MICRO FOCUS

Customer Success Story

Security

Rabobank

Rabobank outsmarts advanced persistent threats with Micro Focus® ArcSight ESM. This international bank now uncovers cyber threats with enterprise security management.

Overview

With the volume and sophistication of APTs on the rise, Rabobank needed to build more complex use cases in its security information & event management (SIEM) solution to improve the accuracy of event correlation and threat detection. By implementing ArcSight Enterprise Security Manager (ESM), Rabobank now correlates a million security logs per day from thousands of data feeds across the enterprise. Using ESM the bank created dozens of advanced use cases to quickly identify abnormal behavior or untrusted devices on its network with a high degree of accuracy. This allows Rabobank to uncover threats that would previously have gone undetected, strengthening security while improving productivity and effectiveness of its security management team.

"ESM reveals security events to us that we were never able to detect before. We're very happy with ESM and confident we can find threats before they compromise our network or disrupt business. ArcSight provides critical insurance against the damage modern cyber-attacks can inflict on an organization."

MARK BEERENDS
Head of Security Operations Center
Rabobank

Rabobank is one of the largest cooperative banking organizations in the world. Founded in the 19th century by a group of farmers, Rabobank has grown from its agricultural roots in the Netherlands to become an international financial services provider, active in banking, asset management, leasing, insurance, and real estate.

Leveraging its unparalleled knowledge in the food and agriculture industry, Rabobank is on a mission to build wealth and prosperity in the Netherlands while resolving food issues worldwide. To fulfill that ambition, it must ensure the highest security for its information network.

Challenge

Like all financial institutions today, Rabobank is barraged on a daily basis with cyber threats from every imaginable vector. Phishing schemes and malware are a constant nuisance, but the biggest challenge comes from advanced persistent threats—stealthy, continuous hacking attacks by very clever cyber criminals. APTs are often difficult to detect and may be active in a network for months until they are found. At that point, however, damage

Rabobank

At a Glance

- **Industry**
  Financial Services
- **Location**
  Netherlands
- **Challenge**
  Build more sophisticated use cases to improve accuracy of identifying advanced persistent threats (APTs) for a more timely and targeted response.
- **Products and Services**
  ArcSight Enterprise Security Manager
- **Results**
  + Strengthened network security management with more accurate event correlation and threat detection
  + Improved security management team productivity and effectiveness
  + Brought entire security posture to a higher level

in the form of data loss or business disruption may already have been inflicted.

For years Rabobank relied on RSA enVision to analyze security alerts. To improve productivity and effectiveness of its security management team, Rabobank needed to build much more sophisticated use cases to provide contextual relevance around security alerts. However, enVision did not provide the necessary capabilities, and new developments from RSA were slow in coming to market.

Solution

To address its mounting security management needs, Rabobank considered alternatives to RSA, including ArcSight and IBM Qradar. After an intensive evaluation of both tools, the bank chose ArcSight ESM for its robust SIEM capabilities.

Mark Beerends, head of security operations center at Rabobank, explains, "What stood out most about ArcSight ESM was the ability to build very complex use cases. However, we also saw added advantages in being able to integrate ESM with our other Micro Focus solutions like Micro Focus Service Manager, which collects a huge amount of data on IT service activity."

High Availability Security Monitoring

Rabobank deployed three instances of ArcSight ESM, one instance in each of the bank's two data centers in the Netherlands to ensure high availability and disaster recovery, as well as a third instance for test and development.

The SIEM is so vital to daily operations that Rabobank wanted to ensure that production security monitoring would never be down for more than an hour in the event of a site loss. The test and development instance enables Rabobank's security management team to run new or updated use cases to understand any impacts of a change before putting the use case into production.

In production, ArcSight ESM collects approximately one million security logs per day from data streams generated by 3,000 HPE ProLiant servers running Microsoft Windows, another 1,000 HPE ProLiant servers running Linux, and more than a dozen HPE Integrity NonStop BladeSystem NB54000c servers.

Rabobank also runs other ArcSight ESM software, Fortify on Demand, and HPE TippingPoint[1] for application security testing. Beerends notes, "If we discover something in ESM that presents a security threat, it's easy to add a filter to TippingPoint to block that threat before it has a chance to cause problems on our network. The next step is integration of SIEM and IPS (intrusion prevention system) functions, but that will take time."

Results

Supports Complex Use Cases for More Accurate Threat Detection

Since deploying ArcSight ESM, Rabobank has developed 30 – 40 complex use cases, greatly improving the accuracy of event correlation and security alerts. These use cases provide important context so the security management team knows whether an alert requires immediate action or not.

For example, a mistyped password is not necessarily a concern. But knowing that a login attempt is being made at an unusual time of day or from an overseas IP address indicates that a much more serious threat may be at play. Ultimately, this level of detail will reduce the number of false positives and strengthen security across Rabobank's network.

"ESM provides more options to correlate events from many different feeds," says Beerends. "Better correlation means higher accuracy in detecting threats. That helps our security analysts know where and when to act. The best thing is we're logging all the data feeds we need, so we can quickly implement new use cases as needed."

One example of a recently developed use case is identifying rogue devices on the Rabobank network. The bank runs an open network, which allows anyone in the organization to connect using a personal device. However, cyber criminals could take advantage of this openness to hack into the network. To prevent such activity, Rabobank uses ESM to correlate data from its DHCP servers, Microsoft Active Directory, and network environment to determine if a device is trusted or not.

Integration between ArcSight ESM and Micro Focus Service Manager has also proven key. This provides Rabobank with insight directly into IT service activity, so if a level one alert occurs on an application, the security management team can immediately determine the seriousness of the threat without manually transferring information into the SIEM.

"With the amount of integration and correlation we can now have, ESM brings our security posture to a higher level," Beerends remarks.

In addition to managing security risk, Rabobank also uses ArcSight ESM compliance reporting to meet regulatory compliance requirements. For example, the bank must be able to prove that system administrators are following proper procedures. Every week ArcSight ESM reports on all administrator activity, allowing Rabobank to easily demonstrate compliance.

---

1 *Since the time of the original publication (December, 2016), HPE TippingPoint has been sold to Trend Micro.*

Contact us at:
www.microfocus.com

Valuable Insurance Against Damaging Cyber Attacks

As a retail bank, Rabobank is a popular target for cyber criminals who are constantly presenting new and more difficult-to-detect attacks. Moreover, the number of attacks continues to rise steadily every year. But with ArcSight ESM, Rabobank now has a powerful enterprise security management solution to uncover even the most sophisticated APTs and other cyber threats to protect its network and valuable information assets.

Beerends concludes, "ESM reveals security events to us that we were never able to detect before. We're happy with ESM and confident we can find threats before they compromise our network or disrupt business. ArcSight provides critical insurance against the damage modern cyber-attacks can inflict on an organization."

Learn More At

www.microfocus.com/arcsightesm