The Five Characteristics of an Intelligence-Driven Security Operations Center

02 November 2015 | ID:G00271231

Analyst(s): Oliver Rochford, Neil MacDonald

Summary

Security operations centers must be architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven. Security leaders should understand how intelligence-driven SOCs use tools, processes and strategies to protect against modern threats.

Overview

Key Challenges

Traditional security operations centers:

- Rely primarily on prevention technologies, and rule and signature-based detection mechanisms that require prior knowledge of attacker methods, both of which are insufficient to protect against current threats.
- Treat intelligence (TI) as a one-way product to be consumed, rather than as a process, leading to an intelligence-poor security strategy.
- Treat incident response as an exception-based process, versus a continuous one.

Recommendations

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: use multisourced threat intelligence strategically and tactically; use advanced analytics to operationalize security intelligence; automate whenever feasible; adopt an adaptive security architecture; and proactively hunt and investigate.

Strategic Planning Assumption

Through 2020, intelligence-driven security operations centers will rise from less than 10% to 40%.

Introduction

The threat and risk environment has evolved rapidly in the past five years, with an increase in active threat actors and an escalation in the sophistication of their techniques. The availability of advanced and lean-forward security technologies, as well as the development of defensive strategies to counter these threats, such as risk-based or kill-chain-based approaches that heavily leverage threat and security intelligence, requires the traditional security operations center (SOC) to adapt to these new realities. Organizations must assume they have already been compromised. Rather than trying to prevent the inevitable breach, organizations must switch to a continuous-monitoring mindset, where threats are prioritized, and focus is given to mitigating and limiting resulting damage from an attack.

An intelligence-driven SOC goes beyond preventative technologies and the perimeter, and beyond events-based monitoring. An intelligence-driven SOC has to be built for intelligence, and use it to inform every aspect of security operations. To meet the challenges of the new "detection and response" paradigm (see "Prevention Is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence"), an intelligence-driven SOC also needs to move beyond traditional defenses, with an adaptive architecture and context-aware components. To support these required changes in information security programs, the SOC must also change. The traditional SOC must evolve to become the intelligence-driven SOC (ISOC).

Analysis

The traditional SOC provides device management and monitoring services for firewalls, intrusion protection systems, proxies, and other perimeter and preventative security technologies. Alongside change management and maintenance of security devices, monitoring system logs and events has primarily been done using a security information and event management (SIEM) platform. Regulatory compliance and control-based frameworks have provided the underlying processes and governance structure, with integrations with help desks or ticketing systems allowing some interaction with the greater organization.

Threat management was cited by over 50% of enterprises as the primary driver for building a SOC. [1] A gap in threat visibility as the greatest gap in their organization's security was cited by 76% of enterprises that Gartner surveyed [2] that are planning a SOC in the next 12 to 24 months; yet organizations that already have a SOC capability do not seem to fare much better, with 82% stating the same sentiment. [3]

Many current attacks bypass the traditional prevention mechanisms, security controls and signature-based approaches that this model has traditionally relied on.

Gartner's adaptive security architecture (see "Designing an Adaptive Security Architecture for Protection From Advanced Attacks") outlines four critical domains: prevent, detect, respond and predict. An ISOC embodies the operational implementation of this architecture, using security intelligence both derived from within and obtained from outside of the organization to guide, inform and prioritize the strategic and tactical decision making on a day-to-day basis, as well as a future basis.

Security intelligence, derived out of threat and operational intelligence, in addition to organizational context, provides the foundation of the "intelligence" in ISOC, but this intelligence is of limited value by itself until it is operationalized. Historically, this has been a manual and labor-intensive process, requiring analytical expertise and real-time data that has not been readily available. This is changing rapidly, however, with security operations, analytics and reporting (SOAR) solutions providing security incident response, security operations automation, and threat and vulnerability management capabilities. SOAR solutions enable the deployment of a SOC strategy that semiautomates many and fully automates some of the day-to-day tasks of security operations.

Threat intelligence technologies and services — whether providing the threat intelligence or, in the case of threat intelligence sharing platforms, the means to curate and share content yourself — are now available and provide the basis for a SOC built for intelligence.

The guiding vision for an ISOC is effective detection and response. Preventative techniques are still important for presenting a hardened surface and ongoing threat containment. But for a SOC to be effective at detection and response, it needs to continuously evolve and adapt to changes in the technology and threat environment.

Herein lies the key difference between an ISOC and a traditional SOC. An intelligence-driven SOC can evolve and adapt because of the use of security intelligence that changes the scope and focus of security operations activities continuously. For rapid response, as much of the mundane work should be as automated as possible, and other human-augmented responses should be aided with decision support systems.

Detective, preventative, response and predictive capabilities are becoming available (see "Intelligence Awareness and Adaptive Security Response Will Transform Network Firewall Markets"), but with true automation and context-awareness still residing, for the most part, in isolated point solutions. This necessitates middleware and human interaction to bridge this gap in the meantime.

Use Threat Intelligence Strategically and Tactically

Threat intelligence for most organizations takes the form of an integrated data feed that provides machine-readable threat intelligence (MRTI; see "Technology Overview for Machine-Readable Threat Intelligence") composed of indicators of compromise (IOCs) intended for correlation with security telemetry data. This approach, while

providing improved detection capabilities, suffers from many of the same weaknesses as traditional approaches that depend on prior knowledge of a threat. In addition, it extracts only the data that is easiest to reuse, losing much of the provided context and actual information content. This use of MRTI is entirely tactical.

In reality, an advisory for malware or a specific threat actor campaign can contain much more information that can be used to improve the overall security posture and operations on a tactical and strategic level. However, client feedback indicates that even leading threat intelligence services provide little in terms of immediately actionable intelligence, still requiring analysts for manual curation and fusion.

Beyond the obvious use case of correlating event or network data with what amounts to an IOC signature feed, the provided intelligence should be used as the basis for strategic planning and tactical execution. It should also be noted that threat intelligence does not only originate externally — security telemetry data gathered by operations and intelligence derived from business activities (for example, a new customer may be a "hacktivist" target) are also factors that should flow into the creation of security intelligence.

Leveraging threat intelligence in this way requires a formalized process and a dedicated resource to manage the threat intelligence life cycle, and to implement a closed feedback loop (see "How to Collect, Refine, Utilize and Create Threat Intelligence"). An IOC describing how a specific malware component can be detected will frequently be the seed for further intelligence derivation. If an IOC is found in network traffic logs (for example, command and control traffic for a specific piece of malware), this should prompt the creation of further intelligence to:

- Check endpoints for installed malware and verify the spread of infection
- Verify access and authentication logs to assess whether privileges have been escalated or laterally transferred
- Provide guidance on risk and mitigate steps to operations
- Evaluate which actors and campaigns the malware is associated with to attempt to deduce the tools, techniques and processes (TTPs), help determine the motivations of the adversary, and anticipate and predict what their ultimate objective may be and what their next targets might be

Threat Intelligence Platforms (TIPs)

TIPs automate the ingestion of a virtually unlimited range of external and internally generated, structured and unstructured threat intelligence from open (Open Source Intelligence [OSINT]), industry (Computer Emergency Response Teams [CERTs] and Information Sharing and Analysis Centers [ISACs]), closed (aka your organization) and commercial threat intelligence provider sources. They then can automatically enrich and correlate this threat intelligence (TI) and assist in the automation of making the TI

actionable by feeding technologies, such as SIEM, incident response platform (IRP), intrusion prevention system (IPS), next-generation firewall (NGFW) and secure Web gateway (SWG). These technologies significantly assist in bringing the prevailing threat landscape to your organization and help deliver "context" (or intelligence) that underpins the goals of the ISOC (see "Technology Overview for Threat Intelligence Platforms").

Use Advanced Analytics to Operationalize Security Intelligence

Gartner defines "advanced analytics" as the analysis of all kinds of data using sophisticated quantitative methods (such as statistics, machine learning, descriptive and predictive data mining, and simulation and optimization) to produce insights that traditional approaches to intelligence — such as query and reporting — are unlikely to discover (see Figure 2 and Note 1).

In the context of security operations, advanced analytics capabilities can support a variety of different processes and tasks, including threat and vulnerability management, advanced threat detection, incident prioritization, and hunting and investigating. Behavioral analytics, for example, can be used to detect suspicious behavior without requiring prior knowledge of technical IOCs, and attack path modelling can be used to predict the potential path an attacker can take to escalate privileges.

Technology Options

THREAT AND VULNERABILITY MANAGEMENT (TVM) PLATFORMS

Threat and vulnerability management platforms usually do not execute vulnerability assessments themselves. They consolidate and normalize output from multiple vulnerability, application security and penetration testing solutions to analyze and prioritize vulnerabilities by applying threat intelligence and advanced risk modeling approaches, such as attack path analysis. Some example vendors are RedSeal, RiskSense, Kenna and NopSec.

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

UEBA solutions detect malicious and abusive activity, and consolidate and prioritize security events and alerts (see "Market Guide for User and Entity Behavior Analytics").

Automate Whatever and Whenever It Is Feasible

The resources required to effectively and efficiently run an intelligence-driven SOC have little relation to what that business does or how large it is. A SOC requires a minimum of eight to 10 people to ensure one available resource for continuous monitoring, and one for investigation and response at any given time over a 24/7 cycle. This count does not consider the actual workload. But the issue is not only related to pure cost — the expertise and skills are not widely available (see "CISOs Should Review Their Enterprise's Security Skills Portfolio Now").

The speed, accuracy and, therefore, effectiveness of response are also major factors to consider. Detection and mitigation must be executed swiftly and with precision to limit the damage from a breach and interrupt the kill chain before data exfiltration. Playbooks and processes should not be learned during a breach — the least forgiving of all teachers— and evidence-gathering and forensics must be done properly to avoid polluting the audit trail or invalidating evidence for legal purposes.

For these reasons, many organizations seek to automate as much of the day-to-day operations work as is feasible.

Full or Semiautomation

Full automation of security incident response is still an emerging topic, with little overall appetite in the market. This is largely a legacy of the first practical attempts at that approach — for example, first-generation intrusion prevention and spam-blocking systems, where false positives were common due to a lack of mature analytics and threat intelligence capabilities, inadvertently blocking legitimate traffic. This perception is still widespread, but swiftly changing due to improvements in detection, analytics and orchestration, and the need for rapid response.

What can reliably and safely be fully automated depends on several factors (also see Note 1).

HOW RELIABLE IS THE DETECTION AND IDENTIFICATION OF A THREAT OR INCIDENT?

This has historically been a weak link in automating security response. There are really two aspects to this: How reliable is a detection of a distinct threat in general, and how sure are we in this specific case? Detecting command and control traffic for a specific malware to a known command and control (C&C) address can often be deemed very reliable if the data is not stale. Recognizing whether an account has been hijacked by a potential attacker, or whether a user has just forgotten their password and is trying to guess it, is a more ambiguous matter. The more reliable the detection and identification, the greater the potential for automated response.

WHAT IS THE POTENTIAL RISK IN NOT AUTOMATING THE RESPONSE?

Some types of threats do not necessarily require immediate rapid response. For example:

- The associated risks and damage potential are low (and thus the threat is not a priority when there are other threats that have a higher potential).
- The incident has been detected early in the attack kill chain (see "Addressing the Cyber Kill Chain"), allowing sufficient time for a more measured response.

Other types of threats, though, especially those that do not require many stages to execute or those that are detected in the final stages of the kill chain, require immediate action to mitigate damage.

WHAT IS THE POTENTIAL DAMAGE IF THE AUTOMATED RESPONSE GOES WRONG?

"What could possibly go wrong?" should, of course, be a major consideration when deciding what to fully automate. Some business activities are crucial, with any form of detrimental impact negatively affecting the organization. Trading platforms, Internet retail portals, or, essentially, anything that generates revenue or is a fundamental aspect of an organization's offering can raise big red flags when it comes to automating a response.

Semiautomation

Rather than to seek full automation of all SOC activities, enterprises should seek "automatability" — the capability of being automated as higher levels of confidence are achieved. Even then, analytics-driven, human-augmented security decision support systems will be used to provide the SOC analyst with the context of the recommended action, along with the details behind the verdict and recommended action. An analyst can then initiate the automated response or action. In this way, a human is still involved in the process, but the process itself is highly automated to make effective use of scarce SOC resources.

Technology Options

Besides offerings from mainstream vendors, such as Intel (McAfee Security Connected) or EMC (RSA Advanced Security Operations Center), there are many emerging technology vendors addressing the increased need for automation.

SECURITY INCIDENT RESPONSE PLATFORMS (SIRPS)

SIRP solutions are used to formalize, enforce and automate incident response playbooks, policies and processes, as well as to provide templates to manage typical security incident scenarios (see "Technology Overview for Security Incident Response Platforms"). These solutions are frequently supported by analytics, visualization, threat intelligence correlation and forensic-evidence-gathering capabilities.

SECURITY OPERATIONS AUTOMATION PLATFORMS (SOAPS)

SOAP solutions provide a selection of connectors, scripts and templates to remediate third-party devices and applications that can be used to fully automate or semiautomate security operations activities. Some example vendors are Swimlane, Hexadite, CyberSponse and Ayehu.

Hunt and Investigate

Proactive threat hunting and investigation is used to detect unknown and advanced threats. Hunting entails analyst-driven investigation rather than relying on signature or rule-based detection mechanisms. In addition, hunting and investigating is proactive, seeking out IOCs and incidents rather than waiting to be alerted and reacting. There are three categories of investigation, as shown in Table 1.

Table 1. Hunting Styles

Style	Description
Hypothesis-driven	This type of hunt begins with an initial hypothesis or question; for example, could or have we been affected by a specific threat actor campaign, with an exploratory investigation based on known TTPs and related security intelligence?
IOC-driven	Known indicators of compromise are used to initiate the investigation and used to search security data for their (or associated IOC's) presence.
Analytics-driven	Advanced analytics, machine learning and other capabilities are used to assist the analyst to identify the most promising areas to begin hunting.

Source: Gartner (November 2015)

In practical reality, an investigation will encompass more than one of these categories. For example, a hypothesis-driven hunt can utilize predictive analytics, resulting in further IOCs to investigate.

Hunting and investigating requires the ability to pivot from one dataset to another, and cross-reference and correlate these with further context or relationships to other entities or historical activity. Your technology stack has to support such nimble data exploration and analysis.

Deception techniques, such as diverting attackers by using commercial honeypots, or monitoring for the use of fake injected "canary" credentials, are examples of this approach. Traffic on a honeypot is always deemed suspicious, as none is expected, and is an example of the initial IOC in an IOC-driven hunting investigation, providing Internet Protocol (IP) address ranges on which to search for inbound or outbound communications.

Technology Options

DECEPTION

Deception technologies detect and disrupt an attack by the use of deceit and feints, such as by simulating a vulnerable system or service to provoke an adversary into accessing it. There are a number of commercial offerings available that provide deception capabilities: for example, from TrapX Security, CyberTrap or GuardiCore.

HUNTING AND INVESTIGATING

Analytics technologies that allow data analysis, visualization and pivoting of data, such as big-data-based solutions, are frequently used in this capacity, as are SIEMs. Although there is not a distinct market, some tools used for hunting and investigating come from Darktrace, Sqrrl, Niara and Paterva (Maltego).

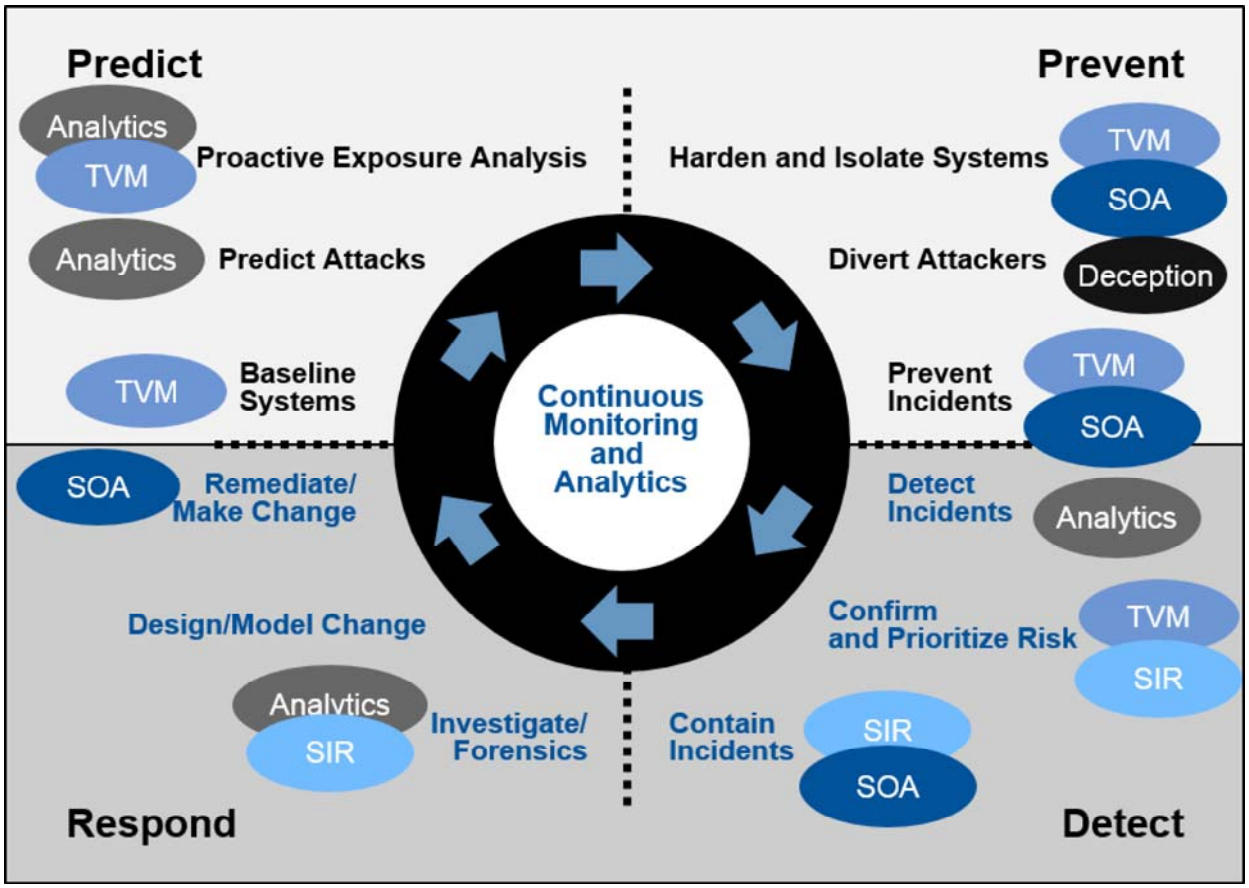
Deploy an Adaptive Security Architecture

An ISOC is designed to control a complex ecosystem and threat environment that changes and evolves continuously and rapidly. Traditional static security approaches and architectures based on security controls, preventative technologies and periodic strategy reviews are now outdated and ineffective before they are even deployed. An ISOC evolves with the environment and threatscape, adapting to new challenges and objectives. It does this through the use of security intelligence, derived from both outside and within the organization, which is used to continuously inform and amend security operations, tactics and strategy. In addition, an ISOC must provide the agility that is needed to detect and respond to advanced threats, and to provide a feedback loop for adaptation and evolution.

Gartner's adaptive security architecture framework (see "Designing an Adaptive Security Architecture for Protection From Advanced Attacks") describes four critical competencies — prevent, detect, respond and predict — and 12 related capabilities that together provide comprehensive, adaptive protection from attacks.

The core of the framework is based on continuous monitoring and analytics, and provides an organizing principle to bring together the people, processes and technologies required for an intelligence-driven SOC approach (see Figure 1).

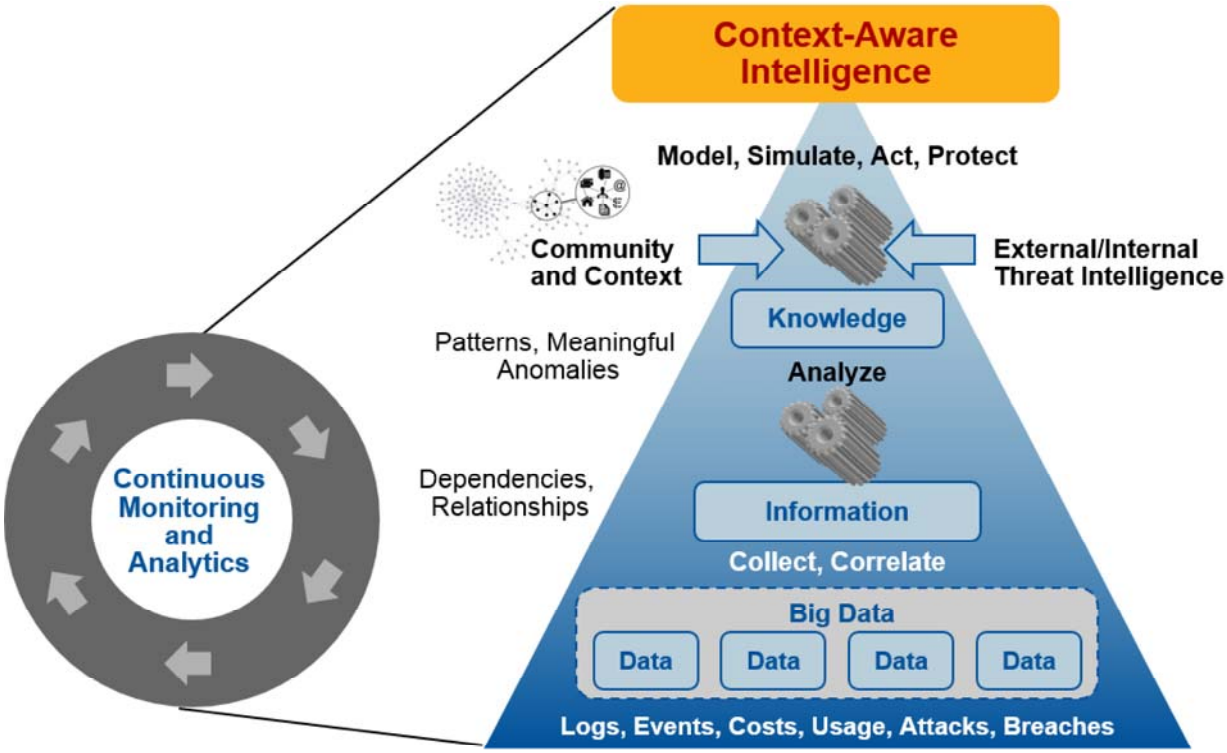
Figure 1. The Adaptive Security Technologies



Source: Gartner (November 2015)

At the center of Figure 1 is a core of continuous monitoring and analytics. Combined with external sources as well as internal context, that core is distilled to "intelligence," seen at the top of the pyramid in Figure 2 — risk-prioritized, actionable insight that drives the heart of the ISOC.

Figure 2. Continuous Monitoring and the Adaptive Security Architecture



Source: Gartner (November 2015)

The Future of the ISOC

Gartner expects ISOC characteristics to expand and evolve in the future. The constantly changing threat environment and the growing proliferation of the Internet of Things (IoT), cloud and mobile technologies will be ongoing drivers, and will necessitate adapted strategies and improvisations on an ongoing basis. If attackers' TTPs change, so must the defenders. The availability and maturity of supporting technologies are improving; opening up new possibilities and approaches to further enhance and augment capabilities with automation intelligence will also catalyze further innovation.

We estimate that currently less than 10% of existing SOCs possess two or more intelligence-driven characteristics. Threat intelligence and security analytics are the most common solutions that Gartner clients have implemented. Through 2020, we expect this number to rise, with 40% of SOCs following an intelligence-driven, or similar, SOC approach.

Although this increase will be prompted by a shift in technology adoption to incorporate more of a "detect and respond" mindset, bringing all of the adaptive security architecture capabilities — prevent, detect, respond and predict — together will entail building synergies between people, processes and technology. The ISOC is a concept that brings these aspects together.

Evidence

This research is based on a combination of briefings from the vendors mentioned in the text, as well as client inquiries.

In addition, we include data from a Gartner Research Circle Survey conducted in 2014.

Methodology:

This research was conducted via an online survey from 5 August through 14 August 2014 among Gartner Research Circle Members — a Gartner-managed panel composed of IT and business leaders.

Engaging the Research Circle community resulted in 146 completed surveys. An invitation to participate was sent to 1,362 members (10% completion rate).

All respondents were screened to ensure their IT leadership role and security focus.

The survey was developed collaboratively by a team of Gartner analysts covering Security, and was reviewed, tested and administered by Gartner's Research Data Analytics team.

NOTE: The results of this study are representative of the respondent base and not necessarily the market as a whole.

[1] 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.

[2] In the Gartner Research Circle SOC Survey, conducted in October 2014, 11 respondents with an in-house SOC were asked, "In your personal opinion, in which of the following areas do you feel there are gaps in your organization's security?" Available responses were visibility of threats, compliance, technology gaps, mobility, lack of staffing, other; 81.9% selected "visibility of threats."

[3] In the Gartner Research Circle SOC Survey, conducted in October 2014, 34 respondents planning on building a SOC were asked, "In your personal opinion, in which of the following areas do you feel there are gaps in your organization's security?" Available responses were visibility of threats, compliance, technology gaps, mobility, lack of staffing, other; 76.5% selected "visibility of threats."

Note 1
Security Automation

For more examples of tasks that can or should be automated, see Anton Chuvakin's Gartner blog post from 11 September 2015, "Security: Automate and/or Die?" (https://blogs.gartner.com/anton-chuvakin/2015/09/11/security-automate-andor-die/)