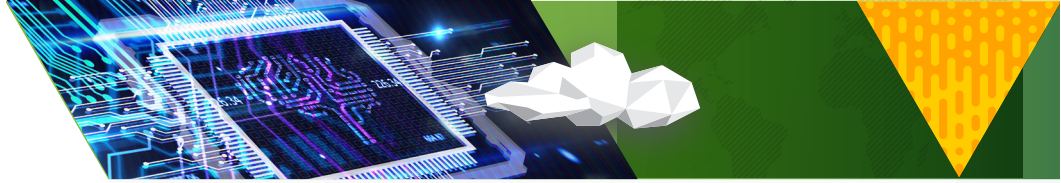
VECTRA
SECURITY THAT THINKS.®



CASE STUDY

DZ BANK enables protection without prying using AI-powered cyberattack detection

"Classical prevention systems like firewalls and intrusion detection and prevention systems don't cover advanced persistent threats or anomalous behavior in the network," says Matthias Tauber, senior services manager for IT security at DZ BANK, which serves as the central institution for more than 900 cooperative banks in Germany.

"Signature-based systems only detect what they know, instead of what they missed," he says. "We wanted to move from a traditional technology to a new one." Tauber and his team were looking to the new class of AI-powered network traffic analysis to detect hidden cyberattacks and stop threats faster.

Achieving security and privacy

With €506 billion in assets in 2017, DZ BANK is the second largest bank by asset size in Germany.

Cooperative banks serve Germany's many small and medium size businesses. As their central credit institution, DZ BANK strengthens their businesses and provides access to capital markets. It offers retail, corporate and institutional banking services. The bank employs 30,000 people across Europe, Asia and the United States.

"Signature-based systems only detect what they know, instead of what they missed."

Matthias Tauber
Senior services manager for IT security
DZ BANK

DZ BANK

Organization

DZ BANK

Industry

Financial services

Challenge

- Detect advanced threats missed by traditional signaturebased firewalls, IDS and IPS
- Distinguish between benign anomalous behaviors and high-risk attacker behaviors

Selection criteria

An easy-to-use network traffic analysis platform that reduces the time to detect threats, automatically triages alerts and speeds-up incident response.

Results

- Detect hidden attackers in data centers and user and IoT devices while complying with strict data privacy laws
- Mitigate the risk of insider threats and IT administrator policy violations
- Reduce the security operations workload with AI-driven threat detection and faster incident response

"With Cognito, I can focus on the highest-risk threats. With other solutions, I have to filter to get rid of hundreds or thousands of false positives."

Matthias Tauber
Senior Services Manager for IT Security
DZ BANK

Tauber's mission to protect the bank's assets, operations and sensitive information is complicated by a broad range of data privacy and financial regulations. Many types of surveillance and electronic monitoring of employees and communications are prohibited in Germany.

German workers' councils, known as Betriebsrat, represent workers at the local or firm level, which also impact DZ BANK's cybersecurity and data protection practices.

In addition, both the European Union General Data Protection Requirement (GDPR) and Germany's Second Markets in Financial Instruments Directive (MiFID II) became law in 2018.

Identify security gaps

As part of the bank's efforts to continually enhance its cybersecurity, Tauber and his team benchmarked the financial institution's security posture against the NIST cybersecurity framework.

"We identified that we had a gap in detecting advanced persistent threats and anomalies in the network," says Tauber.

To close that gap, DZ BANK chose the AI-driven Cognito® cyberattack-detection and threat-hunting platform from Vectra®. Cognito enables DZ BANK to detect threats in real time, automatically triage alerts and respond quickly to hidden attackers in data center workloads and user and IoT devices.

Blending human expertise with a broad set of data science, machine learning techniques and behavioral analytics, Cognito automates manual, time-consuming threat hunting and response. Cognito condenses days and weeks of threat hunting into minutes, which reduces the security operations workload by 36X.

Find threats faster

Cognito's always-learning behavioral models detect attackers in real-time to enable quick, decisive response and a logical investigative starting point.

"With Cognito, I can focus on the highest-risk threats," says Tauber. "With other solutions, I have to filter to get rid of hundreds or thousands of false positives."

Cognito automatically triages alerts with threat and certainty scores that are displayed on the intuitive Vectra Threat Certainty Index™. As a result, DZ BANK instantly knows which host devices with attack indicators pose the biggest risk with the highest degree of confidence.

Because Cognito analyzes enriched network metadata, relevant logs and cloud events – not payloads or communications content – DZ BANK automatically detects advanced threats in real time while complying with strict privacy laws.

A coordinated effort

"Cognito helps close the skills gap," says Tauber. "Cognito is easy to use and understand, and that makes it simpler for us to write runbooks for the security operations team to follow."

Front-line operations are handled by a managed security service provider. Tier 1 and Tier 2 agents use Cognito to detect cyberattacks and escalate the highest-risk threats to the DZ BANK security team, who also use Cognito for further investigation.

"With Cognito, we can see behaviors in the gray areas," says Tauber. "If we see suspicious activity, we can check out what's happening around the client."

Reducing the risk of rogue employees

Although DZ BANK selected Cognito to detect advanced threats and distinguish benign anomalies from attacker behaviors across its global network, it quickly became an essential tool to reduce the risk of insider threats.

The accounts of IT administrators are especially valuable to attackers. As part of DZ BANK's security practices, IT administrators can only perform their work from designated, specially-protected clients. But in haste or forgetfulness, people sometimes skip these precautionary steps.

> "We have guidelines that all administrators must only use their specific administrative clients," says Tauber. "We use Cognito to make sure that they do."

If, for instance, Cognito detects remote command-and-control behaviors, it might be an indicator that someone is working from an unapproved IT administrator's client. Or it could be a compromised account.

With Cognito, the security operations team can quickly determine if it is a high-risk threat. And if it was internal, the team can find out why the IT administrator was not following policy guidelines.

An automation journey

Tauber and his team are advancing the use of AI-driven Cognito to automate the detection of threats in real time and speed-up incident response while reducing the security operations workload for in-house and outsourced teams.

Cognito is also part of DZ BANK's well-coordinated security ecosystem. Cognito events are also published to its Splunk security information and event management (SIEM) system.

Tauber is now considering extending the Cognito platform capabilities to perform faster, more conclusive incident investigations and hunt retrospectively for covert cyberattacks.

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

Email info@vectra.ai vectra.ai