Faster response based on Threat Intelligence

NetGuard Endpoint Security TI helps to react to security alerts

Use case

Chief Information Security Officers (CISOs) and senior IT executives make strategic decisions about cybersecurity. They need to allocate human and technical resources to where they can have the biggest impact reducing risks.
Nokia’s Threat Intelligence information reduces the analyst’s time and effort in responding to security alerts, moves security response earlier in the kill chain, and establishes a methodology for responding to future attacks. NES TI distinguishes between real threats and hype, and simplifies communication with the CEO and board.

Situation

The majority of successful cyber attacks are effectively zero-day, exploiting unknown software vulnerabilities. They can easily evade “set it and forget it” prevention-based tool sets that block potential threats based on signatures and known patterns of behavior. The traditional strategy of waiting for an attack is no longer enough. Protecting data in today’s complex threat environment requires actionable intelligence that can be used to develop informed tactics for mitigating current threats, and to plan for threats that may exist in the future.

Threat intelligence services provide high-quality, actionable information about the security threat environment that most enterprises cannot derive on their own.

Solution

Threat intelligence is one way for security analysts to respond to different cybersecurity threats they face. Threat intelligence is a way to gather up multiple security threads – from ransomware to malware and more – and then come up with an actionable plan to best respond to those threats.

NetGuard TI provides security experts with information to help assess the risks, impact and further objectives of an attack and to prioritize a proper response. For example, it is a way for security analysts to identify outbound connections to an external IP address known to be an active command and control server.

Data from NetGuard TI can be integrated with NetGuard Security Management Center (SMC) or any SIEM platform in the form of watch lists, correlation rules and queries in ways that increase the success rate of early breach detection.

Benefits

• Reliable and actionable intelligence from NetGuard can help the CISO and IT executives:
  • Identify and prioritize risks based on threat intelligence that’s relevant
  • Make better strategic decisions on security budgets and staffing.
  • Respond effectively to incidents through a better understanding of threat actors and their tactics, techniques and procedures.
  • Keep top management aligned about risks, threats, security preparedness and responses.
About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

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.

© 2018 Nokia

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1805025089EN (May) CID205170