THE TRIPLE PUNCH OF MANAGED DETECTION AND RESPONSE, **MICROSOFT SENTINEL, AND SASE SPEEDS CYBERSECURITY RESPONSE**

MIKRON

With more than 100 years of experience in developing and producing automation solutions, machining solutions, and cutting tools for customers across the globe, Switzerland-based Mikron is known for its highly precise products that are rooted deeply in the Swiss culture of innovation.

> The sensors in SASE observed the malware and we were able to block its spread almost immediately. Had we not been notified by Open Systems' solution, the results could have been catastrophic.

Rolando Galeazzi, Mikron CISO

WHY CHANGE?

- Too many cybersecurity vendors
- Not enough security staff
- Threat alert volume difficult to handle
- Threat risk too high

THE NEW REALITY

- Unified solution: SASE SD-WAN + Microsoft Azure Sentinel + MDR
- 24x7 SOC

WHY IT'S BETTER

- Separate noise from real threats
- Enriched threat information
- Direct response by Open Systems
- Mikron out of the cybersecurity business

One thing the company didn't want to be known for is being vulnerable to cyberthreats. A breach could shut down IT systems, leak client data and intellectual property, and potentially halt production.

To combat threats like these, CISO Rolando Galeazzi says the company has "been building up our security infrastructure for two years, shifting from several third-party vendors to a single vendor."

That vendor was Microsoft. Like many companies, Mikron enabled Microsoft Azure Sentinel SIEM (security information and event management) as part of its Microsoft 365 E5 license to bolster cybersecurity. However, Galeazzi found himself buried in threat alerts, unable to separate the true threats from noise. With so much coming in, it was impossible to keep up – or to efficiently respond to threats – on a 24x7 basis.

THE MISSING PIECE: MANAGED DETECTION AND RESPONSE

Mikron already worked with Open Systems' SASE platform for a secure, cloud-based SD-WAN. Galeazzi learned that Open Systems' Managed Detection and Response (MDR) service is built on top of Sentinel, allowing him to still make use of Mikron's investment in Microsoft, enable seamless integration across both Sentinel and SASE, and keep vendors unified.

This triple integration means Open Systems' SOC analysts manage the work of investigating and reacting to threats, even when they originate outside the network. Their access to the network and immediate action helps minimize the time threats have to spread, thus mitigating potential damage.

"I'm alone in this security journey. My IT team is our infrastructure people; their main job is not watching alerts. The purpose for this integration is having a 24x7 SOC, as it's quite difficult for one man to be awake for 24 hours a day," says Galeazzi.

DETECTION AND RESPONSE IN ACTION

Galeazzi notes that he's gaining more visibility into cyberthreat activity through enrichment of Sentinel data from the Open Systems SOC engineers. Says Galeazzi, "Sentinel is the center point of the whole picture, and Open Systems is the enabler for it."

Open Systems is able to reduce false positive rates through enrichment, correlation, and further investigation to eliminate alert fatigue and save valuable time for customers.

"Alerts that I receive from Defender are pure information. Open Systems is able to enrich and provide context for alerts with additional information gathered by people. In the end, you can have all the artificial intelligence you want, but you still need a human component," he says.

WHEN YOU NEED IT FAST...

72 hours
Average time for security change requests at Mikron prior to Open Systems.

15–30 minutes
Average time for security change requests at Mikron with Open Systems.

This shift to a unified managed detection and response is part of a larger trend away from best-of-breed-era security that no longer works in the cloud age.

"In the near future, this integration will be standard," says Galeazzi. "It's useless at this point to have logs flowing up and down from on premises to the cloud or vice versa. It's best to keep them in a single location. Managed security providers will have to face the shift toward cloud-based SIEMs or die."

With an integrated solution that's ahead of the curve, Mikron can face the future knowing its cybersecurity needs are handled.