Solution: **IBM Security**   Industry: **Professional Services**

Excellium Services

Helping companies effectively detect and defend against security threats

In building its SOC, Excellium Services needed to rapidly and

IBM Case Studies

to reduce millions of security events to a manageable, prioritized list of offenses requiring action, helping Excellium save labor and accelerate detection and response.

Business challenge

As Excellium Services launched new security operations services for Luxembourg companies, it needed a platform to reduce the noise and help its security analysts rapidly detect and respond to threats.

Transformation

Excellium Services deployed IBM QRadar Security Intelligence Platform, which uses sophisticated sense analytics to baseline normal behavior, detect anomalies and uncover threats rapidly.

Results

More than 2X

faster time-to-value out of the box as compared to other security platforms

Highly accurate

incident detection with robust security intelligence

Optimizes

staff productivity and saves labor

Business challenge story

Helping companies more effectively detect and thwart security threats

When Excellium Services was launched in 2012, executives sought to fill a need in the Luxembourg marketplace for managed security operations center

Contact IBM

(SOC) services.

> "The security intelligence from X-Force and the out-of-the-box analytics capabilities made QRadar stand out from competitors."

—**Christophe Bianco, Managing Partner and Chief Technology Officer, Excellium Services**

With decades of experience in security operations, company executives had heard from many small-to-medium sized businesses in Luxembourg that they

IBM Case Studies

"Companies with 2,000 to 3,000 employees face the same security exposures and needs as big organizations, but they don't have the budget to build and scale their security operations," says Christophe Bianco, managing partner and chief technology officer, Excellium Services. "We heard from many in the marketplace that they were looking for a SOC service that was cost-effective and could scale to address the growing number of threats."

> "The processing and correlation of unstructured data using cognitive capabilities will give us more context for even more accurate, actionable recommendations, and will make the lives of security analysts easier on a day-to-day basis."

—**Christophe Bianco, Managing Partner and Chief Technology Officer, Excellium Services**

Contact IBM

Transformation story

Detecting threats quickly and cost-effectively

Through its EyeGuard service, Excellium offers security expertise, continuous surveillance and provisioning of all controls. Its clients represent a variety of industries—from professional services and finance to critical infrastructure organizations, such as energy and transportation companies. Excellium's SOC services have been so successful, that the company is hiring at least one security analyst each month to support client demand.

One of the keys to its success has been the use of the IBM QRadar Security Intelligence Platform, which uses sophisticated sense analytics to baseline normal behavior, detect anomalies and uncover threats rapidly.

In building its SOC, Excellium executives evaluated solutions from HP, Splunk and IBM, selecting the IBM QRadar platform based on fast-time-to-value and rich intelligence.

"The security intelligence from IBM X-Force® and the out-of-the-box analytics capabilities made QRadar stand out from competitors," says Bianco. "If we would have deployed another platform, it would require a lot more resources in order to gain a similar level of visibility."

IBM's integrated approach and extensive investment in security was also critical.

"IBM's continued investments gave us tremendous confidence," says Bianco. "For example, the addition of incident forensics, vulnerability management and risk management capabilities along with the ability to integrate feeds from other security products enables us to give each client the level of visibility they

IBM Case Studies

With the QRadar platform, Excellium can rapidly onboard new clients and deliver value within weeks instead of months.

"With other security intelligence systems, it can take months or require more money to realize benefits," says Bianco. "With QRadar, we can deliver value to a new client within four weeks, which is quite unusual in our market. We are growing rapidly because we can provide value rapidly."

Results story

Reducing "noise" and gaining highly accurate incident detection

Using the IBM QRadar Security Intelligence Platform, Excellium has been able to more quickly and accurately detect advanced threats for companies while gaining greater ease of use and lower total cost of ownership. For example, the IBM QRadar platform helps reduce millions of security events to a short, manageable and prioritized list of offenses requiring action so security analysts can meet the company's service level agreements (SLAs) for incident detection and response.

Soon, Bianco says the addition of new cognitive computing capabilities through IBM Watson™ for Cybersecurity, will help security analysts scale their expertise and make faster and more accurate security decisions.

"The processing and correlation of unstructured data, using cognitive capabilities will give us more context for even more accurate, actionable recommendations, and will make the lives of security analysts easier on a day-to-day basis," says Bianco.

Training is a critical step in the advancement of cognitive solutions, and Bianco says the work that IBM is currently doing to train the system up front will enable organizations to benefit immediately from IBM Watson for Cybersecurity. For example, during its beta test, IBM is working with leading universities and their students to train Watson on the nuances of security

Contact IBM

research findings and how to discover patterns and evidence of hidden cyberattacks and threats that could otherwise be missed.

"The work IBM is doing to train Watson in security is very important, " says Bianco. "If you can contextualize the threats, you can take real action, and that's what Watson will help us do."

EXCELLIUM
Your first call when it comes to IT and Security!

About Excellium Services

Based in Luxembourg, Excellium Services is an information security consulting and technological integration firm, guiding companies in the struggle against new threat vectors. The company's EyeGuard services provide companies with security expertise, continuous surveillance and security controls to help them protect and defend their data and infrastructure

IBM Case Studies

Solution components

- IBM® QRadar® Security Intelligence Platform
- IBM X-Force® Threat Intelligence

Take the next step

To learn more about IBM security intelligence and operations solutions, visit:

ibm.com/software/products/en/category/security-intelligence

View more client stories or learn more about IBM Security

Print

Contact IBM