CASE STUDY

Solving Security Challenges with Trellix solutions

Industry

Software

Solutions and Services

- Trellix Living XDR SecOps Platform including:
- Trellix DLP Endpoint
- Trellix EDR
- Trellix ePolicy Orchestrator (ePO)
- Trellix Helix
- Trellix Insights

Benefits

- Decreases mean time to respond with automated security policy orchestration
- Leverages existing tools with open integrations and unified processes
- Detects advanced threats with machine learning, AI, and real-time cyber intelligence

Customer Profile

The Trellix Security Operations Center (SOC) is using the open and native Trellix Living extended detection and response (XDR) SecOps Platform to manage advanced threats and stay confident in the protection and resilience of their operations.

Trellix adopts XDR-based cybersecurity strategy for its SOC

Seeking a solution for common security challenges

In a recent survey of IT and cybersecurity professionals conducted in conjunction with analyst firm, ESG, Trellix found that SecOps are looking to XDR for advanced threat detection and prioritization, as well as to improve staff productivity.

The Trellix Security Operations Center (SOC) team in Cork, Ireland, is no different.

> "The challenges they're trying to overcome as we build out our SOC are probably the same challenges our customers are trying to overcome--having multiple teams in multiple locations that need 24x7 monitoring capability—and we all need to be looking at the same pane of glass."
> —Bernadette Moloney, Security Operations Manager, Trellix

Multi-technology portfolio addresses the promise of XDR

A result of the merger of McAfee Enterprise and FireEye, Trellix was launched as a company in early 2022 to provide XDR solutions with automation, machine learning, extensible architecture, and threat intelligence.

The core members of the Trellix Security Operations Center (SOC) team are Bernadette Moloney, and security analysts Lauren Driscoll and Niamh O'Connell.

All three team members have hailed from McAfee.

Moloney explains, "We're divesting from McAfee, and bringing in FireEye at the same time as we build out a new SOC and a whole new team."

For data protection, endpoint security, and analytics, the Trellix SOC team uses Trellix EDR, Trellix ePolicy Orchestrator (ePO), Trellix Helix, and Trellix Insights, which are all core components of the living security Trellix XDR.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.Trellix.com

Trellix XDR offerings seamlessly integrate with the company's broad portfolio of endpoint, email, network, cloud, and other security products. It also easily connects with third-party security apps.

This functionality is helpful for new analysts to come up to speed because they don't have to learn multiple ways of reading logs; they're all the same, and they're all in the same place.

> "From an investigation standpoint, having everything in one place is a lot easier for an analyst. It saves us from having to log into multiple tools and then perform different search queries to get the information. Instead, you see the big picture."
> — Lauren Driscoll, Security Analyst, Trellix

Accelerating the effectiveness of security operations

As "customer zero," the Trellix SOC team has enjoyed the ability to automate security policies, reduce complexity, and increase efficiency. Moloney shares, "It's fast, it's easy, and if we make a change to an alarm, we only have to do it in one place, so our overhead is reduced as well."

The Trellix XDR solutions offers a unified experience that give users the power to detect advanced attacks across all vectors, predict and prevent emerging threats, and prioritize the most critical security concerns. "Having the logs in one place can also help identify lateral movement, which is very critical for us as a SOC," concludes Moloney.

> "My favorite part is how quickly and easily we can allowlist IP host names to reduce false positives."
> — Niamh O'Connell, Security Analyst, Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.