Case Study

Intelligent SOC Drives "Defense in Depth" Strategy at Sonesta Hotels

Overview

Cybersecurity is neither a "one size fits all" nor an "all or nothing" undertaking. For most enterprises, security infrastructures and best practices evolve in phases according to fast-changing goals, resources, and priorities.

Sonesta Hotels is no exception. With sites spanning eight countries, the fast-growing hospitality chain takes a methodic, multi-layered "Defense in Depth (DiD)" approach to sequencing security processes and mechanisms to defend its attack vectors. As part of the strategy, Sonesta enhanced its security operations center (SOC) capabilities by adopting Intelligent SOC from Netenrich.

Intelligent SOC combines IBM QRadar security incidents and events management (SIEM) with Netenrich's Resolution Intelligence and deep SOC expertise. This new outcome-driven approach improves real-time monitoring and visibility to speed response while freeing the Sonesta team to become more analytical and proactive.

Evolving with Intelligent SOC

Scaling a company's cybersecurity infrastructure takes a dynamic, nuanced mix of strategies and innovative best practices. Sonesta began implementing its DiD approach by addressing visibility challenges.

"We asked questions like, 'are we getting the right amount of alerts? Do we know what our vulnerabilities are'?" Security Engineer Dave Borman recalls. "Once you've got all this information, the next step is looking at what needs to be fixed, what needs to be fixed first, and which of the resources we had available could resolve issues fastest."

Company

One of the fastest-growing hospitality companies in the US, Sonesta Hotels manages nearly 300 properties under seven brands operating across eight countries.

Challenge

Implementing a methodic, multi-layered "Defense in Depth (DiD)" cybersecurity strategy to improve real-time threat monitoring and response while improving efficiency and ROI.

Solution

Sonesta adopted Intelligent SOC from Netenrich featuring Threat & Attack Surface Intelligence and IBM QRadar SIEM capabilities. The Netenrich solution helps prioritize and contextualize threats to speed response, improve ROI, and save Sonesta analysts time.

> ***With Netenrich, we get a lot more information and it's easier to absorb and make assessments as to whether something needs to be fixed right away, and the best way to do it. It's far and away better than what we were using previously.***
>
> ***- Dave Borman, Security Engineer, Sonesta Hotels***

As Sonesta's cybersecurity needs and infrastructure evolved, the team decided to engage Netenrich to manage alerts, logs, and security incidents and events management (SIEM) capabilities. Netenrich's Intelligent SOC solution features IBM QRadar SIEM capabilities to overcome challenges with real-time monitoring and visibility while leveraging proprietary threat intelligence and deep analyst expertise from Netenrich.

Netenrich's outcome-driven solution gives Sonesta a reliable view of which security tools are reporting and what triage is taking place. "The application we were using before was a bit kludgy," Borman recalls. "We would get notifications that an issue existed, but the details and reporting weren't always there. It was difficult to determine whether we had already seen a particular issue and didn't need to see anymore. We might also go a few months without realizing a certain tool wasn't reporting into the system."

With Intelligent SOC improving real-time monitoring and contextualization of threats, Sonesta successfully distilled its incident response strategy down to a simple process: Determine what the issue is, context and fix the issue, then verify that it stays fixed. Borman maintains that while "nothing is 100 percent," the company's evolving DiD approach ensures the right things get fixed at the right time—and stay fixed—and that nothing important slips through the cracks.

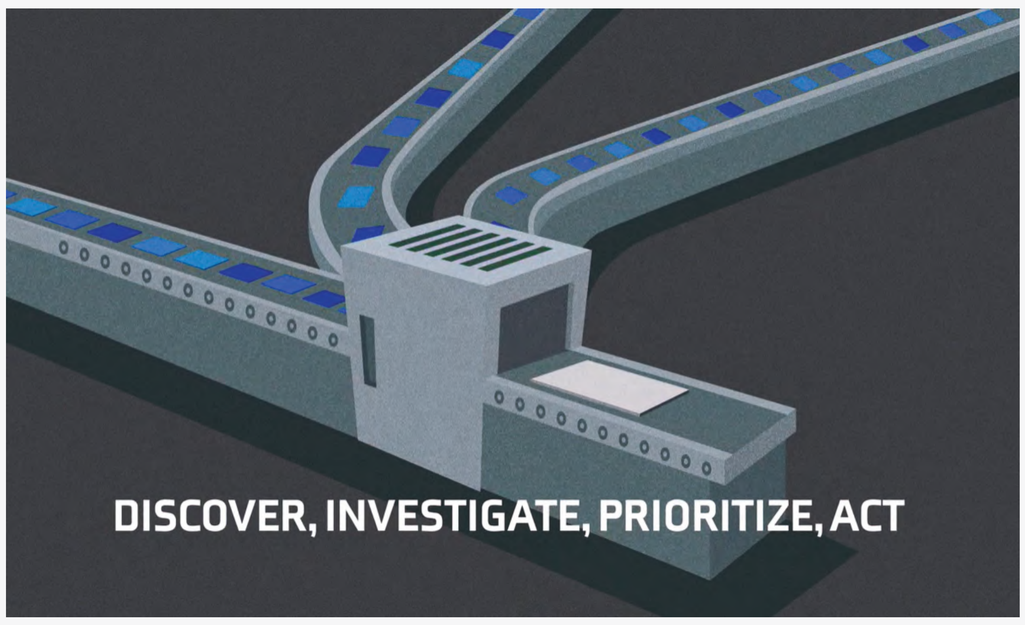
Reducing Risk by the Day

Having enhanced its basic block-and-tackling, Sonesta soughtto make cybersecurity operations more analytical and proactive. The company now uses rich threat context and deep expertise from Netenrich to prioritize patching efforts and shrink its digital attack surface, Sonesta leverages rich threat context and deep expertise from Netenrich to improve prioritization.

Sonesta looks at which systems and applications are most critical, which vulnerabilities represent the greatest risk, and what controls are already in place. "If we have a significant vulnerability in one application, we look at whether we've already got two or three corresponding controls for it, which would give us more time to fix it," Borman says. "If we only have one control in place and something fails, we've got a problem, so those things get fixed right away."

Netenrich's Attack Surface Intelligence (ASI) solution provides ongoing discovery of external risk to guide prioritization and speed response. ASI discovers brand and domain exposure, vulnerabilities, and misconfigurations that might be used by adversaries to launch cyberattacks.

A complement to pen testing and Red Team exercises, ASI combines with Netenrich Knowledge NOW (KNOW) global threat intelligence to correlate and contextualize risk.



See what hackers see with ASI

Watch video

> *"ASI lets us know about expired certificates. It's also good to see any issues with sites belonging to restaurants located within our hotels."*

Right-sizing SOC resources and results

Evolving cybersecurity strategies must continue to balance fast-changing needs with available resources and the ability to demonstrate value. The key to achieving success and return on investment is more and better intelligence, and an inherently flexible approach.

Intelligent SOC lets Sonesta invest in ongoing optimization and innovation simultaneously. "Efficiency is always important, but it's also wrapped inside new initiatives," Borman says. "We're efficient, and we've outsourced some of the day-to-day things to Netenrich so that our team can go out and investigate new applications and tools, and integrate all these things together, which is always a major challenge."

Like many enterprises, Sonesta remains reluctant to have security issues remediated automatically without first making experts aware. The team would, however, consider turning more hands-on remediation over to trusted managed security service provider (MSSP) partners at some point.

"If we find a problem and the partner knows what to do, or it's something we don't have the time or resources to fix ourselves, we could let them go ahead and take care of the issue to free up even more resources on our side," Borman says. "You just have to have a level of trust and a lot of good communication."

Learn more about Intelligent SOC

Netenrich's expansive Intelligent SOC portfolio also positions enterprises to consume new capabilities as needed on a "pay as you grow," outcome-based basis. With outcome-driven engagements and capabilities to address attack surface management, Shadow IT, and cloud, Intelligent SOC delivers the speed, expertise, and flexibility to scale security best practices for years to come.

Enterprises can get what they need—when, where, and how they need it—to continually speed response, retain skills, and reduce run costs as they improve their security posture.

Intelligent SOC-as-a-Service

Smarter Ops for Smarter Security

Watch video

Sign up for Netenrich's Intelligent SOC

About Netenrich

Netenrich delivers complete Resolution Intelligence to transform digital operations into smarter business outcomes. With 15+ years' innovation across IT, NetOps and SecOps, Netenrich applies a dynamic mix of machine and expert intelligence through a wide range of products and SaaS-based offerings. More than 6,000 customers and organizations worldwide rely on Netenrich to help drive digital transformation, mitigate brand exposure, increase efficiencies, and bridge skills gaps. Netenrich is based in San Jose, California.

Visit the Netenrich site to learn more and try ASI.