ANOMALI®

Global Manufacturing Company

Company Restructures Threat Intelligence Program, Reducing Time Needed to Detect and Respond to Threats

CHALLENGE

To better detect and respond to cyber threats, this consumer foods manufacturing company had built an impressive defensive capability made up of a cyber operations center, cyber incident response team, and multiple platforms. Despite being well positioned to confront the modern attack environment in principle, to be effective the company discovered it still needed to further reduce the time it took to detect and respond to adversaries, more accurately identify the threats relevant to its business and industry, and reduce the volume of false positives it was chasing down.

SOLUTION

By leveraging Anomali ThreatStream via Verizon Threat Intelligence Platform Services (VTIPS), the company has cut the amount of time it takes to detect and respond to threats from several days to mere hours, been able to focus on the adversaries that are most relevant to its business, and reduced significantly the number of false positives it devotes resources towards.

RESULTS

- Broader threat visibility
- Immediate detection
- Faster investigations
- Automated threat blocking

> *The time needed to conduct an investigation decreased by 40 percent*

> *"We turned to Anomali to help us build a threat intelligence program that would strengthen our ability to know when we are being attacked and to then make smarter decisions about how to respond."*
>
> *– Senior Manager, Cybersecurity*

OVERVIEW

This company is a top producer of retail food products sold in consumer markets across approximately 90 countries, with brands that are high-visibility household names. Its annual revenues exceed €2.8 billion, it employs approximately 4,000, and operates more than a dozen global manufacturing facilities. All of these characteristics combine with a complex global supply chain to make it a prime target for threat actors looking for opportunistic ways to monetize cybercrimes, and steal data and IP. To defend itself, the company invested in a strong mix of solutions and talent, but soon realized that the only way to remain ahead of the threats it faced was to further augment its capabilities in order to detect and respond faster and more efficiently.

SECURITY SITUATION

With its existing security solutions, the cyber operations center and cyber incident response team found it needed up to four days to determine if a threat was genuine, what level of risk it presented, and to then respond. This process was too slow and was further exacerbated by the frequency with which, at the end of the investigative trail, a threat turned out to be either irrelevant or a false positive.

It soon became clear that the threat intelligence lifecycle process was broken. The company could reach an actionable conclusion, but the amount of time and resources needed to figure out if a threat was real left it exceedingly vulnerable to malicious actors. The company then took a hard look at how it was collecting, analyzing, prioritizing, and responding to incidents taking place in its environment.

> *"The only way to prevent your business from becoming the victim of an advanced cyberattack is to have technologies in place that give your team the power to execute."*

THE ANOMALI SOLUTION

The company turned to Verizon Threat Intelligence Platform Services (VTIPS), which helped it to deploy a new threat intelligence lifecycle capability built on Anomali ThreatStream, the market leading threat intelligence platform (TIP), and Anomali Lens, an automated threat knowledge tool that uses NLP to convert any web-based threat content into actionable intelligence.

With Verizon and Anomali, the company was able to start executing in a very short period. TIP deployment was fast, threat feed aggregation was easy, and IOC collection began almost immediately. The company's analysts soon found that they were conducting faster investigations and creating threat intelligence that could be operationalized into existing security controls for automated detection and blocking across their security infrastructure.

In the manufacturing sector, some threats are of more concern than others. The prospect of not being able to respond quickly to ransomware campaigns or attacks on industrial control systems is among the things that keep its security team up at night. Missing critical attacks such as these could cause operations to come to a standstill.

> *"With Anomali we can do things like create custom rules for ransomware and other specific threats. Critical features such as these allow us to remain focused on what we need to track and to act on the highest-priority incidents."*

THE ANOMALI IMPACT

Prior to Anomali, the cyber operations center and cyber incident response teams needed as long as four days to detect, respond, and take action to address threats. It now takes only a few hours to detect, analyze, investigate, and then operationalize intelligence downstream to security controls. With a reduction in false positives, productivity levels have further increased.

> *"Anomali has exceeded our expectations and vastly improved our ability to remain protected against advanced threats. We are especially pleased with its capacity to scale, which will allow us to maintain a secure posture as we continue to grow our business."*

There are many specific performance improvements the company has experienced:

- The time needed to conduct an investigation has decreased by 40 percent.
- The ability to block malicious IOCs has reduced significantly the risk of falling victim to a ransomware attack.
- Threat intelligence integration into security controls has been broadened to include Zscaler, Crowdstrike, and Windows Defender Advanced Threat Protection (ATP).
- The ease by which sandboxing is supported further increased the speed at which malware analysis is performed.

ABOUT ANOMALI

Anomali is the leader in intelligence-driven cybersecurity. More than 1,500 public and private sector organizations rely on Anomali to see and detect threats more quickly, reduce the risk of security breaches, and improve security operations productivity. Anomali solutions serve customers around the world in nearly every major industry vertical, including many of the Global 2000. As an early threat intelligence innovator, Anomali was founded in 2013 and is backed by leading venture firms including GV, Paladin Capital Group, In-Q-Tel, Institutional Venture Partners, and General Catalyst. Learn more at www.anomali.com.

ANOMALI®