Hewlett Packard Enterprise

Case Study

NEOSECURE SABEMOS DE SEGURIDAD

Neosecure transforms security maturity, improving efficiency and competitive advantage

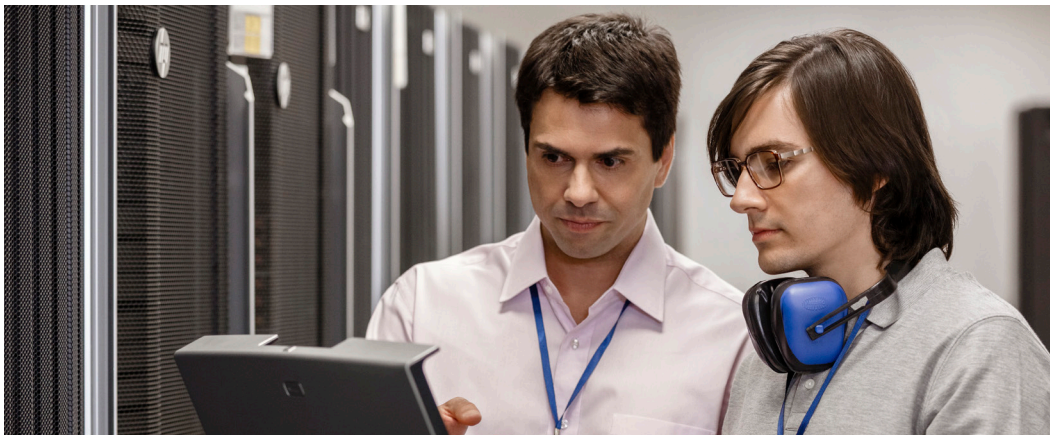
Latin American MSSP builds world-class security practice with HPE Security

Objective
Adopt enterprise security management best practices to deliver world-class managed security services for diverse clients across Latin America

Approach
Engage HPE Security Intelligence and Operations Consulting to recommend best practices for maximizing client value from HPE Security ArcSight analysis

IT Matters
- Aggregated 250 million discrete events down to 80 million events, enabling security analysts to focus on priority issues
- Created approximately 500 rule sets to detect complex attack scenarios across a broad range of data sources for more complete security operations visibility
- Gained deep intelligence to uncover threats in near real time, reducing response time from hours to minutes

Business Matters
- Reduced events per analyst hour from 40 to 20, improving analyst efficiency and reducing costs
- Transformed business practices to achieve the highest security maturity score for an MSSP in Latin America
- Strengthened competitive advantage through improved analyst efficiency and more responsive client services



A long-time HPE Security ArcSight user, Neosecure engaged HPE Security Intelligence and Operations Consulting to perform a maturity assessment, which transformed the company into a world-class service provider delivering highly responsive managed security services to clients across Latin America.

As a leading managed security services provider (MSSP) in Latin America, Neosecure knows what it takes to protect network and information assets from cyber attacks. The company has built a comprehensive suite of enterprise security management solutions delivered by a team of experts that all share a passion for excellence. It's no wonder Neosecure has grown to serve major corporate clients across Argentina, Chile, Colombia, and Peru.

Central to Neosecure's success is using the right technology and applying proven best security management practices in every aspect of security. The company has its own Malware Research Center and Security Operation Center (SOC)—the second in the world to be certified under ISO 27001. Its security analysts are also certified by many

> "Before getting the maturity assessment from HPE Security, we didn't know how our security practices compared to world-class organizations. Now we've transformed our organization to the point where Neosecure achieved the highest maturity score for an MSSP in Latin America."
>
> — Fernando Fuentes, Senior Manager, Innovation and Services Portfolio, Neosecure

leading industry organizations, including ICS2 (CIISP), ISACA (CISM), and CERT. And when it comes to security information and event management (SIEM), Neosecure has put its trust in only one solution for the last 10 years: HPE Security ArcSight.

Fernando Fuentes, senior manager for the innovation and services portfolio at Neosecure, explains, "Many of our clients are financial institutions that have a lot of critical security technologies such as intrusion prevention and anti-malware, but they have no way to monitor them in an integrated way. So it's nearly impossible to see where and when a threat is entering their network. That's where the correlation of ArcSight comes in. With ArcSight, we can monitor our clients' entire infrastructure and correlate data from all their technologies to provide faster and more precise threat detection."

Provides clients with peace of mind

ArcSight enables Neosecure to deliver a range of important security management benefits to its clients. First, Neosecure analysts can detect threats quickly and alert clients of the situation while an attack is still in its early stages — before it has a chance to disrupt the business. Neosecure analysts can also use ArcSight to perform more extensive event correlation research on security event data. This is key to uncovering anomalies that could indicate the presence of more persistent threats. In addition, the company monitors information shared on social networks, which can uncover potential threats affecting one client or an entire industry. This advanced warning allows Neosecure to prepare appropriate procedures for its clients to protect their businesses.

"Our clients get peace of mind knowing that we are watching their network and alerting them to any possible threats," says Fuentes. "ArcSight allows us to adjust our monitoring to focus on a specific threat and gain intelligence on where the attack came from so we can help our clients respond more quickly and precisely."

In one example, Neosecure detected an anonymous attack operation specifically targeting clients in Chile. The company created several new views in ArcSight to observe increasing traffic within and from outside Chile, and quickly uncovered patterns that indicated the threat would most likely involve denial of service and website defacement. As a result, Neosecure notified its clients of the impending attack so they could address it proactively and prevent any impact on their businesses.

Detects complex attack scenarios in near-real time

Neosecure has created approximately 500 rule sets in ArcSight to detect complex attack scenarios that could affect its clients. This allows the company's security operations analysts to increase visibility across a broad range of data sources to not only see an event, but also have context to know where and when the event occurred.

In addition, Neosecure uses ArcSight to aggregate 250 million discrete events per day down to 80 million composite events. ArcSight then further distills these events into several dozen prioritized security issues for analysts to address.

"Because ArcSight provides a consolidated view of security events, our analysts can spot anomalies in almost real time," Fuentes remarks. "This, combined with our 24 x 7 monitoring, allows us to reduce our response time from several hours to a matter of minutes. It is this kind of fast, intelligent action that enables Neosecure to prevent security incidents from impacting our clients. In fact, we have some clients with us for 10 years that have never been compromised by a cyber attack."

Granzotto adds, "It's impossible to do this kind of managed security work without a solution like ArcSight. It is an essential part of our service offering and the key to delivering efficient and effective security monitoring. You can monitor an intrusion prevention system or a firewall, but there's no way to get the complete information you get with ArcSight. It allows us to correlate information from several clients, giving us an eagle-eye type of vision."

Case study
Neosecure

Industry
Managed security services

Customer at a glance

Application
- Security information and event management

Software
- HPE Security ArcSight

HPE Services
- HPE Security Intelligence and Operations Consulting

Dramatic advance in security maturity

Providing world-class managed security services goes beyond having the right security management technology. It also requires highly skilled security operations professionals. However, in Latin America security experience is scarce and Neosecure had no gauge for how well its team performed in comparison to global standards of excellence. So the company engaged HPE Security Intelligence and Operations Consulting to perform a security maturity assessment.

The maturity assessment looked at 240 characteristics across four key areas—business components, people, processes, and technology—and compared the results to industry peers. Neosecure's objectives were clear: 1) determine whether the company's security management practices were optimal based on global standards, and 2) adopt the appropriate best practices where needed. The impact of the assessment was profound.

"Before getting the maturity assessment from HPE Security, we didn't know how our security practices compared to world-class organizations," notes Fuentes. "Now we've transformed our organization to the point where Neosecure achieved the highest maturity score for an MSSP in Latin America."

Recommendations from the maturity assessment also enabled Neosecure to improve its business processes. For example, the number of events handled per analyst hour—a key industry measure of efficiency—was reduced from 40 to 20. The company expects to improve analyst efficiency another 20 – 25% through additional security operations automation. This efficiency improvement translates directly to enhanced value for Neosecure's clients.

"Here in Latin America, price for managed services is very important," Fuentes explains. "By increasing analyst efficiency we reduce costs and can be more competitive. It also allows our security team to spend more time on analysis, reducing mistakes and providing more complete, higher quality service to our clients."

Strengthened competitive advantage

Neosecure has built a world-class managed security services practice through the advanced capabilities of HPE Security ArcSight. And the company's business has surged after leveraging the expertise and guidance of HPE Security Intelligence and Operations Consulting.

Fuentes concludes, "HPE Security consultants enabled Neosecure to look at our operations in a very methodical way and optimize our efficiency with their expert recommendations. Working with people that have experience in world-class SOCs was very important to us. It allowed us to align our practices with the best global standards to improve our service and deliver higher customer satisfaction. Also, by improving our security maturity, we have a strong business message to take to market. HPE Security has absolutely helped us improve our competitive advantage."

Learn more at
hpenterprisesecurity.com

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-2764ENW October 2015