SECURITY ANALYTICS: AN INTRODUCTION

Enterprise IT security is driven by data. Network endpoints generate vast volumes of log metrics data that describe the traffic behavior in real-time. When a security incident occurs, the network behavior changes. Certain nodes route traffic to servers with restricted access to authorized internal users. Network logs cannot predict what's going to happen next, but only describe what's happening now.

For security experts, visibility and analysis of historical and real-time network data can help identify the pattern of network behavior and predict what's going to happen next—a practice known as security analytics. In this article, we will discuss the key components of end-to-end Security Analytics for your enterprise security.

What's Security Analytics?

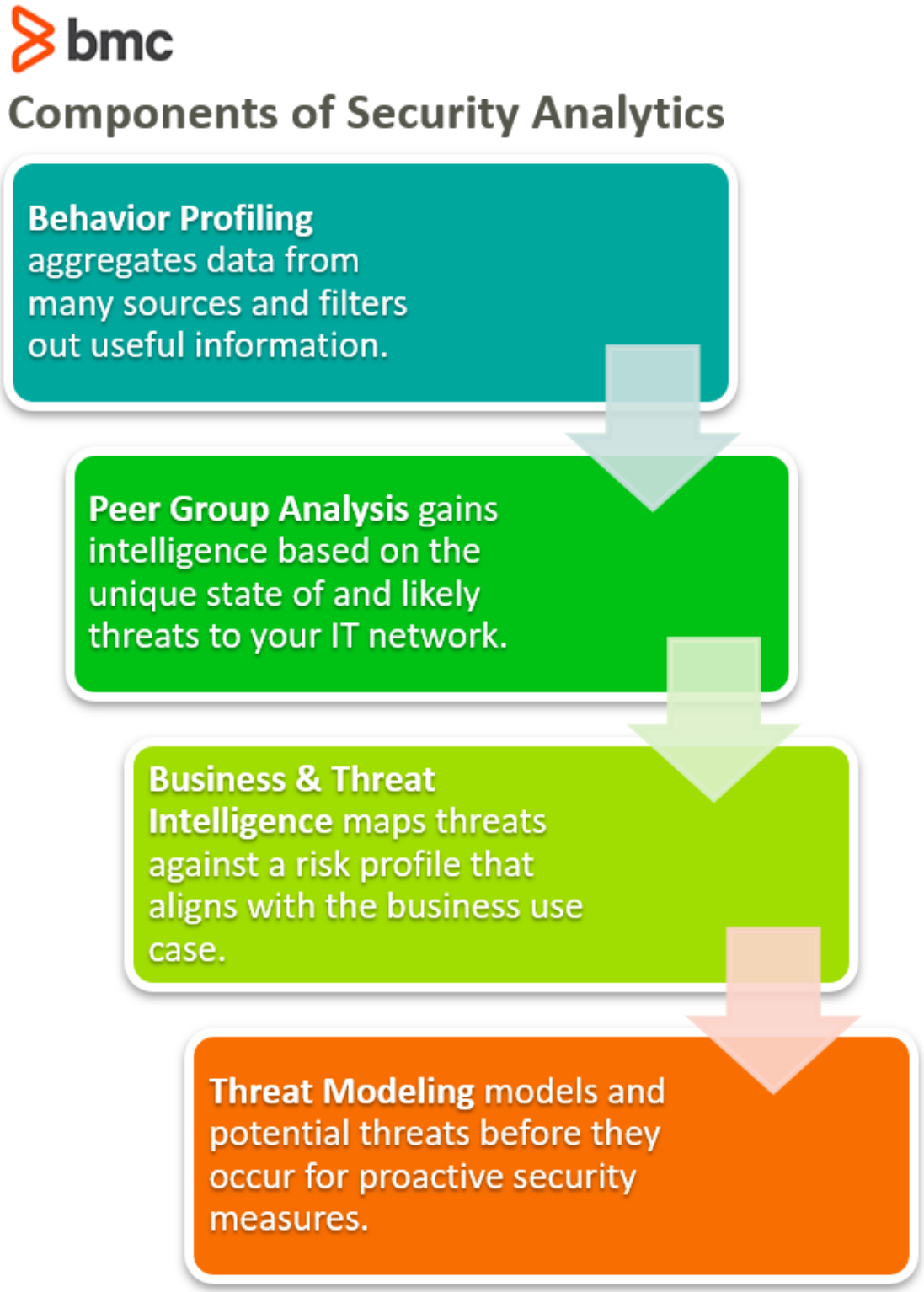
Security analytics is the process of collecting and analyzing data to perform proactive security controls. It forms the basis of modern data-driven enterprise security systems capable of reducing the impact of a security incident.

The process involves capture, storage, and processing of raw data logs aggregated across the network infrastructure. The sources of data include network and physical layer devices such as routers, switches, IoT and server hardware, to application interfaces at the client side. The data is cleaned, combined, and correlated. Advanced machine learning and AI algorithms help make sense of the data and provide meaningful insights in the form of intuitive reports.

Key components in Security Analytics

Security analytics has its roots in machine learning and mathematical statistics. These methodologies are used to discover, interpret, and communicate security insights so that organizations can take proactive security measures before experiencing the impact.

Consider the following key use cases in security analytics:



Behavior Profiling

Network log data can be overwhelming, especially when a range of metrics must be evaluated to

extract the most meaningful insights on network traffic. It can take several complex models to distinguish between normal and anomalous behavior across any metric category. There may be no specific definition of 'normal' especially with so many things going on in the network:

- Traffic variations
- Changing workloads
- Connections to apps, services, and IoT

Additionally, an anomalous behavior doesn't always qualify as a threat.

This is where security analytics comes into play. Security analytics technologies would take the output of anomaly detection systems that filter out the noise and the statistically normal traffic behavior. This behavior is profiled based on the network state and correlated across other behavior profiles to develop a score of trust. Once a network behavior at a given state reaches a certain threshold, it can be accurately classified as a threat and, then, recommend appropriate corrective measures. This threshold can be adjusted dynamically as the threat landscape evolves.

Peer Group Analysis

A threat is often raised when multiple network nodes report anomalous behavior. Security analytics groups the collective behavior of network nodes by common attributes. This behavior is then compared by similar groups internally within the organization and external industry benchmarks, if available. This provides information on relative performance of a grouped set of entities within the network, with respect to historical (internal) or external benchmarks.

Using this approach, security analytics technologies rely on limited resources to yield insightful information. Instead of developing complex detection models, machine learning models develop contextual understanding from data that is already available through past experiences and compared against the known benchmark performance.

Business & Threat Intelligence

Organizations have to find an optimal tradeoff between network performance, complexity, cost, business challenges, and opportunities. They can invest in expensive security solutions that evaluate a range of metrics across the risk landscape. The challenge here is to prepare for the risks that are most likely to compromise your network security. It means asking the right questions that provide an accurate threat context so you can allocate resources accordingly.

The role of security analytics is particularly useful in separating meaningful and actionable insights

from false alarms. It helps create risk scores and prioritize security actions that are most aligned with your security strategy and organizational policy. The resulting threat intelligence can help you understand:

- The business impact of certain threats
- The advantage of taking certain corrective measures at the cost of specific resources

It is like viewing security as a business problem, allowing you to address the most impactful threats without compromising other aspects of business such as network performance and cost.

Threat Modeling

The threat landscape evolves continuously and cyber criminals always seem to find new ways to attack IT networks. In the world of enterprise security, adoption of new technologies with the underlying vulnerabilities and zero-day exploits always gives hackers an edge. While security experts attempt to model the threats, the uncertainty and variations in security threats require organizations to prepare for a variety of threat models.

The concept of threat modeling is prevalent in the domain of security analytics, especially as it is focused on future predictions and proactive security measures. Given certain past network behavior and its state of security in the present threat landscape, security analytics technologies can help you prepare for the most likely threats well before they occur. The tools offer forensics capabilities to understand past security attacks, investigate the cause and network vulnerabilities, and provide remediation actions that prevent similar incidents from happening again. The same principles can be applied to a variety of threats, including internal risks associated with human error and malicious employee intent, as well as external cyber-attacks.

End-to-end enterprise security

These elements combine to formulate an end-to-end data-driven enterprise security process. It starts with aggregating data from a variety of sources and filtering out the most useful information. It then gains contextual intelligence based on the unique state of your IT network and the likely security threats facing your organization. The threats are mapped against a risk profile that aligns with the business use case. Finally, future threats are modeled to prepare for potential threats before they occur.

Security analytics relies on advanced AI technologies to do all of this heavy lifting at the backend while providing actionable and intuitive reports for IT and security executives.

While this makes security analytics an important component of your enterprise security, developing the right security strategy is a prerequisite to maximizing the value of your security analytics investments.

Additional resources

For more on this topic, check out these BMC Blogs:

- BMC Security & Compliance Blog
- What is Security Information and Event Management (SIEM)?
- SIEM vs Log Management: What's the difference?

- AIOps Machine Learning: Supervised vs Unsupervised