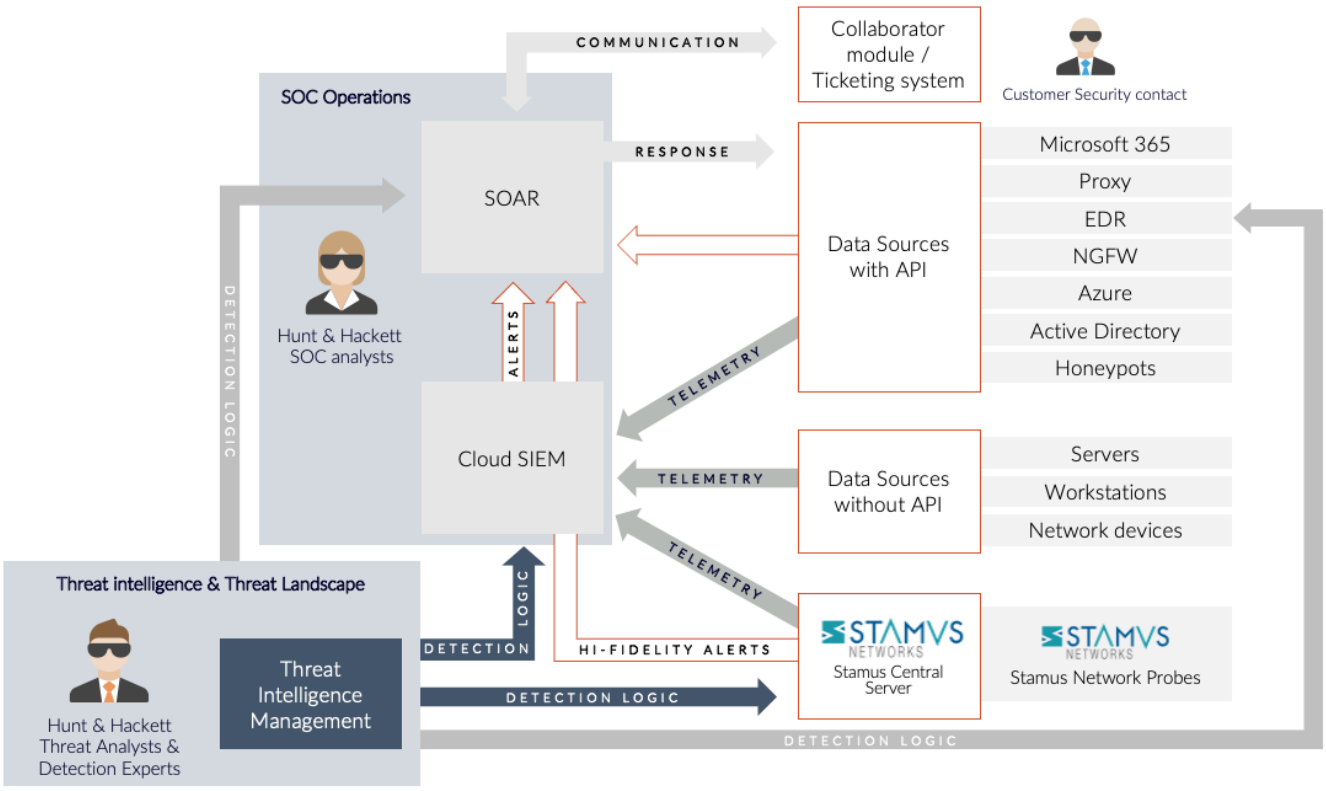
SSP provides explainable and transparent results with evidence, automatically escalating only the most serious and imminent threats to the analyst or incident response system.

Other related file, packet capture, flow, and protocol events, produced by the embedded Suricata engine, are available for review as evidence during an incident investigation or a threat hunt.

Because SSP is built with open interfaces, it integrates easily with other platforms. For Hunt & Hackett, this made for a relatively easy integration to their Google Chronicle cloud-native SIEM, detection pipeline and their Cortex XSOAR.

The Stamus Central Server can run in the cloud, which was ideal for Hunt & Hackett's needs. Flexible deployment options and open interface allows SSP to operate in nearly any environment.

Additionally, SSP operates seamlessly in both cloud and on-premise environments, allowing Hunt & Hackett to maintain efficient and effective threat detection regardless of their customers' probe set-up.



For Hunt & Hackett's flexible service deployment model, the Stamus Security Platform built-in VPN was an important capability. This enables remote network probes to be securely connected to the central server, supporting a variety of deployment architectures.

In addition, the API allows Hunt & Hackett to access the SSP data from multiple systems. Finally, automated Webhook push notifications to the SOAR enable the Hunt & Hackett SOC analysts to react to high fidelity, high confidence Declarations of Compromise™ with context, from multiple organizations at once, ensuring fast response times.

To address the Hunt & Hackett billing challenges, Stamus Networks was able to offer Hunt & Hackett a fitting billing plan addressing their unique requirements as a managed security service provider (MSSP). This made for a mutually beneficial relationship between the two companies.

> *The Stamus Networks team provided extensive technical support and made the adoption of the platform as painless as possible. This is not something to take for granted.*
>
> - Joost Bijl, product manager at Hunt & Hackett

The Stamus Networks team partnered with Hunt & Hackett to ensure that all systems integrated effectively, and we continue to maintain a strong support relationship. Ultimately, it was this partnership that drove Hunt & Hackett to select the Stamus Security Platform for their MDR service offering.

OUTCOME

The Stamus Security Platform gives Hunt & Hackett SOC analysts greater visibility into their client's networks, ultimately detecting more threats, reducing their time to respond, and mitigating the client's risk.

The platform gives Hunt & Hackett to have everything they wanted in a network detection and response (NDR) solution without making sacrifices in their service capabilities. The flexibility of SSP has allowed them to cherry pick the systems in their security stack without fearing their NDR solution will have difficulty communicating across platforms.

The Stamus Networks team partnered with Hunt & Hackett to ensure that all systems integrated effectively, and continues to maintain a strong support relationship

Hunt & Hackett has been able to grow and scale their business while continuing to include highly effective network security as an important part of their service portfolio.

> *We built our managed service's network detection on Stamus Security Platform because we can depend on it for highly accurate detection and to gather the evidence needed for a detailed incident investigation. Stamus Security Platform is easy to setup, use and integrate. It provides actionable insights into what's going on in the network, completing the visibility picture.*
>
> - Joost Bijl, product manager at Hunt & Hackett

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As organizations face threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. The global leader in Suricata-based network security solutions, Stamus Networks helps enterprise security teams know more, respond sooner and mitigate their risk with insights gathered from cloud and on-premise network activity. Our Stamus Security Platform combines the best of intrusion detection (IDS), network security monitoring (NSM), and network detection and response (NDR) systems into a single solution that exposes serious and imminent threats to critical assets and empowers rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com