CUSTOMER CASE STUDY:

Blackhawk Network Holdings

ANOMALI®

BLACKHAWK NETWORK

> *Anomali enabled us to spend less time dealing with noise, and more time focusing on critical issues.*
>
> *– Devin Ertel, CISO, Blackhawk Network Holdings*

CHALLENGE

Blackhawk Network Holdings threat intelligence was the result of a combination of tools pieced together, none of which were integrated with their SIEM implementation, or provided enough context around IOCs to understand their potential impact.

Blackhawk Network Holdings needed a way to easily investigate potentially risky alerts without having to log in to multiple security product dashboards, reduce their manual overhead requirements, and maximize their resources so their analysts could better focus on critical issues.

SOLUTION

Anomali® ThreatStream® offered Blackhawk Network Holdings a way to sync actionable threat intelligence with their SIEM alerts, integrate disparate threat feeds into one single-view dashboard, and provide the context around IOCs necessary to understand their true importance.

RESULTS

- Single dashboard and consolidation of all threat intelligence feeds
- Seamless SIEM integration
- Sandboxed testing environment to detonate payloads
- Improved threat analysis and response times
- More efficient and effective workflow
- Reduced false positives by over 95%

OVERVIEW

Blackhawk Network Holdings Inc. is a privately held company that operates in the prepaid debit card, gift card, and payments industries. Blackhawk Network Holdings' network is wide and diverse, reaching people through a number of different channels including in-store and online and mobile purchases. In essence, they operate like an online merchant, a physical store, and a bank all at once. The very nature of their business, and the large amount of financial information they process, make them a natural and frequent target for financially motivated attackers.

Before Anomali, Blackhawk Network Holdings relied on a variety of different security tools to manage their threat intelligence—a task they found extremely challenging. Like many organizations, they leveraged their security information and event management (SIEM) system to correlate events and help their analysts stay on top of trends. The problem was they had several systems in their IT environment that provided outside threat intelligence, each with its own portal and own dashboards. None of the systems integrated directly with their SIEM or communicated with each other. And the information was often duplicated or even worse, in disagreement. That meant whenever their SIEM pointed to a threat indication, their security analysts had to spend an inordinate amount of time analyzing and verifying indicators of compromise (IOCs) related to outside IP addresses. Thousands of alerts a day were more than the team could manage, let alone respond to.

Blackhawk Network Holdings wanted to simplify their threat intelligence processes so their analysts could focus more on forensics and remediation and less on research, management, and manual correlation. And they wanted to understand not just the type of attacks they were seeing, but the context of who their attackers were. They wanted a tool that could move their security forward but could also integrate with their current processes.

THE ANOMALI SOLUTION

Blackhawk Network Holdings deployed Anomali ThreatStream, giving them an immediate threat intelligence solution via four key benefits:

1. Consolidation:
   ThreatStream consolidated all of Blackhawk Network Holdings' sources of threat information into one dashboard view within their SIEM, reducing duplicated information and false positives. In turn, they were able to minimize much of their security team's manual overhead, allowing them to focus on resolution and not research.
2. Integration:
   ThreatStream integrates directly into Blackhawk Network Holdings' SIEM, so analysts do not need to reroute their analysis process and can do their early investigation from there.
3. Correlation:

   ThreatStream gave Blackhawk Network Holdings a way to correlate actionable threat intelligence SIEM alerts within their SIEM. ThreatStream tells analysts the threat score for each IP address, along with the confidence level based on a reputation ranking of its maliciousness.

> *Unless we know who is after us, alerts lack context without Anomali.*
>
> *– Devin Ertel, CISO, Blackhawk Network Holdings*

4. Detonation:

   ThreatStream enables analysts to replay executables in a sandboxed environment, giving them a safe place to test and a way to perform early analysis of potential IOCs and threat indicators.

> *When a suspicious email comes in, we can detonate it in a sandboxed environment to see if it's a threat. We couldn't do that before.*
>
> *– Pablo Vega, Principal Security Engineer, Blackhawk Network Holdings*

> *"Before Anomali, we had tons of information without context. We had to look through thousands of alerts quickly just to see what stood out and then react to those."*
>
> *– Devin Ertel, CISO, Blackhawk Network Holdings*

THE ANOMALI IMPACT

ThreatStream gave Blackhawk Network Holdings the key capabilities and threat intelligence context that allowed their analysts to shift from searching through emails and dashboards to verify alerts to focusing on critical threats and issues.

With ThreatStream, Blackhawk Network Holdings has higher confidence that critical alerts are malicious and not false positives. ThreatStream has provided them with greater visibility into what threats they confront. And since false positives have been very low in both number and criticality, *analysts have been spending less time chasing non-existent problems and more time focusing on solutions.*

The value of ThreatStream is in the *time it saves analysts and the opportunity they have to address more threats than they once could*. Because the tool automatically handles a large analytical workload, Blackhawk Network Holdings was able to increase capacity without having to hire additional staff.

ThreatStream has been an incredible solution for Blackhawk Network Holdings, allowing them to maximize resources and focus on the threats that matter most. ThreatStream gives Blackhawk Network Holding the ability to curate and filter the information they need from all of their sources of threat intel. And they've been able to apply ThreatStream security context around their alerts, helping to separate the high priority threat intel from low priority alerts to improve their overall security posture.

LONG TERM SUCCESS

Blackhawk Network Holdings is now looking at integrating Anomali ThreatStream intelligence context into more internal security tooling, giving them the potential to automatically respond to threats with very high malicious confidence ratings. Blackhawk Network Holdings is interested in expanding their capabilities with Anomali Match™ and Anomali Lens™.