Case Study

Black Hat: Securing the World's Premier Cybersecurity Conferences

> The performance of the Gigamon Deep Observability Pipeline has been exceptional. I don't even know where the ceiling is because we haven't even come close to hitting it. Everything that we've wanted to do with the company's solution, we've been able to do.

NEIL R. "GRIFTER" WYLER
Network Operations Center Lead at Black Hat

Challenges

- The Black Hat team has a very short window just a few days — to stand up the equivalent of a full-scale enterprise network.
- Reliable access to data
- Reliance on SPAN ports

Solution

- Gigamon Deep Observability Pipeline
- GigaVUE® HC Series
- GigaSMART® with Application Intelligence

Customer Benefits

- Increased visibility into network traffic
- Lower security tool costs
- Elimination of tool port contention

Black Hat is one of the most important event series of the year for information security. The world's top cybersecurity researchers and practitioners descend on Las Vegas, London and Singapore for each region's annual conference. Participants come to learn about the latest exploits and vulnerabilities, and to understand how they can best protect their organization against future risks. In 2017, a recordbreaking crowd of 17,400 security professionals and more than 200 companies participated in the 20th anniversary event in Las Vegas.

Challenges

The Black Hat team has a very short window — just a few days — to stand up the equivalent of a full-scale enterprise network. With more than 100 people in the Black Hat Network Operations Center (NOC) working to help make this happen, it's still a challenge.

To complicate matters is the expertise of Black Hat attendees — many of whom are black hat and white hat hackers — also known, respectively, as proactive and reactive hackers. They naturally tend to poke holes in any network they use and, given this, there is extra pressure to make sure the network is not only stable and scalable, but also secure.

Prior to their relationship with Gigamon, the Black Hat NOC team was limited in the amount of traffic they could monitor with the equipment in place. At times, the network SPAN ports got so overloaded with traffic that the team would have to disconnect one security tool in order to use another. This was a situation that led to an incomplete picture of the security needs of the network.

"The SPAN ports we had in place before working with Gigamon weren't always reliable. We needed better visibility into the traffic to ensure network security," said Bart Stump, operations manager at Black Hat. "Previously, we only had a switch repeating traffic. However, this takes the lowest priority when you start loading up the switch with traffic. It could draw packets, but there were many things we couldn't see without the Gigamon Deep Observability Pipeline in place."

"Essentially, we had a problem of scale — and not just from a stability or volume standpoint, but also a visibility standpoint. We needed to have insight into what was taking place on the network at any given time and be able to react quickly." Neil R. "Grifter" Wyler, NOC lead at Black Hat.

Solution

Recognizing Gigamon as the leader in network traffic visibility for cybersecurity and visibility applications, the Black Hat team turned to the company to help ensure they had insight into issues on their network in real time.

"At Black Hat, we want to work with best-of-breed solutions and the companies that we know are going to help us deliver the reliable network service our attendees have come to expect. We reached out to Gigamon to be a part of this solution," said Black Hat General Manager Steve Wylie.

The Black Hat NOC team chose to implement the Gigamon Deep Observability Pipeline to optimize the delivery of network traffic to security tools. The solution offers a consolidated, extensible and powerful foundation that gives pervasive visibility across all infrastructures — physical, virtual and cloud — to better uncover and mitigate threats. Its functionality includes traffic deduplication and header stripping to improve efficiency and reduce unnecessary processing overhead, as well as NetFlow generation that feeds metadata traffic to security tools, including RSA NetWitness and Plixer Scrutinizer.

When coupled with the Gigamon Deep Observability Pipeline, Plixer Scrutinizer, for example, delivers the forensic data necessary to rapidly perform root-cause analysis and help select the best course of action post security incident, dramatically reducing time-to-resolution. Plixer Scrutinizer leverages the automatic traffic load balancing and aggregation functionality deep observability pipeline to reduce bottlenecking and port oversubscription.

In addition, the Gigamon Deep Observability Pipeline provides complete access to the virtual traffic data that RSA NetWitness Suite needs to help detect advanced persistent threats (APTs) through lateral movement within east-west traffic even when it doesn't touch the physical network. RSA NetWitness also monitors and analyzes unsampled NetFlow data generated by the platform.

Results

"The performance of the Gigamon solution has been exceptional. I don't even know where the ceiling is because we haven't even come close to hitting it. Everything that we've wanted to do with the company's solution, we've been able to do," said Grifter.

"Our whole experience using products from Gigamon has been amazing. They've done a great job in supporting us and the deep observability pipeline has handled the voluminous traffic very well," added Stump, Black Hat network operations lead.

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