Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING WHITE PAPER

Cloud Security Strategies:
The Power of Proactive Processing

A Heavy Reading white paper produced for Nokia Networks

NOKIA

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

Communications service providers (CSPs) are now more than five years into their network functions virtualization (NFV)-based cloud virtualization journey. Although during this period CSPs have made measurable progress in transforming their networks, they have also encountered formidable challenges.

Unfortunately, the pace of change in the next five years will likely only increase as mass commercialization of CSP cloud networks is realized. And one topic that will continue to figure prominently in the discussion is cloud security.

As it stands, securing the cloud is already a major concern, but looking forward we anticipate an even greater number of challenges to materialize. In our view, the fundamental driver here is the fact that the measures and processes required to secure telco networks are fundamentally changing. This change is driven by the need to rely exclusively on automated software-based systems that integrate advanced intelligence techniques to enable proactive security enforcement leveraging analytics and automation.

Accordingly, in the third quarter of 2017, Heavy Reading, in conjunction with Nokia Networks, undertook the creation and execution of a global survey designed to assess CSP readiness to support these advanced cloud-driven security techniques. The key findings from the survey are documented in this white paper.

THE PERIMETER PREDICAMENT

One of the attributes of the cloud that is driving this seismic change in security management is the cloud-native service delivery model that embodies it. Specifically, this translates into an unlimited software distribution model in which service logic and accompanying security policies are reused and natively pushed as close to the user as possible, to minimize service latency and maximize end-user programmability.

This concept of unlimited software distribution at the edge is currently driving 5G architecture, the Internet of Things (IoT) and multi-access edge computing (MEC). While these three technology waves have major security impacts in their own right, we believe they are only the first wave of many that will require increased security vigilance.

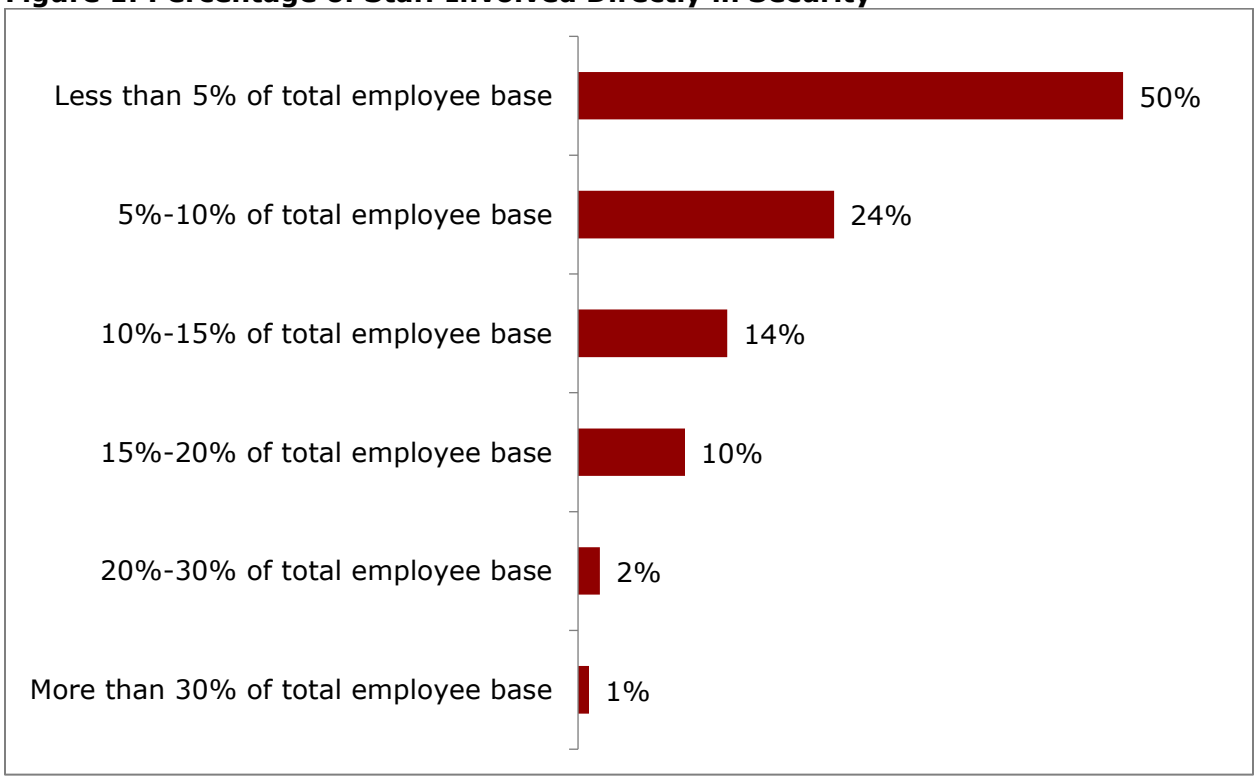
Accordingly, achieving a workable cloud security strategy will require CSPs to adopt new approaches and quickly shift from the practices and processes they have relied upon and trusted in the past. One area we believe CSPs must immediately address is an acceptance that the concept of a well-defined network security perimeter is no longer conceptually relevant in a cloud-native deployment.

In a security context, the changes associated with the perimeter predicament are profound. The reality is that traditional network-centric approaches to security, which focused on deploying security heavily at the perimeter, are no longer sufficient, given that the conventional notion of a network perimeter is no longer valid. This started with mobile devices such as smartphones and will accelerate as more and more IoT devices and services emerge. However, in reality, even today CSPs are confronting the daunting task of securing a massive attack surface.

At the same time, the historical focus on legacy network perimeters means that CSP security teams are inherently small and can become easily overextended when dealing with the new cloud requirements.

This reality is reflected in **Figure 1** below with survey input confirming that security experts represent a very small percentage of total CSP staff. For half of the respondents, this equates to 5 percent or less. For 24 percent, security experts constitute only 5 percent to 10 percent of the total employee base.

Figure 1: Percentage of Staff Involved Directly in Security

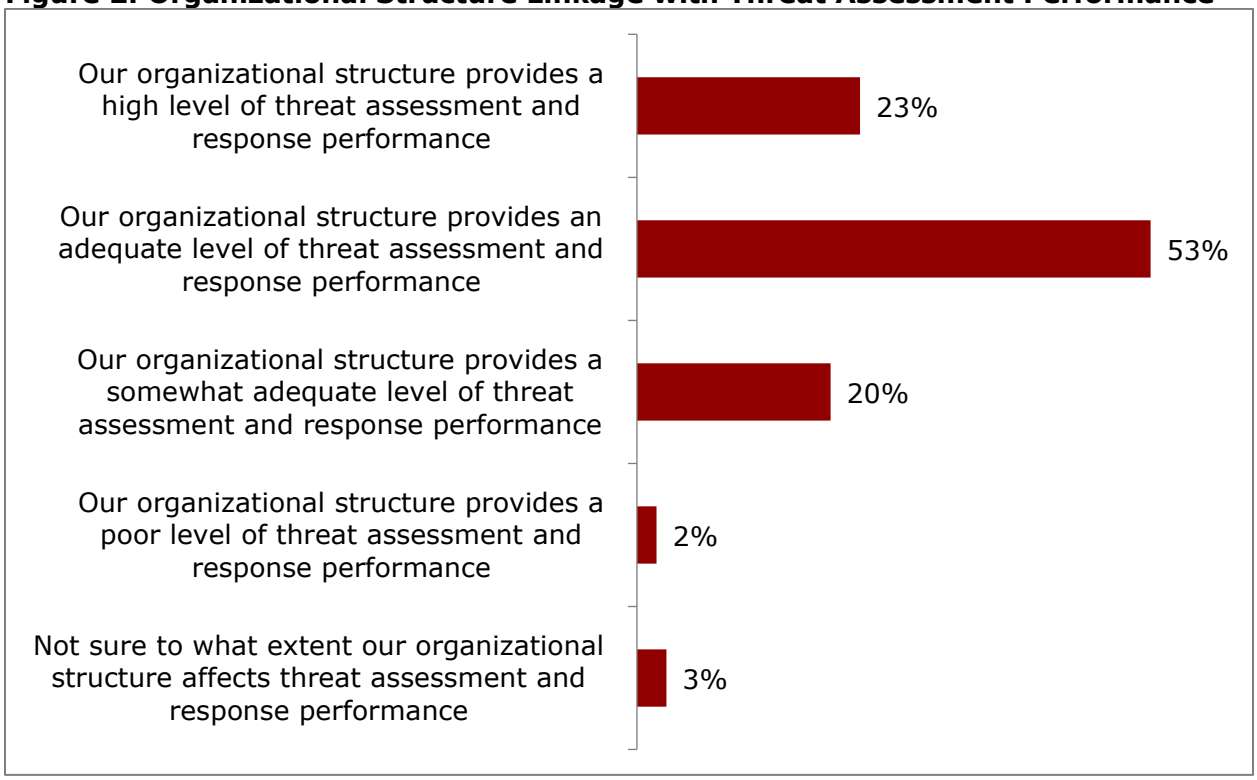


Question: What percentage of your company's total staff is involved directly in security? (N=102)
Source: Heavy Reading Nokia Networks Custom Survey Q317

Additionally, these CSPs will also need to reconsider organizationally how these precious team resources will be utilized within the corporate structure in a cloud environment. Just as the physical security infrastructure can no longer be simply deployed at the perimeter, security team resources must also be reorganized to be fully integrated into the corporate structure to foster cross-training and strategic information sharing.

This cultural requirement was also noted in the survey data. As depicted in **Figure 2**, more than half of the respondents (53 percent) felt that the current organizational structure provided an "adequate" level of threat assessment and response performance. While this metric does constitute a "passing grade," it does not indicate that CSPs have in place an organizational structure that is sufficiently "hardened" to withstand a major cyber event. Even more disconcerting is the 22 percent of respondents who assessed their readiness as either only "somewhat adequate" (20 percent) or "poor" (2 percent).

Figure 2: Organizational Structure Linkage with Threat Assessment Performance



Question: Which of the following best reflects the overall state of your company's security threat assessment and response performance? (N=99)
Source: Heavy Reading Nokia Networks Custom Survey Q317

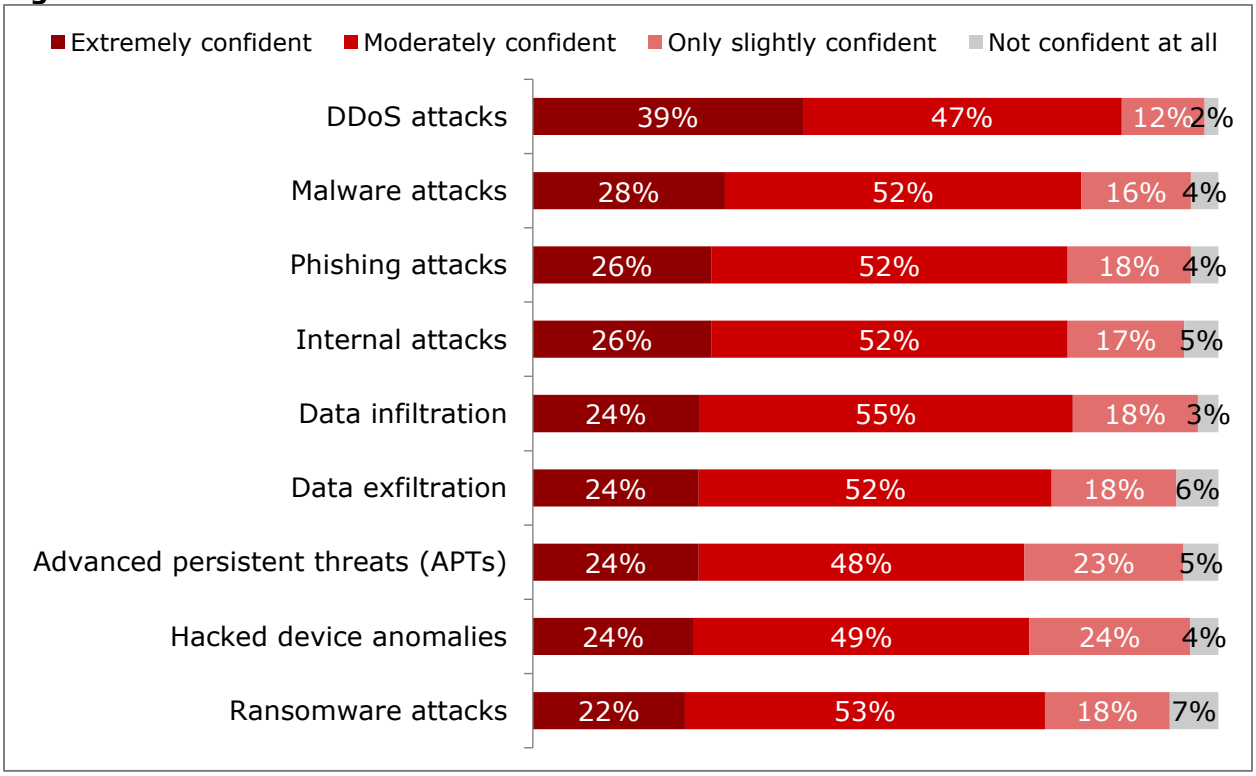
Given the above, there is little doubt that CSPs will need to both scale up and reorganize their security teams to manage the additional cloud security requirements associated with 5G, IoT or even delivery of managed security services to enterprises.

Yet even without factoring in these considerations, we believe CSPs must adopt new security measures and strategies, given that the baseline number of threats continues to escalate year-over-year, which hinders their ability to investigate cyber incidents. Based on data from Nokia, larger organizations are now receiving 10,000 alerts per day, of which only 30 percent are investigated. Further, both internal data from Nokia and various external sources, such as the Ponemon Institute, indicates that approximately 72 percent of these alerts are false, which needlessly ties up valuable security team resources.

Because the volume, velocity and variety of security data are overwhelming security teams, CSPs need additional resources. As a result, as depicted in **Figure 3** approximately half of CSPs are only "moderately confident" in their ability to detect a broad range of threat vectors, and only approximately 25 percent of CSPs are "extremely confident" that they have in place the technology and processes to meet or exceed current threat detection requirements.

With 5G and IoT on the horizon, this must change – and rapidly – since a moderate level of confidence can at best deliver only a moderate level of security enforcement success, which will be unacceptable in meeting the advanced security requirements of a fully loaded commercialized telco cloud.

Figure 3: Threat Detection Confidence



Question: How confident are you in your company's ability to detect the following threat or event types? (N=98-100)
Source: Heavy Reading Nokia Networks Custom Survey Q317

Although adding additional resources and deploying them in an optimized organizational structure will most certainly assist CSPs in navigating the threat landscape, it is really only half of the equation. The second consideration is the need to provide these resource teams with more intelligent tools and capabilities, based on automated processes that support a real-time proactive response model.

SECURITY SYSTEM AUTOMATION & THE PROACTIVE PROCESSING PARADIGM

As noted, working more intelligently demands a new security reference model: one that is based on the adoption of automation and analytics. Both of these are vital, since they provide the required level of visibility necessary to understand – and proactively respond to – threat patterns that the network is experiencing in real time. Accordingly, in this section of the white paper, we consider in greater detail the attributes and security characteristics of analytics, automation, and the proactive processing paradigm they empower.

Analytics is the logical starting point for the discussion, since it provides the foundation for automation and proactive response. In this context, analytics delivers a real-time view of network security performance, which is crucial to providing the level of distributed visibility required to secure the entire cloud.

While the application of analytics is conceptually straightforward, it's important to note that over the past four years, analytics – in lockstep with the adoption of NFV – has also undergone a significant shift, transitioning from a solitary, silo-based model to a multi-dimensional model.

This multi-dimensional model is critical, since it enables CSPs to seamlessly and uniformly apply analytics across a variety of systems to identify threats that may be otherwise missed. This, in turn, means it is possible to identify anomalies from normal behavior, to minimize time spent on false positives. The other value of this multi-dimensional view is that it fosters a holistic integration of analytics with automation and machine learning into security processes.

Within this holistic integration model, analytics is used as the first step to proactively identify harmful actors, which helps security analysts prioritize risk, while automated software security systems and processes are used to control and limit access to key operational systems and assets. While this may at first glance appear to be a logical progression, it does represent a major step up from the current security model, in which analytics and limited automation tools – if they exist at all – are supported via an *ad hoc* system model.

As a result, while legacy *ad hoc* security incident response strategies are hampered by prolonged response and mitigation times, they are also burdening the precious security team resources with too many manual processes that ultimately restrict their ability to keep pace with the diversity and dynamic velocity of threat vectors.

In contrast, the analytics- and automation-based proactive security model is designed to support a new performance level. Adoption of this model requires a shift to automated processes that can support a broad range of responses to meet the needs of the individual services, and that delivers the flexibility to proactively respond and secure any application, anywhere in the cloud, in real time.

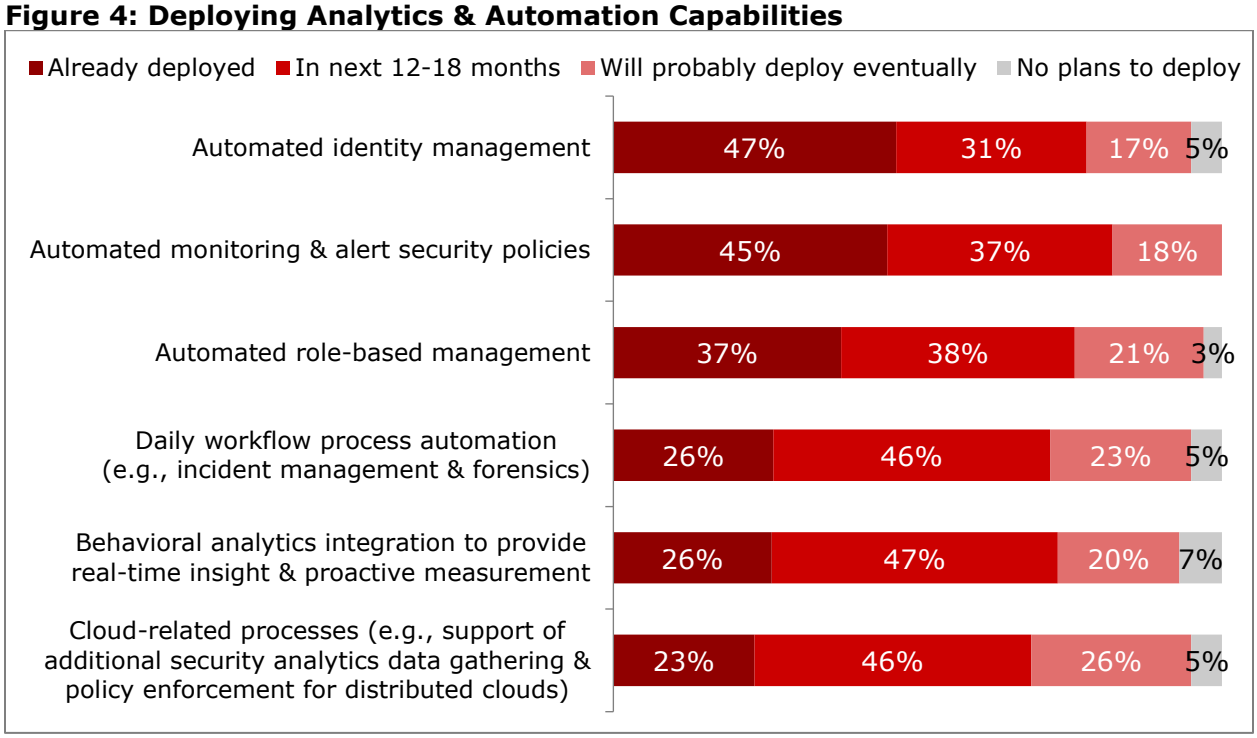
One of the keys to achieving and implementing this level of proactive security enforcement is contextual intelligence. With contextual intelligence supported by analytics and automation, it is possible to understand not only the nature of the threat, but also the nature of the service, the affected endpoints, and the most appropriate automated response. In the cloud, where there is no longer a defined perimeter, not every threat can be managed the same way as in the legacy perimeter model. What is required instead is a prioritized view, understanding the consequence of a mitigation action for a critical application such as a medical IoT device.

The other value proposition of this approach is that it fosters the sharing of threat intelligence among user communities, which is increasingly relevant for applications such as IoT that may traverse various clouds. Threat intelligence can also provide information such as attacker methodologies, tools and tactics, indicators of specific malware, and details of specific attack vectors. Without question, knowing which attackers are trying to target your network – as well as how, why and when – is a valuable tool to proactively thwart attacks such as Mirai and WannaCry on a variety of endpoints, including mobile and IoT devices.

While, as noted in the previous section, CSPs' organizational security strategies have not kept pace with the acceleration and sophistication of cyberthreats, the positive news is that CSPs are making plans to implement analytics and automation to support proactive responses. For example, as depicted in **Figure 4**, a significant number of CSPs have already deployed some automated processes (23 percent to 47 percent), while the greatest share (31 percent to 47 percent) plan to implement automated processes in the next 12-18 months. Moreover, the

broad adoption of behavioral analytics (47 percent), cloud-related processes (security analytics and policy) and daily workflow automation (both 46 percent) are well suited to meeting the requirements inherent with the proactive processing paradigm.

Figure 4: Deploying Analytics & Automation Capabilities



Question: What are your company's deployment plans for the following types of security capabilities? (N=99-100)
Source: Heavy Reading Nokia Networks Custom Survey Q317

CONCLUSION

CSPs continue to push forward and execute their cloud strategies – and for good reason, since the cloud represents their future. However, to successfully execute those strategies requires profound change on a number of fronts, including security. In order to effectively execute in the security realm, CSPs must adopt a more progressive security strategy that fully addresses the unique security requirements the cloud introduces.

This genesis of this strategy is based on accepting that there is no longer a discernible security perimeter to enforce, and that the only viable security strategy in the cloud is one based on integrated analytics that provides baseline network behavior data to automated, real-time security systems to enable predictive proactive security policy enforcement.

While the implementation of these advanced security strategies may take some CSPs out of their "comfort zone," as we have documented in this report, most understand that the *status quo* perimeter approach is no longer an option, and therefore plan to start implementing automated security processing within a 12- to 18-month window. Once this is accomplished, one of the final hurdles associated with cloud commercialization will be resolved, thereby enabling CSPs to finally harvest the true potential of the cloud.

ABOUT NOKIA NETWORKS: FOCUS ON PROACTIVE SECURITY

Tackle the New Challenge in Cybersecurity

Security teams need a better way to not only gather the supporting information about the security state from a wider range of sources, but also automate security processes. Proactive security is able to prevent, pinpoint and address security threats before they result in breaches.

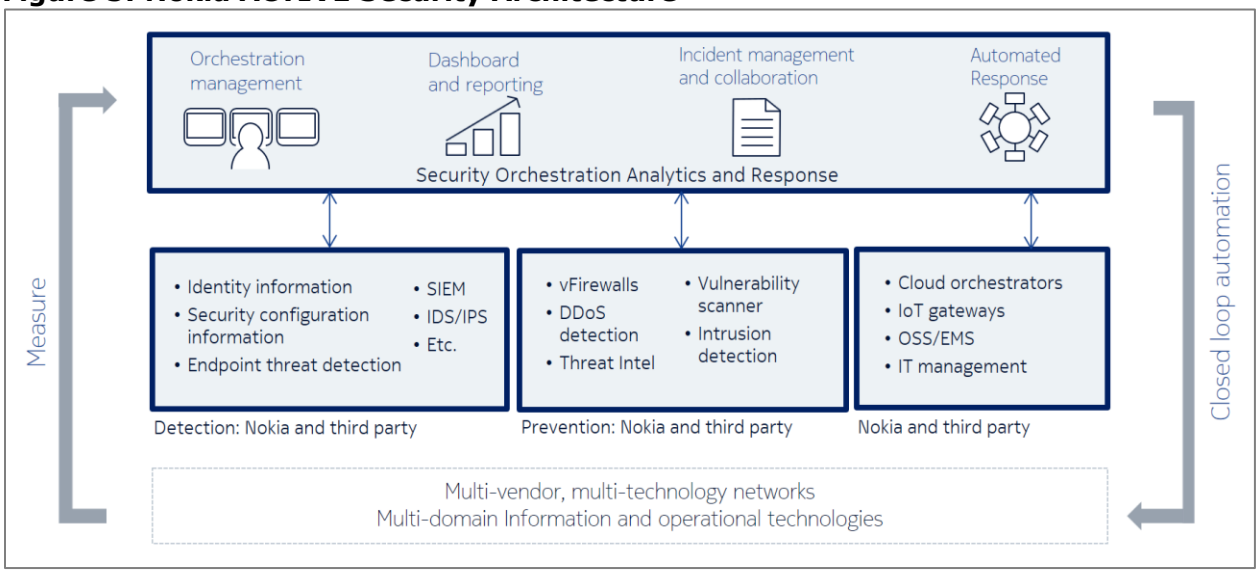
An essential module for a proactive cybersecurity architecture is Security Operations, Analytics and Reporting (SOAR), which can automate response workflows to gather and analyze security data from various sources, and make them available and consumable by different stakeholders. A platform that uses intelligent analytics, artificial intelligence and machine learning would continuously evaluate the risk posture and the state of the environment to enable informed decision-making, formalize and automate responsive actions in real time. Such cognitive analytical and automated technologies measure rather than monitor to provide formalized workflows and enable informed remediation prioritization.

Enriching Traditional Security Management Systems

The traditional security management system capabilities to detect and investigate unknown threats and exfiltration are insufficient alone. There is an important distinction between an intrusion when unauthorized entities gain access to the network, and exfiltration when data leaves the network (or in other words, a breach is occurring).

Traditional systems such as SIEMs typically do not provide the contextual analytics necessary to identify potential threats that may indicate exfiltration, nor are they able to determine post-incident what data may have been exfiltrated or which systems were compromised. They are typically deployed to look at the perimeter of the network. Outsiders that have already infiltrated the network, whether by stealing hardware or taking over an insider's account, can roam freely in a perimeter-centric security system. Malicious insiders pose a significant risk as well, as they are already inside the network.

Figure 5: Nokia ACTIVE Security Architecture



Nokia's NetGuard Security Management Center: A SOAR Solution for More Efficient Security Operations

NetGuard Security Management Center (SMC) is Nokia's portfolio brand for SOAR. The solution provides cognitive analytics and aggregates and correlates security data from a variety of sources, enriching it with a telco context to help security operations teams assess business risks, improve decision-making processes, and better control costs and risks. This makes it possible to quickly identify trends and anomalies, and initiate automated responses by triggering cyber playbooks.

NetGuard aggregates inputs from various network and system data sources, and correlates this data to identify patterns that match specific threat vectors. As new threats are identified by Threat Intelligence, updated detection algorithms and playbooks are provided to meet these threats. The NetGuard SMC solution includes automation of typical day-to-day workflow, automation of analysis to increase the efficiency and effectiveness of security investigation, and automation of threat responses to trigger countermeasures to respond to threats before data is exfiltrated. The solution manages orchestration processes, security policies and their lifecycle. Nokia's solution uses cyber playbooks (security operations workflows) to enable automated responses.

Using multiple tools from multiple vendors creates unnecessary complexity. A SOAR solution streamlines automation, analytics and reporting coming from many cross-vendor tools in use, helping analysts to integrate disparate tools. Previously siloed information can be put into context and viewed as part of an unfolding storyline.