Excellium Services optimizes threat detection with IBM QRadar

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.

Solution

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

Benefits

More than 2X faster time-to-value out of the box as compared to other security platforms and highly accurate incident detection with robust security intelligence. Excellium also optimizes staff productivity and saves labor.

In building its security operations center (SOC), Excellium Services needed to rapidly and cost-effectively detect advanced threats. The IBM QRadar Security Intelligence Platform used automation and analytics to reduce millions of security events to a manageable, prioritized list of offenses requiring action, helping Excellium save labor and accelerate detection and response. This way Excellium can help companies effectively detect and defend against security threats.

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 against advanced threats.

Detect and thwart security threats

When Excellium Services was launched in 2012, executives sought to fill a need in the Luxembourg marketplace for managed SOC services. With decades of experience in security operations, company executives had heard from many small-to-medium sized businesses in Luxembourg that they were having difficulty finding security experts to address the many new threats appearing daily. "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."

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

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

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.

IBM QRadar

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 need while being very efficient."

Providing value rapidly

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."

"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"

Less noise and accurate 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."

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 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."

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world- renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Belgium n.v/s.a
Avenue du Bourget/Bourgetlaan 42
1130 Bruxelles

IBM Nederland B.V.
Johan Huizingalaan 765
1066 VH Amsterdam

IBM Belgium sprl - Luxembourg Branch
Parc d'activités WestSide Village
89C rue Pafebruch
L- 8308 Capellen

Produced in The Netherlands -01-2017

GVC00000-LXEN-01