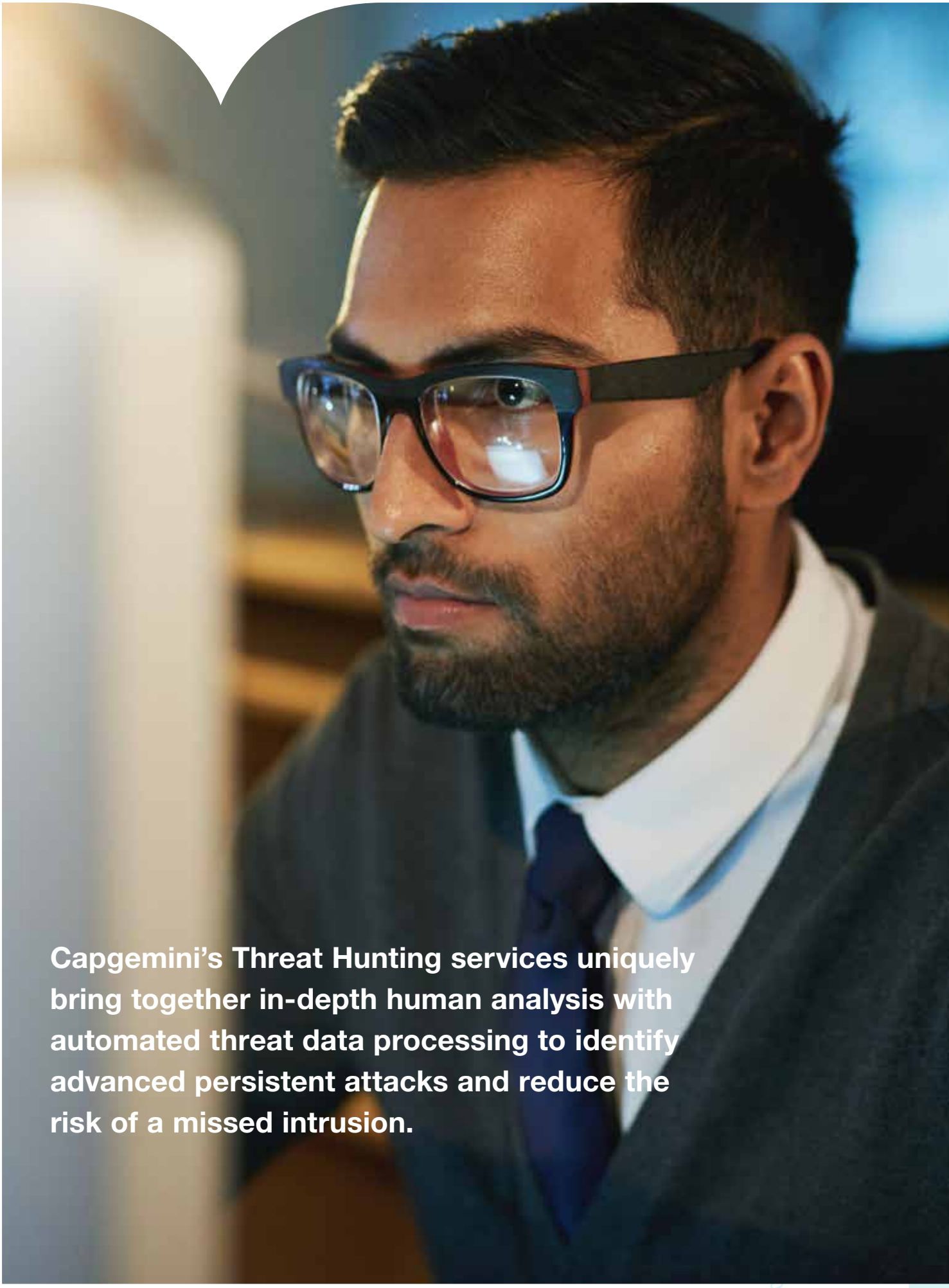
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Have you been hacked?

Spot attackers hiding in your IT system when protection and monitoring measures have failed to detect them.

People matter, results count.



Capgemini's Threat Hunting services uniquely bring together in-depth human analysis with automated threat data processing to identify advanced persistent attacks and reduce the risk of a missed intrusion.

The challenge

Hunting down the cyber threat before it causes untold damage

Every organization has the potential to be hacked, even when protection measures are in place. Today's cyber attackers are patient, smart, and willing to spend time and resources to achieve their goals. This means that having gained access to your corporate network and systems, a hacker might hide inside your organization for weeks, or even months, carefully learning and waiting. During that time, information can be compromised or stolen, while a dormant malicious code could stay out of sight and ready to strike at any time. Indeed, research suggests that it can take more than one hundred days to detect an attack on your system.

The threat is very real. Thus, investment in protection and monitoring capabilities is an accepted strategic priority in the digital enterprise. Many organizations believe that these measures make a malicious intrusion impossible. This is a dangerous perception. Evidence from across the world clearly shows that 100% protection can never be guaranteed.

Simply installing virus protection will not keep out the hackers. And reporting or stopping bogus attempts won't mitigate the threat already inside your system. As cyber attacks become ever more sophisticated, Chief Information Security Officers (CISOs) are expected to know whether their organization has been hacked.

Forward-thinking CISOs recognize that in today's connected world they must assume their defenses have been breached, even if existing protection and monitoring measures have not spotted the intrusion. That's where our Threat Hunting services can help. Recognizing that no protection is wholly proof against attacks, we complement automation with expert human analysis to keep you on top of evolving threat methods. This reduces the risk of automated data analysis on its own missing malicious intrusions.

Capgemini's Threating Hunting services go beyond known threats to consider both unknown and advanced persistent threats, thwarting even the most determined cybercriminals.

Our response

Combining expert in-depth human analysis with automation

Capgemini's new Threat Hunting offering recognizes that protection and monitoring measures are not infallible. It is also difficult for detection tools to stay on top of evolving threats. As such, it is vital to spot a malicious intrusion as quickly as possible to limit the damage caused.

Acknowledging both the strengths and the limitations of an automated response, our Threat Hunting services incorporate expert in-depth human analyses alongside the automated collection of threat data. This combined human-automated approach reduces the risk of automated data analysis on its own missing an unknown attack and identifies advanced persistent threats.

Capgemini's Threat Hunting services have been designed by experts in our R&D team. It equips our clients with the skills and resources needed to set up and maintain a continuous threat hunting capability.

Our Threat Hunting services provide:

- Automated tools and a dedicated team with specific expertise in identifying the source of threats;
- Constantly evolving skills within a team that is available however often, and whenever it is needed;
- Knowledge of where malicious code is coming from, enabling the prevention of future breaches.

Absence of immediately evident intrusion does not mean that a system is clean. A new Zero-Day Vulnerability was discovered every week, on average, in 2015. This was a 125% increase over the previous year.

2016 Internet Security Threat Report[1]

1 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Key differentiators

A unique approach to spotting cyber attacks

Capgemini's Threat Hunting services are designed to spot attackers that have successfully entered an IT system when protection and monitoring measures have failed to detect them.

Among the key differentiators are:

- Human analysis reduces the risk of missing an attack, while a focus on anomalous behavior and unwanted changes to authorized programs detects unknown attacks;
- Our inclusion of in-depth human analysis recognizes that automation requires strict security rules, which can miss malicious activity or generate too many false positives. Further, it addresses the failure of machine learning to spot an attacker already inside the IT system;
- We keep our scope narrow and focus on a defined critical perimeter. At the same time, we do not restrict the number of alerts flagging suspicious activity, enabling us to focus on all manner of suspicious behavior;
- Managed Security vendors offer similar services as part of their Security Operations Centers (SOCs), but they rely on logs that can be modified by motivated attackers. Nonetheless, SOCs are a powerful tool in the cybersecurity armory and base their detection on a large perimeter for future attacks. Our Threat Hunting takes a different approach by considering both unknown and advanced persistent threats.

In its annual Cost of a Data Breach Study 2016, the Ponemon Institute reported an increase in the average cost of a data breach from US$3.79 million to US$4 million.

According to research, ransomware is "the fastest-growing malware across all industries in 2016" and "on track to be a US$850 million crime in 2016, according to FBI data", up from $24 million in 2015.[2]

2 https://www.carbonblack.com/wp-content/uploads/2016/12/16_1214_Carbon_Black-_Threat_Report_Non-Malware_Attacks_and_Ransomware_FINAL.pdf

“Threat Hunting is a compelling and exciting development in Capgemini’s cybersecurity portfolio.”

Franck Greverie
Cloud & Cybersecurity Leader, Capgemini Group

The Benefits of Threat Hunting

Reducing the risk of undetected intrusion

Increasing digitization has created wide-ranging vulnerabilities for the modern enterprise. As cyber attackers find ever smarter ways to breach security defenses, research suggests that more than half of attacks take months to be detected. This is a huge concern. The cost of failing to identify an attack has severe implications for your bottom line, ranging from a loss of customer confidence and potential theft of intellectual property, to fines for data security non-compliance.

Capgemini's Threat Hunting services reduce this risk. They detect unknown attacks and flag suspicious activity.

By uniquely combining expert human analysis and automated detection of anomalous behavior and unwanted changes to authorized programs, Threat Hunting delivers:

- Rapid identification of a malicious intrusion, preventing attackers remaining hidden for long periods of time;
- Reduced risk of automated data analysis on its own missing malicious intrusions;
- Continual development of threat awareness as the threats evolve;
- Knowledge of both unknown and advanced persistent threats;
- Sight of suspicious activity that existing security measures have failed to spot.

Client stories

Cybersecurity at a Government Agency

In a two-week project, during which 50,000 alerts were generated for a small, defined critical perimeter, Capgemini's analysts investigated 18 suspicious behaviors. Designed to prevent the likelihood of a missed intrusion into their IT system, these investigations covered specific user requests, such as those for tools and internal development, as well as for non-standard usage, including the testing of new software. The results confirmed the integrity of the defined perimeter.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Contact details:

Mike Turner
Cybersecurity COO, Capgemini Group
mike.a.turner@capgemini.com

Arnauld Mascret
Global Head of Threat Hunting Services
Capgemini Group
arnauld.mascret@sogeti.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.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 3,000 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT, industrial systems, and the Internet of Things (IoT) products & systems. We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, eight security operations centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

Learn more about us at

www.capgemini.com/threat-hunting

MCOS_GI_AH_20170120