OUTSMART ADVANCED CYBER ATTACKS WITH AN INTELLIGENCE-DRIVEN SECURITY OPERATIONS CENTER

HOW TO ADDRESS GARTNER'S FIVE CHARACTERISTICS OF AN INTELLIGENCE-DRIVEN SECURITY OPERATIONS CENTER

VERINT®

POWERING ACTIONABLE INTELLIGENCE

TABLE OF CONTENTS

ADVANCED CYBER ATTACKS ARE HERE TO STAY

IN ITS GLOBAL RISKS 2015 REPORT[1], THE WORLD ECONOMIC FORUM RANKS CYBER ATTACKS AMONG THE TOP FIVE HIGH-IMPACT GLOBAL RISKS FOR THE COMING DECADE.

Recent cyber attacks against the likes of Sony Pictures, Anthem and the US Office of Personnel Management (OPM) underscore the complexity of these threats, as well as the risks of a potential data breach. In terms of costs, the average financial loss attributed to reported cyber security incidents in 2014 was $2.7 million[2].

IT'S TIME TO RECALCULATE YOUR SECURITY MINDSET

These breaches clearly illustrate the fact that most Security Operations Centers (SOCs) are simply not equipped to counter sophisticated and targeted cyber attacks, which sail through the gaps left by existing siloed security tools. Traditional signature-based perimeter tools only look for known attacks at the point of entry. In an attempt to overcome this limitation, some SOCs have incorporated advanced detection sensors that specialize in specific vectors, which work alongside Security Incident and Event Management (SIEM) systems to provide situational awareness. Neither was designed to perform in-depth investigations of multi-faceted attacks. And while forensics tools may add visibility, they often lack automated analytics and require manual searches by extremely specialized analysts.

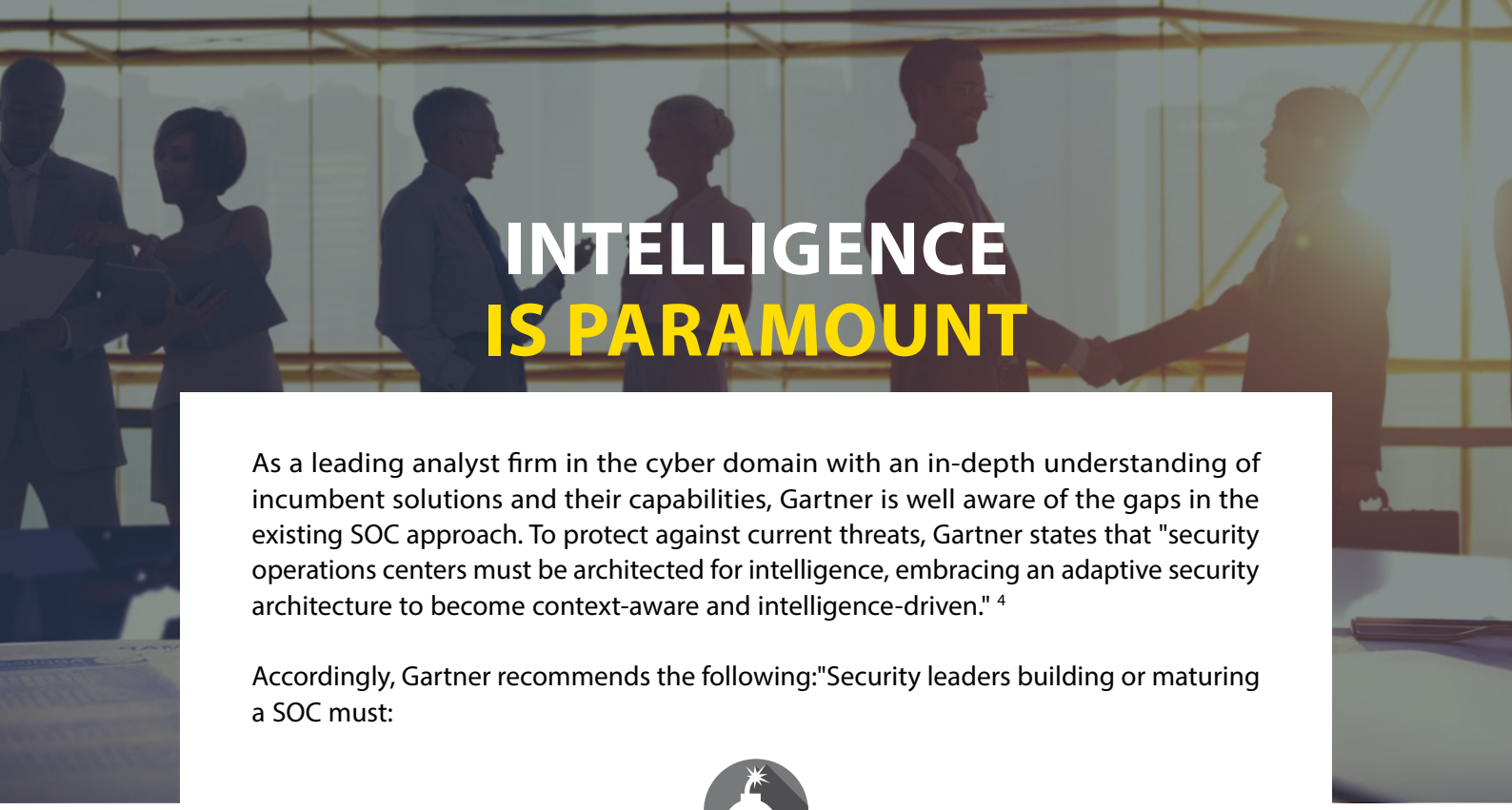
Meanwhile, SOC teams lack the resources to sift through thousands of daily alerts, detect high-priority cyber-attacks and remediate them in a timely manner. While the average enterprise spends $1.3m[3] a year dealing with false positive cyber security alerts, while average time to detect, investigate and remediate attacks remain unacceptably high. Organizations fail to realize the criticality of an integrated, automated and adaptive architecture.

---

1 Source: reports.weforum.org/global-risks-2015/part-1-global-risks-2015/introduction/

2 Source: PricewaterhouseCoopers, The Global State of Information Security® Survey 2015

3 Source: Computer Weekly, False malware alerts cost enterprises $1.3m a year on average, January 2015



INTELLIGENCE IS PARAMOUNT

As a leading analyst firm in the cyber domain with an in-depth understanding of incumbent solutions and their capabilities, Gartner is well aware of the gaps in the existing SOC approach. To protect against current threats, Gartner states that "security operations centers must be architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven." [4]

Accordingly, Gartner recommends the following:"Security leaders building or maturing a SOC must:

Adapt a mindset that is based on the assumption that they have already been compromised.

Instrument their SOC for comprehensive visibility.

Follow an intelligence-driven SOC approach with these five characteristics:

1. Use multisourced threat intelligence strategically and tactically

2. Use advanced analytics to operationalize security intelligence

3. Automate whenever feasible

4. Adopt an adaptive security architecture

5. Proactively hunt and investigate" [5]

---

[4] Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015

[5] Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015

ALL THE INTELLIGENCE YOU NEED IN ONE UNIFIED SOLUTION

VERINT HAS APPLIED OVER 20 YEARS OF INTELLIGENCE EXPERIENCE AND MARKET-LEADING ANALYTICS TO ADDRESS THE CHALLENGES PRESENTED BY THE NEW BREED OF CYBER THREATS.

Based on our experience in protecting some of the world's most sensitive and targeted organizations, as well as the efforts of global security research teams, Verint has built a unique, intelligence-driven cyber security platform that enables enterprises to effectively detect and respond to advanced and unpredictable cyber attacks.

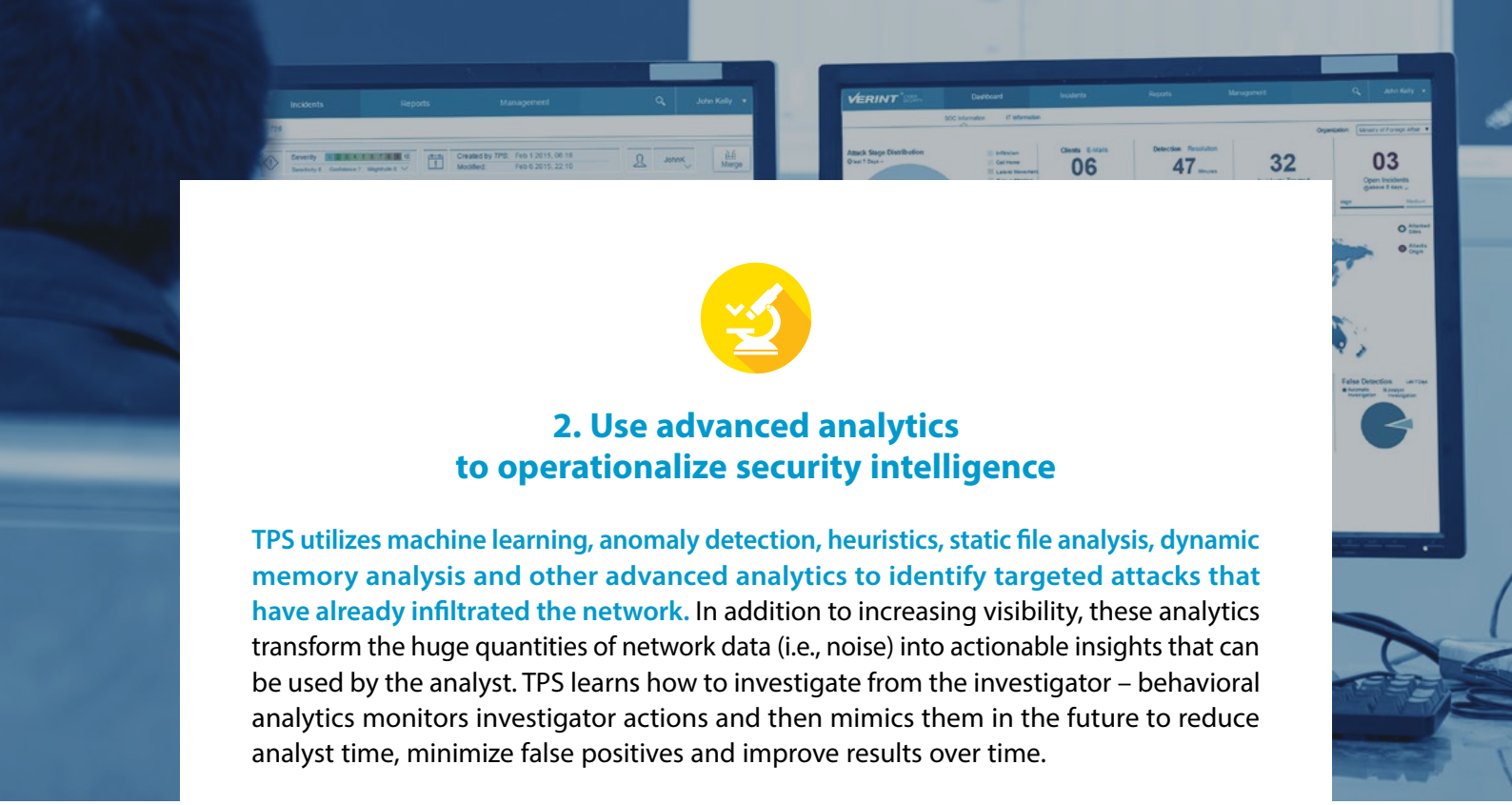
Verint® Threat Protection System™ (TPS) enables SOC teams to protect critical networks, IT systems and information assets against advanced cyber attacks. TPS offers comprehensive detection, prioritization, investigation, and protection capabilities based on a unified security approach designed to increase threat visibility and streamline threat management without increasing the size or expertise of security operation teams.

VERINT THREAT PROTECTION SYSTEM - ENABLING AN INTELLIGENCE-DRIVEN SOC

TPS IS FULLY ALIGNED WITH GARTNER'S INTELLIGENCE-DRIVEN SOC APPROACH, IMPLEMENTING ALL FIVE KEY CHARACTERISTICS.

1. Use multisourced threat intelligence strategically and tactically

Verint TPS orchestrates intelligence gathered from specialized and fully integrated engines that work across an organization's network to detect malicious files, command and control communications, lateral movement and infected endpoints. **Spanning network, payloads and endpoints, TPS applies different sources of threat intelligence,** such as hash values, blacklists, URL categorization, network anomalies, registry changes, and even behavioral analysis that learns on the fly, **to augment existing threat intelligence.** Insights collected are analyzed in real time and cross-validated in the TPS brain to create further threat intelligence.



2. Use advanced analytics to operationalize security intelligence

TPS utilizes machine learning, anomaly detection, heuristics, static file analysis, dynamic memory analysis and other advanced analytics to identify targeted attacks that have already infiltrated the network. In addition to increasing visibility, these analytics transform the huge quantities of network data (i.e., noise) into actionable insights that can be used by the analyst. TPS learns how to investigate from the investigator – behavioral analytics monitors investigator actions and then mimics them in the future to reduce analyst time, minimize false positives and improve results over time.

3. Automate whenever feasible

By automating detection, incident processing and intelligence-driven investigation workflows across the kill chain stages, TPS enables SOC teams to improve threat management, accelerate time to remediation and allow senior analysts to focus on resolving the more complex attacks detected on the network. **Sophisticated fusion features, powered by the TPS brain, work in sync to automatically combine alerts, metadata and intelligence into incidents representing a potential attack**, which are then prioritized based on risk.

TPS enables automated prioritization, such as running a network forensics query on an entity involved in an alert, remotely scanning a potentially infected endpoint, or fetching a file for deeper inspection. The analysis and evidence gathering workflow is also automated, and dynamically adjusts itself as findings accumulate. Once enough evidence has been discovered, the automated TPS investigation engines hand over the findings, conclusions and recommended next steps to the SOC analyst.

4. Deploy an adaptive security architecture

TPS supports critical capabilities of Gartner's Adaptive Security Architecture out-of-the-box in a unified and tightly integrated manner. Built by intelligence experts, TPS enables SOC teams to prevent known threats across attack surfaces, detect threats already within the network, automate forensic analysis and response, and apply gathered intelligence for predicting the next attack.

5. Proactively hunt and investigate

TPS automatically hunts for threats in the environment by uniquely combining broad visibility, specialized detection and automated forensic investigation. For example, TPS may automatically trigger endpoint forensics as soon as an indicator of compromise is identified in the network. At the same time, TPS facilitates proactive hunting by security analysts by providing them with a visualized and information-rich investigation platform, which brings the attack story to life. These capabilities help analysts to unearth hidden threats, better understand the tactics, techniques and procedures (TTPs) of advanced attacks and, as a result, anticipate future attacks. The TPS data model is based on STIX and TAXII standards to help analysts leverage external threat intelligence or online research tools.

As illustrated, TPS employs an intelligence-driven approach that embeds Verint's unique intelligence methodology across the solution. Multiple engines operate as intelligence sources, constantly monitoring all attack vectors and sharing intelligence throughout all stages of an attack. This context-aware intelligence enables analysts to understand the attack story as **TPS connects seemingly isolated incidents into a narrative that can reveal a large-scale, long-term campaign. The end result is a marked improvement in threat visibility and management,** which were cited by over 50% of enterprises as the primary driver for building a SOC[6].

[6] Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015, Gartner Research Circle, G-14524 SOC Survey, October 2014 (In the Gartner Research Circle SOC Survey, conducted in October 2014, 52% of 69 respondents that had or were planning to invest in a SOC stated that their primary driver was "threat management." For a further 29%, threat management was at least the secondary driver.)

CONCLUSION

TPS IS FULLY ALIGNED WITH GARTNER'S INTELLIGENCE-DRIVEN SOC APPROACH AND IS SPECIFICALLY DESIGNED TO ENABLE SOC TEAMS TO EFFECTIVELY MITIGATE ADVANCED CYBER THREATS.

Constant real-time monitoring and analysis of payloads, network traffic and endpoints, together with on-demand forensics and automated investigations, provide complete threat visibility and efficient threat management across the operation. In addition to tactical incident detection and response, TPS also gives SOCs a strategic solution with predictive capabilities that help to proactively anticipate and hunt for the next likely attack. Verint's intelligence-driven approach results in better protection of critical assets from targeted attacks, more efficient investigation processes and lower organizational risk.

"WE ESTIMATE THAT CURRENTLY LESS THAN 10% OF EXISTING SOCS POSSESS TWO OR MORE INTELLIGENCE-DRIVEN CHARACTERISTICS"

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015





START IMPLEMENTING ALL 5 KEY INTELLIGENCE CHARACTERISTICS IN YOUR SECURITY OPERATION CENTER. CONTACT VERINT

VERINT CYBER SECURITY. FOR THREATS IMAGINED, NOT YET IMAGINED, AND IMPOSSIBLE TO IMAGINE.

Verint® Systems Inc. (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions for customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in over 180 countries use Verint solutions to improve enterprise performance and make the world a safer place. Learn more at ***www.verint.com***.

VERINT®

info.cyber@verint.com
www.verint.com/cyber