IBM

Accelerated security threat detection and priority response

Integrating data, analyzing logs and prioritizing incidents speeds up threat remediation

by Tom Farre

5-minute read

As enterprises pursue digital transformation, they face increasing danger from cybersecurity threats. COVID-19 has caused a massive increase in the number of vulnerable endpoints for remote workers. Employees, partners, suppliers and customers access company resources on multiple devices from virtually anywhere, further raising vulnerability. And the penalties and bad publicity from data breaches can set back any business.

Such issues were recently on the mind of Tran Phu Nghia, Cybersecurity Director at NovaGroup, parent company of the Novaland real estate investment and development firm in Vietnam.

"Enterprises have to maintain a good reputation, yet cyberattacks are on the rise because criminals can use the internet to attack without limit," Nghia says. "Users are subject to phishing attacks from cybercriminals. They scan systems every day and at all times are trying to gain customer lists and intellectual property. And security teams must be vigilant against insider threats."

Adding to the challenges, enterprise systems may be siloed and security log data unintegrated. This makes it difficult to analyze the data and proactively plan for cyberattacks. Plus, security tools often generate false positives, making it hard to prioritize serious threats and resolve them quickly.

In assessing these challenges and Novaland's security posture, the security group resolved to add a centralized Security Information and Event Management (SIEM) solution, a foundational tool for cybersecurity management. But which one to choose? To make the selection, the security teams evaluated leading security solutions. They chose the IBM Security® QRadar® SIEM platform.

The IBM Security QRadar SIEM platform

accelerates

cyberthreat detection and response

Intelligent analytics built into the QRadar platform significantly

reduce

the investigative workload

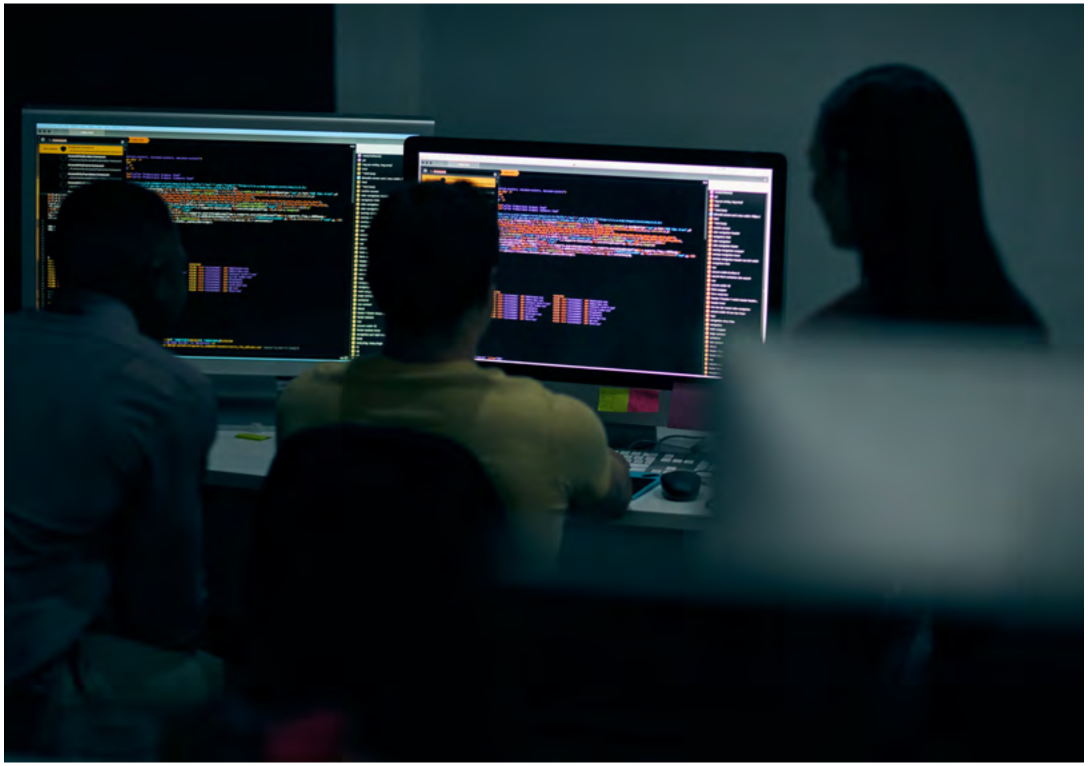
The QRadar platform is cost effective for Novaland because it

boosts

the security team's productivity

Powering a foundational security ecosystem

In evaluating the SIEM solution landscape, Novaland's cyber group considered research from Gartner, Inc. and Forrester, comparing a range of offerings among the leading brands. "Gartner rates IBM Security QRadar particularly high for hundreds of use cases and it supports the largest information security ecosystem," says Nghia.



The evaluation team liked QRadar's ability to automate security information analysis to quickly detect threats; its stability and extensibility; and its integration of a variety of components such as extensions, APIs and the IBM QRadar Pulse operational dashboard, which streamlines monitoring and administration. The team also liked that QRadar is open and scalable, and that it offers features in line with Novaland's operational requirements to ensure business resiliency, data security and privacy.

"We decided that IBM QRadar was a highly suitable solution because of its features and its scalability," explains Nghia. "And the threat detection rules are adaptable to our needs."

Assisted by IBM Security Services, Novaland's cyberteam deployed the QRadar SIEM platform. Then, the team used the tool to perfect incident response procedures and scenarios, optimize rule sets to identify attack signs, and develop playbooks for security incident response.

Novaland also uses the QRadar platform to strengthen the IT environment against future threats. Separated into Red, Blue and Purple teams, the cyber group meets weekly to review past threats, note the teams' responses and use the results to customize QRadar incident response playbooks. In addition, the Red team uses tools and their own scripts to conduct Breach and Attack Simulation (BAS) to verify the Blue team's efficiency.

"We need to understand how fast the Blue team can respond—does it take 15 minutes or 50 minutes?" Nghia says. He is pleased with typical responses in the 15 – 30 minute range. "It's just faster with QRadar."

> "We decided that IBM QRadar was a highly suitable solution because of its features and its scalability. And the threat detection rules are adaptable to our needs."

Tran Phu Nghia, Cybersecurity Director, NovaGroup

Protecting systems, information and intellectual property

Accelerated threat detection and fast response are clear advantages of the IBM SIEM solution. But its intelligent analytics also save time by lessening the number of false positives for investigation. Novaland’s Blue team uses it to optimize the rules that detect cyberattacks. This reduces the number of incidents detected from as many as 1,000 per day to less than 100, and the prioritization lessens the team’s workload by pinpointing the most dangerous threats.

> “We need to understand how fast the Blue team can respond. It’s just faster with QRadar.”
>
> **Tran Phu Nghia**,
> Cybersecurity Director,
> NovaGroup

These capabilities help Novaland better protect its systems, customer information and intellectual property—thereby strengthening the trust of investors and customers. And the solution is cost effective due to the security team’s higher productivity. “Without using QRadar, we would have to expend more human resources to protect our siloed systems,” Nghia says. Another plus is that free training from IBM Security Services has raised the security team’s skillset.

Looking ahead, Novaland’s security group is exploring an upgrade to the IBM Security QRadar SOAR Platform. Standing for Security Orchestration and Response, SOAR provides more intelligent threat detection, faster incident response and continuous improvement of response processes.

Integrated data, faster threat detection, more productive analyses and faster responses all come from IBM’s cost-effective security ecosystem. “Multiple tech vendors have come to us to promote their cybersecurity capabilities,” says Nghia. “IBM is the priority choice for now.”

Based on his experience at Novaland, what advice does Nghia have for enterprises that want to improve their cybersecurity capabilities? “The quickest way to boost cybersecurity capabilities is to ensure the cybersecurity teams keep listening, observing, analyzing, troubleshooting and cooperating,” he says. “This way, an enterprise can develop teams and procedures to enhance cyber resilience together.”

About Novaland

With over 10,600 hectares of land bank, Novaland (external link) focuses on developing three key product lines: Residential Real Estate, Hospitality Real Estate and Industrial Real Estate. Through a journey of 30 years of establishment and development, Novaland currently owns a portfolio of more than 50 projects with trend-leading projects and products in Residential Real Estate and large-scale Residential Hospitality Real Estate. Novaland is one of the 30 largest listed companies by market cap on HOSE (VN30 Index), and also has international convertible bonds listed on the Singapore Stock Exchange (SGX).

Solution components

- IBM Security® QRadar® SIEM
- IBM Security QRadar SOAR Platform
- IBM Security Services

Produced in the United States of America, April 2022.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.