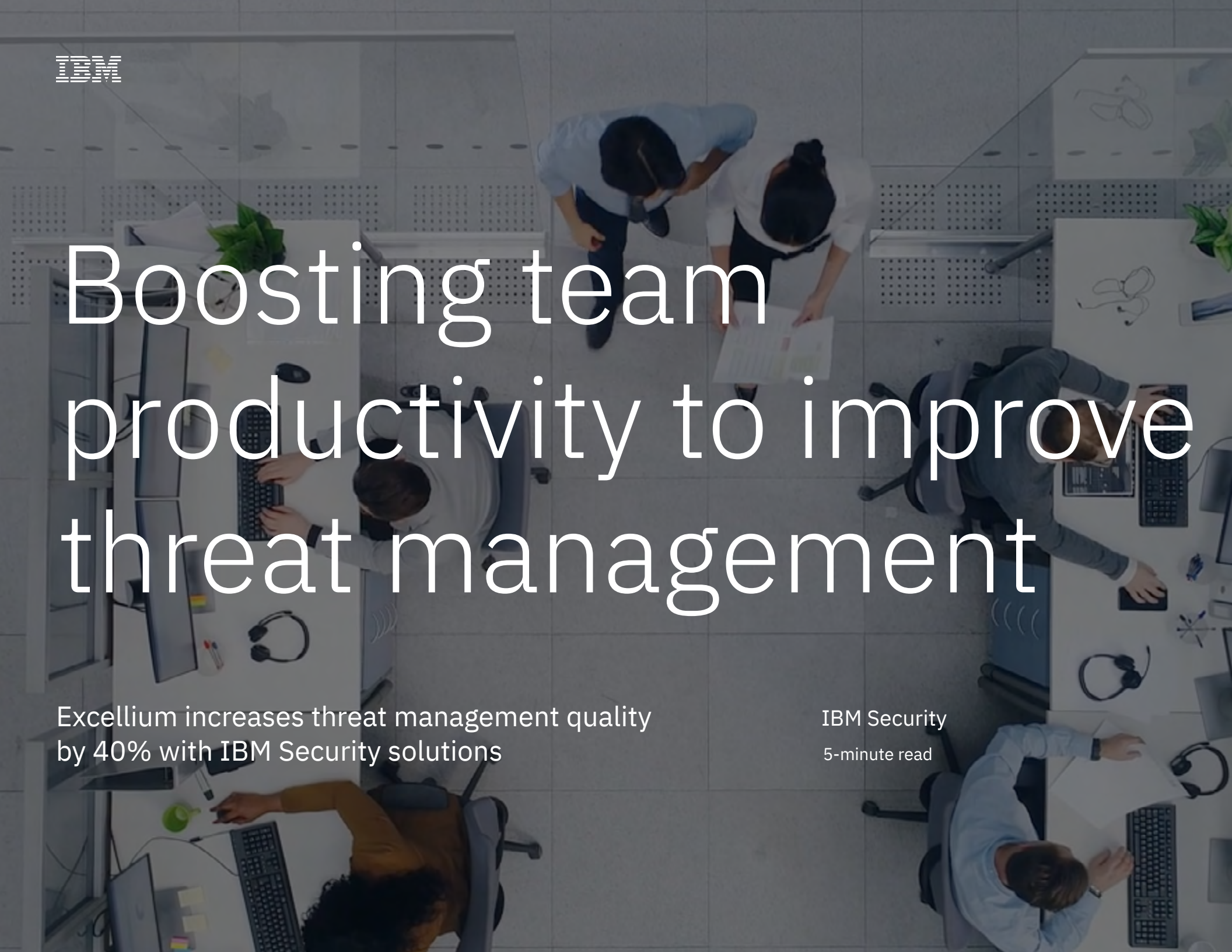


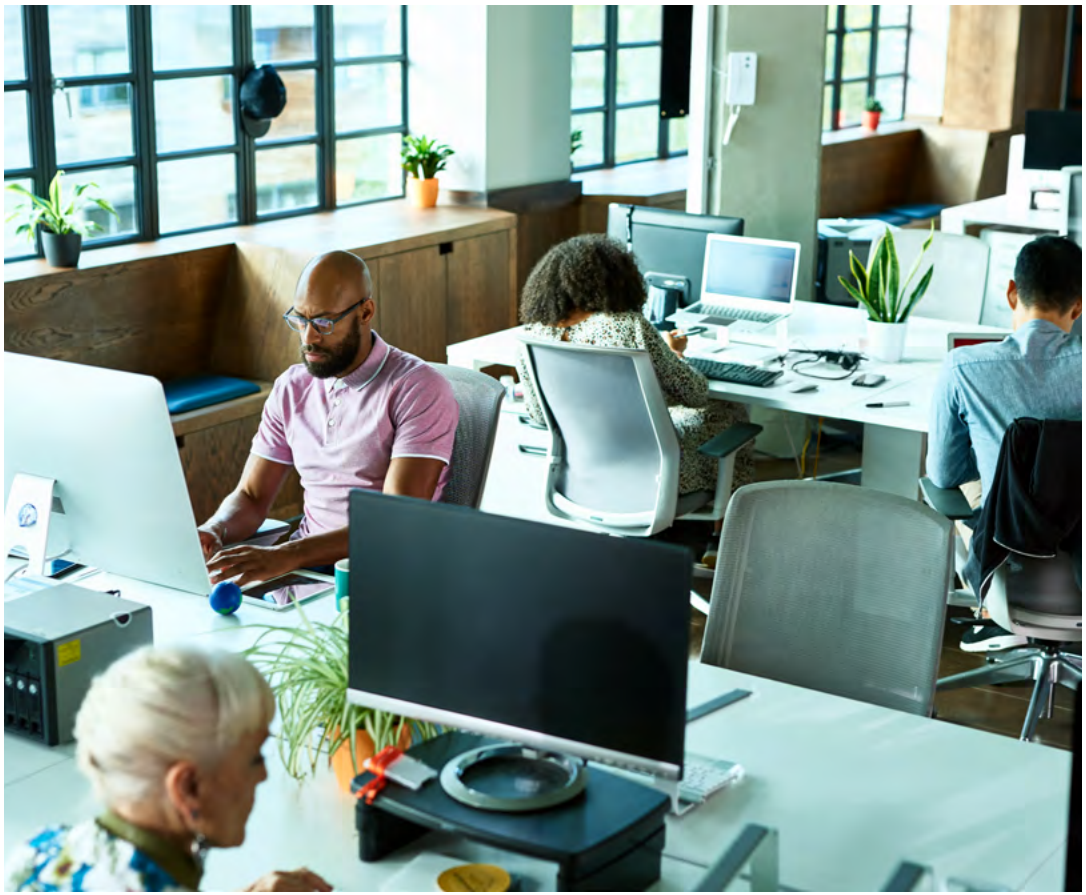
Boosting team productivity to improve threat management

Excellium increases threat management quality by 40% with IBM Security solutions

IBM Security

5-minute read

TrickBot. Gozi. NovaLoader. BackSwap. ShadowHammer. These are not monikers for superheroes or constellations. They're the names of malware, ransomware, botnets and other cyberattacks that pose serious threats to organizations, infrastructures and even society. And new, more complex threats emerge each year.



According to the IBM® X-Force® Threat Intelligence Index 2020 report, over 8.5 billion records were breached in 2019 — more than three times greater than 2018 year-over-year. To make matters worse, there's a chronic shortage of skilled IT security professionals to combat these threats, and many organizations struggle to hire and retain talent.

The combined relentlessness of cyberthreats and lack of skilled workers have changed the relationship between organizations needing security services and those providing

them. With internal IT security teams overwhelmed, small to midsize businesses (SMBs) look to managed service providers for intelligent security solutions to help protect their digital assets. In effect, the responsibility of managing, detecting and mitigating threats is becoming a collaborative effort.

Therefore, when Luxembourg-based Excellium Services SA launched its proprietary cybersecurity management solution, EyeGuard Cyber SOC, in 2013, it filled an urgent need for cost-effective and scalable security services. Built on IBM QRadar® next-generation Security Information and Event Management (SIEM) technology, the EyeGuard platform allows organizations to monitor their critical assets in real time so they can detect and respond to malicious activity quickly and proactively.

By subscribing to EyeGuard Cyber SOC Services, Excellium customers can extend the capabilities of their internal security teams. SMBs gain the expertise of EyeGuard professionals who provide services such as 24x7 advanced and proactive asset monitoring based on defined service level agreements (SLAs). They also identify external vulnerabilities and help customers develop security policies and procedures.

“Data breaches happen on a regular basis, and lack of resources is a real issue,” explains Christophe Bianco, Co-Founder and Managing Partner at Excellium. “So the trend in cybersecurity is that customers are looking for partners, more than just resellers of technology. Customers are saying, ‘I need you to complement my operation, to be an extension of my IT operational security team in the context of a resilience need.’”

But the lack of skilled specialists isn’t just a challenge for Excellium customers; Excellium itself also felt the staffing pinch. Since launching its SOC platform, the company has grown from six to more than 120 employees. Already a trusted provider for more than 180 organizations, its customer base is growing rapidly while Excellium expands into new markets and regions.

“Because there are more regulations and digitalization, the need for security is huge,” says Bianco. “But resources are scarce. For us to manage and deliver more services to customers, we needed to increase our efficiency and the productivity of the people in our SOC services. And to sustain our growth, we needed to develop our capabilities and transform emerging technology into a service for our customers.”

"With Resilient, we can scale more rapidly with fewer resources."

Christophe Bianco, Co-Founder and Managing Partner, IBM Business Partner Excellium Services SA

Expects to improve quality of threat management by

40%

by formalizing security processes

Speeds autonomy of new employees up to

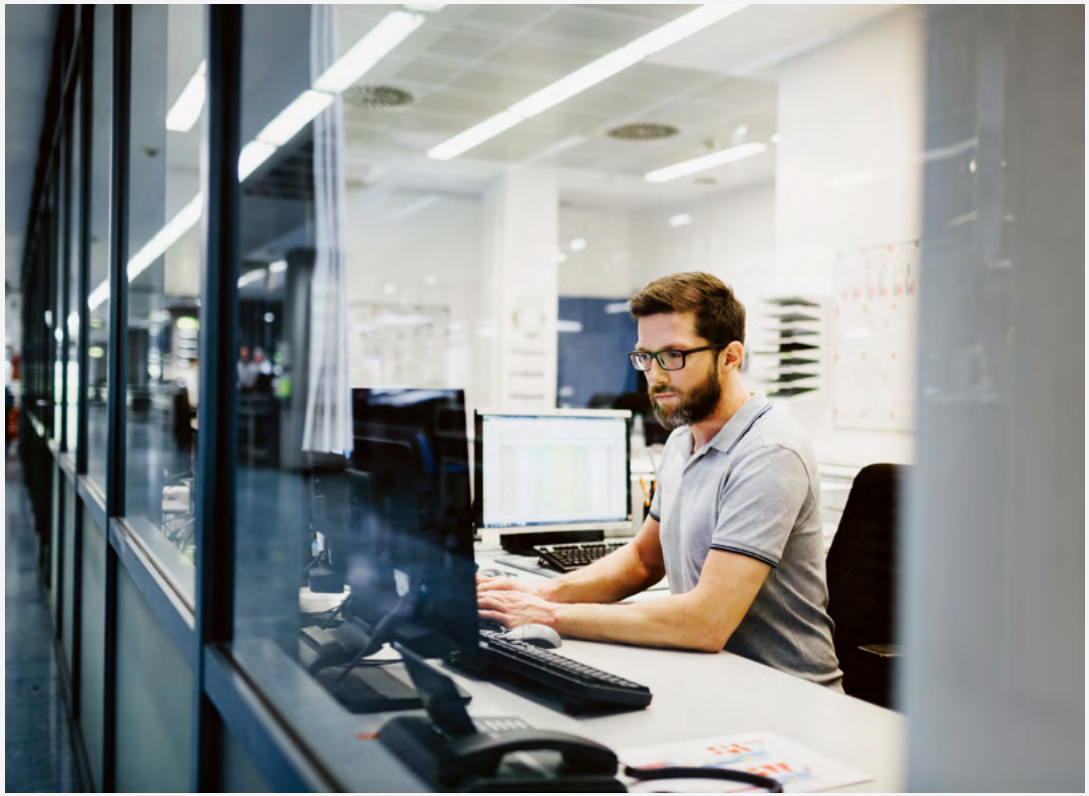
30% – 40%

by automating response procedures

Solutions that give threats no place to hide

To support the efficiency and productivity of its SOC team and expand the capabilities of its overall security technology ecosystem, Excellium is implementing a host of IBM Security® offerings.

A key technology is the IBM Resilient® Security Orchestration, Automation and Response (SOAR) Platform. The platform automates tasks related to handling cyber events, such as data breaches, and orchestrates the people, processes and technology associated with incident response. Through integration with Excellium's existing QRadar SIEM technology, the



Resilient SOAR Platform can share data and provide action plans to help SOC teams respond to and remediate security events faster. It also provides intelligence and context around incidents, giving Excellium the insight it needs to respond to more complex cyberthreats.

The company also uses Resilient SOAR technology to support expansion into new markets and connect new customers and partners to its operations. Through the platform, Excellium can better ensure all analysts and security specialists are following the same governance, processes and methodologies, no matter their location. By doing so, the company can offer consistent high-quality service to its customers near and far and better mitigate noncompliance risks and penalties.

"Customers are generating more and more events for us to manage and consider, so we need to automate and formalize our processes," Bianco elaborates. "Resilient allows us to expand our processes and governance inside our partners' operations so we can deliver services transparently to customers. With Resilient, we can scale more rapidly with fewer resources."

According to a white paper by Enterprise Management Associates (EMA), 99% of cyberattacks traverse the network in some way. To expand its network visibility, Excellium implemented IBM QRadar Network Insights software. The technology helps analysts gain a deeper understanding of network traffic to identify suspicious or malicious activity in real time. It also provides additional network context that helps security analysts make decisive triage decisions.

Finally, Excellium incorporates intelligence from the IBM X-Force Exchange platform into its SOC service offering. With X-Force Exchange, the company gains access to critical information and reports about the latest security incidents and threats, such as potentially malicious IP addresses.

"We're always looking for additional technology we can plug into the QRadar SIEM capability to improve our ability to detect and react to threats," says Bianco.

A SOC team that can do more, better

With IBM Security offerings supporting its operations and EyeGuard Cyber SOC Services, Excellium is improving the productivity and efficiency of its security analysts, and onboarding partners and customers more quickly. It also expects to enhance the quality of its incident management.

Excellium can formalize its processes and operations across locations and partners for more consistent service delivery. SOC teams also have more context, insight and intelligence about security threats, enabling them to adapt their remediation strategies accordingly.

Bianco has high expectations: “The quality of the service we deliver should increase significantly because it’s consistent, regardless of who’s in the operation at the moment of an incident. So, I’m expecting at least a 40% improvement in the quality of incident management.”

By automating tasks and processes that were once manual and mundane, Excellium’s SOC teams can focus their time on what they were hired to do: detect and remediate threats.

“European customers understand that it’s quite impossible to detect everything,” explains Bianco. “What they expect is that we go deeper in the way we look at their system from a risk-based approach. With Resilient, we can focus more on the premium activities — going deeper into analyzing and deeper into the customer’s information system to target the big challenges, like a massive threat on a key system.”

In 2016, one of Excellium’s many customers faced a significant outage.

Bianco recalls: “At the time, we were already their security provider. We detected and responded to the threat and limited its impact on the business. But more than that, we developed and deployed all the capabilities to help them restore production as fast as possible. And by focusing on restoring production, we became a trusted partner.”

As Excellium expands into Africa and other markets, it’s also using Resilient technology to expedite the partner onboarding process. In the past, because the company had to deploy the necessary technologies and conduct training, getting a new partner up to speed could take several months. The company would then have to manage interactions between the disparate teams to ensure consistent incident response.

Today, Excellium can connect with new partners through the Resilient SOAR platform, significantly speeding the onboarding process. “We are expanding our business quite thoroughly in Africa. Unfortunately, I’m not growing my SOC capability at the same speed that I’m onboarding customers,” explains Bianco. “Using Resilient is a way for me to onboard a partner in my operation and have him follow my process, my governance and my documentation, but with his own local capability. Now, we expect that we can plug them into our operation and make them operational in less than two months.”

Excellium also onboards new customers more quickly, enabling Bianco’s team to detect threats faster. “The concern

for our customers is a breach at the business application level," he says. "But it used to take us a long time to onboard a customer, get the processes in place and start detecting. With this technology, I expect to onboard them in about half the time it used to take."

Inside Excellium's SOC, new employees are quickly becoming more autonomous when it comes to process workflows and governance; in fact, up to 30% – 40% faster. Previously, it took 6 – 8 months before new hires could run a shift by themselves. "Now, because Resilient supports our processes, new employees can be guided more quickly," says Bianco. "In one month, an employee can be operational."

According to Bianco, IBM Security provides Excellium with a competitive edge over larger companies. "Our main difference compared to our competitors is agility and proximity," he concludes.

"Resilient allows us to expand our processes and governance inside our partners' operations so we can deliver services transparently to customers."

Christophe Bianco, Co-Founder and Managing Partner, IBM Business Partner Excellium Services SA

About Excellium Services SA

Founded in 2012 and based in Contern, Luxembourg, IBM Business Partner Excellium (external link) is a leading cybersecurity and SOC services provider with strong competences in integration, consulting and auditing. It offers a broad range of customizable services for financial, multinational and governmental organizations and serves more than 180 customers in seven geographies. Excellium has expanded operations in Belgium, France, Senegal and Morocco and employs more than 120 people, including 100 cybersecurity specialists.

Solution components

- IBM® QRadar® Network Insights
- IBM Resilient® Security Orchestration, Automation and Response (SOAR) Platform
- IBM Security®
- IBM X-Force® Exchange
- IBM® X-Force Threat Intelligence