VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Vectra stops data breaches across one of Europe's largest drug store chains

With more than 2,196 drugstores in Germany and another 1,892 stores in Eastern and Southeastern Europe, ROSSMANN is one of the largest drugstore chains in Europe, with a total of 4,088 stores and 56,200 employees.

As one of the largest retailers in Germany, ROSSMANN's IT security team needed a solution to identify threats inside its network.

The ROSSMANN IT security team, headed by Team Lead Daniel Luttermann, began the process of strengthening its security posture to catch cyberattackers at the network perimeter and to identify threats inside the network.

Before evaluating vendors in the proof-of-concept (POC) testing phase, ROSSMANN conducted a red team exercise to identify potential security weaknesses and vulnerabilities.

The results of this penetration test were used to gauge vendors in the POC phase. The team ultimately chose a diverse roster of solutions that included the Cognito® network detection and response (NDR) platform from Vectra®.

"The Vectra Threat Certainty Index™ automatically prioritizes detections so it's easy to see the most critical threat behaviors. For us, it consolidates hundreds of events and historical context to pinpoint host devices that pose the biggest threat."

Daniel Luttermann
Security Team Lead
ROSSMANN IT

ROSSMANN

Organization

ROSSMANN

Industry

Retail

Challenge

Needed a way to identify threat behaviors and decryption without deep packet inspection

Selection criteria

A network-centric detection and response solution that captures security-centric metadata to identify threats without prying into payload or contents of traffic

Results

- Consolidation of hundreds of events to pinpoint host devices that pose the biggest threat
- Greater understanding of the context behind every threat
- Automated scoring and prioritization by the Vectra Threat Certainty Index

> "The Cognito platform exposed red team behaviors in a very short time, We realized that this would enable us to respond quickly to mitigate real threats."

Daniel Luttermann
Security Team Lead
ROSSMANN IT

Evaluation criteria

"To identify threat behaviors, decryption using deep packet inspection is not an option," says Monika Engel, security analyst in charge of GDPR compliance and audits. "We adhere to strict data protection laws, which only allow us to investigate the content of data traffic in certain situations and to a certain extent."

The ROSSMANN IT security team was impressed at how Vectra extracts security-enriched metadata from all network traffic to detect suspicious and threatening behaviors.

"Vectra offers protection without prying," says Luttermann. "Instead of looking at the payload or contents of traffic, it only captures the security-centric metadata to identify threats. Vectra is GDPR compliant and it was approved for the POC test internally and also by our Worker's Council."

The Vectra solution was up and running quickly in the POC test and showed speedy time-to- value, according to Luttermann.

"The Vectra Threat Certainty Index™ automatically prioritizes detections so it's easy to see the most critical threat behaviors," he notes. "For us, it consolidates hundreds of events and historical context to pinpoint host devices that pose the biggest threat."

Vectra automates the hunt for cyberattackers, reveals where they're hiding and tells you what they're doing. The highest-risk threats are instantly triaged, correlated to compromised host devices and prioritized so IT security teams can respond faster to stop in-progress attacks and avert data loss.

"We realized that Vectra's ease of use and automation – combined with low noise and a strong threat signal – would save us time and give us a greater understanding about the context of every threat," Luttermann says.

These were major factors in choosing the Cognito NDR platform from Vectra.

Up and running

After deploying the Cognito NDR platform, the ROSSMANN IT security team conducted another red-team penetration test.

"The Cognito platform exposed red team behaviors in a very short time," says Luttermann. "We realized that this would enable us to respond quickly to mitigate real threats."

Capable of finding and stopping cyberattackers in the cloud, data center, IoT, and enterprise environments, the Cognito platform uses AI to deliver real-time threat visibility and put threat details at your fingertips.

By combining advanced machine learning techniques – including deep learning and neural networks – with always-learning behavioral models, the Cognito platform quickly and efficiently unveils hidden and unknown threats before they cause damage or steal data.

How it's used

The Cognito platform provides enterprise-wide visibility into hidden threat behaviors by analyzing security-enriched metadata from all network traffic – in the cloud, enterprise, authentication systems, SaaS applications like Office 365, workloads, and user and IoT devices.

Leaving attackers with nowhere to hide, the analysis of security-enriched network metadata is applied to all internal (east-west) traffic, internet-bound (north-south) traffic, the virtual infrastructure, and cloud environments.

"We intuitively know to watch for alerts in the Cognito dashboard," says Luttermann. "There's no need to sift through mountains of logs and chase down every single one. The automated scoring and prioritization done by the Vectra Threat Certainty Index saves us a lot of time."

By automating the manual and time-consuming analysis of security events, the Cognito platform condenses months of work into minutes and significantly reduces the security analyst's workload. This enables IT security teams under siege to stay ahead of attackers and respond faster to hidden threats.

"The Cognito platform doesn't require much labor to be an effective weapon against cyberattacks," Luttermann observes. "It sends a strong, high-fidelity threat signal, there's no noise, and no alert fatigue. If a critical detection appears in the dashboard of the Cognito UI, we know it's worthy of our attention."

With Vectra up and running, the ROSSMANN IT security team is now building out its incident response capabilities to respond even faster to mitigate advanced threats.

"It sends a strong, high-fidelity threat signal, there's no noise, and no alert fatigue. If a critical detection appears in the dashboard of the Cognito UI, we know it's worthy of our attention."

Daniel Luttermann
Security Team Lead
ROSSMANN IT

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai