Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Finding the blind spots in your network security knowledge

The threat posed in today's rapidly evolving digital world is clearly very different to that of the 1990s. Cybercrime is more prevalent than ever before as it provides easy pickings for the modern digitally-smart criminal.

A significant shift in the enterprise security model reveals a growing awareness of the need to ramp up the way in which corporate assets, data and systems are protected. That shift is a steady move towards the Security Operations Center (SOC) model, with estimates suggesting a 38% year-on-year growth in uptake[1] . Of course, SOCs are not new: they have been around since the early 1990s. What's rapidly changing is the security threat landscape, both in volume/frequency and in sophistication. In response to this change we see a new generation of SOCs emerging, those with a focus on intelligence and analytics, rather than response.

The threat posed in today's rapidly evolving digital world is clearly very different to that of the 1990s. Cybercrime is more prevalent than ever before as it provides easy pickings for the modern digitally-smart criminal. Indeed, the latest Intelligence Index[2] from IBM shows that cyber attacks are more advanced and audacious, as well as more varied in focus, from stealing intellectual property to writing malicious code, to lodging political protests. That, in itself, comes as no surprise. Perhaps more surprising for some is the inability of many enterprises to respond in an appropriate and timely manner. As an example, the 2016 Mandiant M-Trends report[3] states that an attacker can be hiding in an organization for 146 days before being discovered. That's almost five months during which a cybercriminal, competitor, or even disgruntled employee has unauthorized access to your business systems and critical information assets.

1 Capgemini Compound Annual Growth Rate calculation based on Gartner estimates

2 IBM® X-Force® Research, 2016 Cyber Security Intelligence Index: A survey of the cybersecurity landscape

3 Mandiant Consulting: M-Trends 2016

Malicious attacks can take an average of **146 days** to identify

Average cost of a data breach to a business: **$3.79M** in 2015

This failure to tackle the cyber threat can put an organization's very existence at risk. After all, few enterprises can afford the reputational damage, system downtime, regulatory penalties and, of course, financial cost of a cyber attack. A recent report[4] into the cost of data breaches found that, for the cross-section of 350 companies interviewed, the average total cost of a data breach in 2015 hit an all-time high of $3.79 million, or $170 per lost or stolen record.

It is figures like this that are prompting Chief Security Officers and Chief Information Security Officers (CSOs and CISOs) to review and overhaul their security approaches. Furthermore, there is tacit knowledge that, as the cyber threat continues to evolve, enterprise IT can't do this alone. At one level, the cost of setting up an internal SOC is hugely prohibitive, let alone the resourcing challenge of finding the people to help you strategize what your SOC should look like. That's why the Managed SOC model is gaining momentum. It offers a cost effective, yet technically advanced and intelligent approach to protecting the digital enterprise.

At another level, the very speed of change across the security landscape is proving almost impossible for enterprises to keep pace with. Cybercriminals move fast: the use of malware, zero day attacks, and more is commonplace, and every minute of every day more enterprise data is at risk of compromise. This speed and the ingenuity of today's cybercriminal has led to the emergence of new generation SOCs offering computer-networked defense.

The standard response to cybercrime has, until now, been first to monitor and then respond to threats. But the speed at which the threat picture changes means that this response is invariably too late. In addition, the response has typically been to 'known' threats, but what about the threats you don't even know exist: the blind spots in your defense? That's a crucial question in today's sophisticated, agile threat environment. And it's where the new breed of SOC comes to the fore.

The intelligent SOC doesn't simply monitor and respond; it gets into the mind of the smartest cybercriminal. It orchestrates the right technology, right processes, and right skills to get ever closer to the things you don't know about and don't want in your network. It finds the blind spots. The new generation SOC takes the threat data available and turns it into relevant intelligence through advanced analytics, enabling the SOC to predict, and thus prevent, cybersecurity incidents.

This analysis is both continuous and wide ranging. For example, it identifies malware-infected hosts, such as servers, desktops and mobile devices, so that they can be contained before gaining access to the network. It provides real-time visibility of user behavior to detect malicious or negligent users, or identify external attacks that compromise user accounts across the enterprise. It processes historical trending on security-relevant data sources and correlates it with monitoring, detection, and analysis of potential intrusions in real time.

This is a very different world of enterprise security. It's a world where security information and event management (SIEM), network security monitoring, endpoints monitoring, payload analysis and offline big data analytics are brought together in one place. But even that isn't enough to thwart the modern cybercriminal.

What's required is the specialist skill to interpret the intelligence gathered and translate it into the effective coordination of resources and direct use of timely and appropriate countermeasures. This is invariably beyond the reach of in-house SOCs. That's because the growing demand for cybersecurity expertise far outpaces supply, with many enterprises lacking the resources in-house to direct, execute and hone cybersecurity strategies. According to ESG (Enterprise Strategy Group) 46% of organizations say that they have a "problematic shortage" of cybersecurity skills

4 Ponemon Institute: 2015 Cost of Data Breach Study: Global Analysis

in 2016, up from 28% last year[5]. This is further borne out by ISACA, which reports that nearly half of global organizations are planning to hire more cybersecurity personnel in 2016, and 94% say they will expect to have a difficult time finding skilled candidates[6].

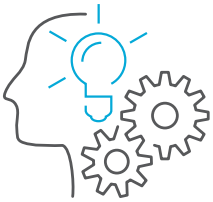
This has prompted the development of intelligence-driven SOC offerings from Managed Security Services Providers (MSSPs). These Intelligent SOCs are human-led and machine-driven. What this latter point means is that they incorporate the latest and smartest technologies to collect information from diverse sources; to sense both machine and human behavior in relation to an enterprise; to analyze those behaviors to understand what the potential impact might be on company data; and to continually learn from what they collect, analyze and understand. The focus of the intelligent SOC is thus on prevention, rather than response.

Can present-day technology do all this by itself? The answer is a resounding no. This means the intelligent SOC has to be human-led. It takes a group of expert professionals in security, technology and business to make sense of what the technologies do for them, and to understanding a company's risk profile.

Even though technologies to spot, predict and correlate relevant data are getting smarter every day, the creative mind that comes up with a new form of cyber threat will always need to be matched by a creative mind focused on an equally smart response to protect the targeted enterprise. This creative mind will pick apart the latest malware code; it will determine which behaviors need more focus than others for a particular client; and it will understand how best to apply new technological advances across clients to get ever closer to and outwit the cybercriminal mind. In the end, it is the combination of people, process and technology that sets the new generation SOC apart from its predecessors

The threat of cybercrime is not going to go away. We must expect to be attacked all the time. It's how you prepare for, monitor, respond to and, importantly, prevent, these attacks that's important. Getting under the skin of the cybercriminal with intelligence-driven defense gives you the opportunity to know what you don't currently know about the threat to your enterprise. That's the value of computer-networked defense through an intelligence-led SOC. The price of protection, fortunately for the enterprise, is increasingly being shifted to a consumption-based model by MSSPs leveraging their evolving capabilities for multiple clients.

46% of organizations state they have a 'problematic shortage' of cybersecurity skills in-house



Intelligent SOCs are **human-led** and **machine-driven**

5 ESG Brief: Cybersecurity Skills Shortage: A State of Emergency, February 2016

6 ISACA's January 2016 Cybersecurity Snapshot, Global Data

For more information contact

Bill Millar
Global CISO Infrastructure Services
Capgemini
bill.millar@capgemini.com

About Capgemini and Sogeti

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security. Sogeti brings together more than 23,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

For more information visit:

www.capgemini.com or **www.sogeti.com**

MCOS_GI_MK_20160609