Successful Gigamon ThreatINSIGHT Integration With StrikeReady Prioritizes Alerts and Enriches Investigations for Insurance Provider

> The integration between ThreatINSIGHT and StrikeReady makes our life easier, and I think it's a killer combination."
>
> ADIL MUFTI
> Senior Director for Global Security Operations at CNA

CHALLENGES

+ Lack of ability to test the security stack
+ Excessive time spent parsing through noise and a lack of prioritization of alerts
+ Inability to push remediations within the same console, negatively impacting operational and staff efficiency

SOLUTION

+ Gigamon ThreatINSIGHT™, tightly integrated with partner platform StrikeReady

CUSTOMER BENEFITS

+ Automated threat detection and prioritized alerting
+ Seamless integration of enriched intelligence into the existing security stack
+ Reduced time spent on investigations
+ Improved operational efficiency, eliminating need for more staff
+ Data retention to aid future investigations

ABOUT CNA

Headquartered in Chicago, CNA is a business insurance solutions provider with a focus on small and midsize businesses (SMBs) and underwriting for organizations and associations. They are a leader in that space, with more than $1 billion in gross written premiums per year through various industry groups. The average length of CNA's partnerships is over 20 years. The company also specializes in international insurance solutions for mid- to large-size companies with a global presence. Insurance offerings include casualty, commercial auto, cybersecurity, equipment breakdown, general liability, management liability, property, business travel, kidnap and ransom, and workers' compensation insurance — with packages tailored to each business's risk management needs.

BUSINESS CHALLENGE

Security is a top priority for CNA, as it operates in a highly regulated industry and is required to comply with many government agencies and directives. Most of CNA's workloads are currently hosted on premises, but they are fast moving into the cloud space. Senior Director for Global Security Operations at CNA, Adil Mufti, is responsible for the SOC and all things related to incident response.

Adil and his team rely heavily on StrikeReady, a cloud-based security automation platform that uses artificial intelligence to provide defenders with the ability to analyze, reason, guide, and resolve issues faster. Even with this sophisticated technology in place, much of the team's time was being taken up by a constant onslaught of alerts and noise. And to compound the problem, attracting and retaining talented security people to help lighten the load was a big challenge. Adil recognized that he needed a better way to leverage the people on his SOC team and increase their operational efficiency.

RESOLUTION

Before evaluating new security solutions, Adil laid out a set of criteria based on a scoring system to help him make the right decision. According to this system, Adil says that Gigamon rated "way above" other vendors. Adil chose Gigamon ThreatINSIGHT, partly because it could be integrated with their existing security platform, StrikeReady. The integration and time to value were rapid.

"Building out the integration is extremely easy, and there is not much education. It's in the tool itself," Adil confirms. He says it took less than an hour to get everything up and running, and walking analysts through how to work within the ticketing system was also quick.

With the combination of Gigamon ThreatINSIGHT and StrikeReady, Adil and his team are now able to quickly index and parse through indicators of compromise (IoCs) and pull out the meaningful alerts to be triaged.

As Adil affirms, "Gigamon ThreatINSIGHT applies intelligent automation to the mountain of alerts coming from our security stacks and prioritizes the most important indicators of compromise. Rather than spend time sifting through the noise, our analysts can now focus on investigating the adversary activity that matters most."

BENEFIT

"The integration between ThreatINSIGHT and StrikeReady makes our life easier, and I think it's a killer combination," asserts Adil. He appreciates that this gives him and his team the ability to retain data for as long as a year at a reasonable cost, which then allows them to retroactively search for some of the IoCs that might show up again, spin up an alert, and then follow their prescribed incident response process.

These threat investigations serve to improve CNA's future cybersecurity defenses. "Going back through your dataset and trying to figure it out is hard," says Adil, "unless you have a technology that can go through the terabytes and terabytes of data. Gigamon ThreatINSIGHT gives us the ability to do that, and StrikeReady helps us automate that piece." With Gigamon, he says he can "have the machine do all the work rather than having an analyst do the work."

"The ease of use, speed, and accuracy of Gigamon ThreatINSIGHT has dramatically increased the speed and efficiency of our investigations," says Adil. "The solution integrates seamlessly with our security stack and has reduced the workload of the SOC team by nearly 50 percent." For example, in response to the Log4j vulnerability, he and his team were able to spin up, within a few hours, a dashboard specifically looking for traffic related to that vulnerability. Increased visibility into East and West traffic has also accelerated their investigations.

Adil appreciates that his team can push remediations within the same console: "With just a click of a button, we have the ability to push blocks into the firewalls, so a lot of the things that we were doing manually or opening separate tickets for, we're able to do within the console."

ABOUT STRIKEREADY

StrikeReady Inc. is a cybersecurity startup based out of California. The company was founded in 2019 and offers the industry's first cloud-based security operations and management platform that enables organizations to increase the effectiveness, efficiency, and affordability of their security operations, while empowering and augmenting cybersecurity teams with institutional knowledge and automation. It's backed by several Bay Area VC firms, along with executives from FireEye, CrowdStrike, Zscalar, and others.

StrikeReady has won numerous awards and mentions in the short time that it has been in existence, including Global InfoSec Awards 2022, Intellyx 2022 Digital Innovator Award, 2022 Govies Awards, 2022 CODiE Finalist Best Emerging Technology, 2022 Artificial Intelligence Excellence Awards, 2022 Cyber Security Global Excellence Awards, 2022 Cybersecurity Excellence Awards.

Connect with us at www.strikeready.co.

ABOUT GIGAMON

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com