Relieving pandemic pressure on security operations teams

Securing networks and data

Use case

Cybercriminals see the “new normal” of COVID-19 as an opportunity to be exploited: they’re adjusting their phishing campaigns and malicious apps to capitalize on the fear associated with the pandemic and people’s need to stay connected. To secure their networks and data when overall traffic is up and user traffic patterns have shifted dramatically, CSPs need automated processes powered by machine learning and artificial intelligence to dynamically scan for threats and determine the best response.

This use case looks at how CSPs can use Nokia NetGuard Adaptive Security Operations — either as an in-house solution or a managed security service delivered by Nokia — to control access to the network, manage certificates for remote workers, and detect and respond to threats in a proactive way.
Use case
Relieving pandemic pressure on security operations teams

CHALLENGE

Less secure networks, bolder attackers

The risk of malware infections and data breaches has may be never been greater. Huge numbers of people are working from home due to shelter-in-place orders, accessing corporate servers and systems remotely. But most home networks aren’t as secure as those at the office — and employees are likely to mix work with personal network-related activities when at home. Large businesses may already have been set up to support secure remote computing, but COVID-19 has put a massive strain on their infrastructure. Smaller businesses, however, are struggling to implement secure access from home.

It’s a situation that cybercriminals are using to their advantage. Over the past few months, hundreds of new COVID-19 domains have been registered, half of them thought to be involved in malicious activity. Hackers are launching broad spam attacks as well as highly targeted, email-based phishing campaigns that prey on people’s need to stay connected during the pandemic. Remote workers are being tricked into activating malware (though infected videoconferencing apps, for example) that gives cybercriminals full access to their companies’ servers and systems.

A proper defense should be proactive, fast and highly automated. But during this challenging time, not every CSP has the in-house skills or resources to protect their networks — and in turn, their customers — against the full spectrum of increasingly sophisticated cyber threats.

70% of all cyber attacks involve accessing privileged accounts using credentials stolen in phishing schemes
APPLICATION

When the CSP is the last line of defense

The COVID-19 pandemic is pushing many CSP security operations teams toward their breaking point. The network is generating a huge number of security alerts, driven by surging traffic volumes. Unable to effectively analyze and prioritize that flood of alerts, many legitimate security incidents are being missed or not being investigated as thoroughly as they should. And because COVID-19 has disrupted the predictable network traffic patterns, unusual behaviors — the kind that could indicate botnets, denial of service attacks and other malicious activity — are much harder to spot.

On top of that, the security operations team is a shell of its former self. Some security analysts may be sick with the virus. Others are working remotely from home. The men and women who remain on site are overwhelmed and overworked, scrambling to keep up.

So what can be done?

Fighting the growing volume of threats posed by COVID-19 requires automated operational workflows and integrated threat intelligence. A high degree of integration enables greater collaboration between security analysts, no matter where they’re located. And when intelligence is embedded across multiple vectors (e.g., endpoints, privileged user access, machine communications), CSPs can detect and analyze potential threats in real time, as soon as they appear, to determine whether they’re malicious or not — capabilities that are critical to guarding against spear-phishing and zero-day attacks that can evade traditional signature- and reputation-based security.
SOLUTION

Security operations optimized for the COVID-19 era

To keep pace with cyber threats in the COVID-19 context, CSPs need to be able to scan for threats, identify and fingerprint new threats as they arise, and understand how best to respond to them, all in real time. Nokia’s telco-centric security orchestration, analytics and response (SOAR) suite, Nokia NetGuard Adaptive Security Operations (NASO), can help by providing an integrated, end-to-end approach to network security.

NASO aggregates, analyzes and correlates security data from a variety of network and system sources, including security information and event management (SIEM) solutions, firewalls, endpoint detection and response (EDR) tools, ticketing systems and other critical security technologies — saving hundreds of hours in manual effort. It enriches that information with telco-specific data (such as radio/core network elements, network performance and customer experience management tools), helping security operations teams assess risk and make smarter decisions when responding to threats.
Cyber playbooks define the incident-response processes and workflows so they can be fully orchestrated and automated across the entire network, improving median time to detect and respond to security incidents.

Integrated, end-to-end security with Nokia NetGuard Adaptive Security Operations

With the automation and intelligence built into NASO, security operations teams are able to:

- Constantly monitor and measure security posture and risk levels across all endpoints and network sessions
- Manage and limit access to key operational systems and assets, protecting against accidental or deliberate misuse of privileged access as more remote workers log in from their home computers
- Detect threats much earlier in the mitigation chain and reduce the number of false positives, saving analyst time and preventing alert fatigue
- Respond rapidly to minimize the impacts of cyberattacks, minimizing the time analysts have to spend handling each incident
Managed security services

CSPs that have smaller security teams or lack the in-house skills to cover the full spectrum of cyber threats may want to consider having Nokia take on the day-to-day management of their security operations.

Our security intelligence and operations center is well staffed and has expertise in both telco-specific and general enterprise IT security architecture and compliance requirements. It also offers the latest security technology (including artificial intelligence and machine learning techniques) with a high degree of automation.

Nokia’s three tiers of managed security services

CSPs can even sell Nokia Managed Security Services as a “white label” offering under their own brand to their own enterprise customers. Our team delivers the services on the CSP’s behalf, providing behind-the-scenes consultancy, planning, implementation and monitoring. Given that the consequences of a data breach or ransomware so severe, many enterprises are turning to managed security service providers for support — making this an excellent opportunity for CSPs to enhance their brand and improve both customer retention and referrals.

We also offer short-term, COVID-19-related transactional emergency security services, including awareness training on pandemic-related cyber threats, remote vulnerability and security configuration management, and monitoring of select critical systems.
Use case
Relieving pandemic pressure on security operations teams

BENEFITS
Keeping customers protected and secure

An automated, intelligent approach to security operations makes it possible for CSPs to:

- **Reduce the risk** of security breaches and malware infections among their enterprise customers
- **Respond rapidly and proactively to threats**, using threat intelligence from across the network to eliminate the time between detection and mitigation
- **Decrease the manual effort** required to analyze and prioritize security alerts
- **Relieve the pressure** on their security teams by automating threat detection and response workflows
- **Deliver managed security services** with greater confidence

Quick solutions to secure network performance and scale to meet dynamic demand

COVID-19 has had a huge impact on all of society and especially how people connect and communicate. By embracing automation and intelligence in their operations, CSPs can overcome the immediate challenges they face today during the pandemic, including the need to secure their customers’ networks and data. By adopting these capabilities today, CSPs will also set themselves up for longer-term 5G success: automation and AI will be essential to capitalizing on 5G opportunities in new vertical markets and assuring end-to-end quality across a diverse range of use cases and business models.

The investments CSPs make today in operations automation and intelligence will pay off in the long run as they evolve toward the 5G era.

Nokia offers a robust portfolio of software-based solutions that can be deployed quickly and remotely right now to help CSPs overcome their COVID-19 challenges, often with no extra hardware or on-site installation required.

Find out how you can deliver the extraordinary during the COVID-19 crisis. Visit our Operations in 5G webpage to learn more.
About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2020 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: SR2005043900EN (May) CID207506