Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Combating a new generation of cybercriminal with in-depth security monitoring

1st Advanced Data Analysis Security Operation Center

The Challenge

Don't leave your systems unmonitored. It takes an average 229 days to detect a system security breach[1]. That's a long time for a cybercriminal, competitor, or even disgruntled employee to have unauthorized access to your business systems and critical information assets.

Even an organization that's well protected with the right tools and the right processes in place leaves itself open to attack if it is not monitoring systems; detecting potential security incidents; and able to make changes to its operations quickly to counter any threat detected. This is because today's hackers and hacktivists are both determined and patient. They will wait, watch, and seize their moment.

Advanced attacks are a real and present threat. More than half (56%) of organizations have been hacked[2], and 2014 saw a 120% increase in reported security breaches[3]. The risk posed by a cyber attack to both reputation and revenue is clear. Some 46% of people globally report leaving or avoiding companies that have had security issues.

[1] FireEye, 2013

[2] HP, 2013

[3] Factiva, 'Major News and Business Publications' database; Thomson Financial, Investext database; databases of various security agencies

The Security Operation Center (SOC)

A SOC is the centralized incident-response team reporting through the Chief Security Officer/Chief Information Security Officer (CSO/CISO).

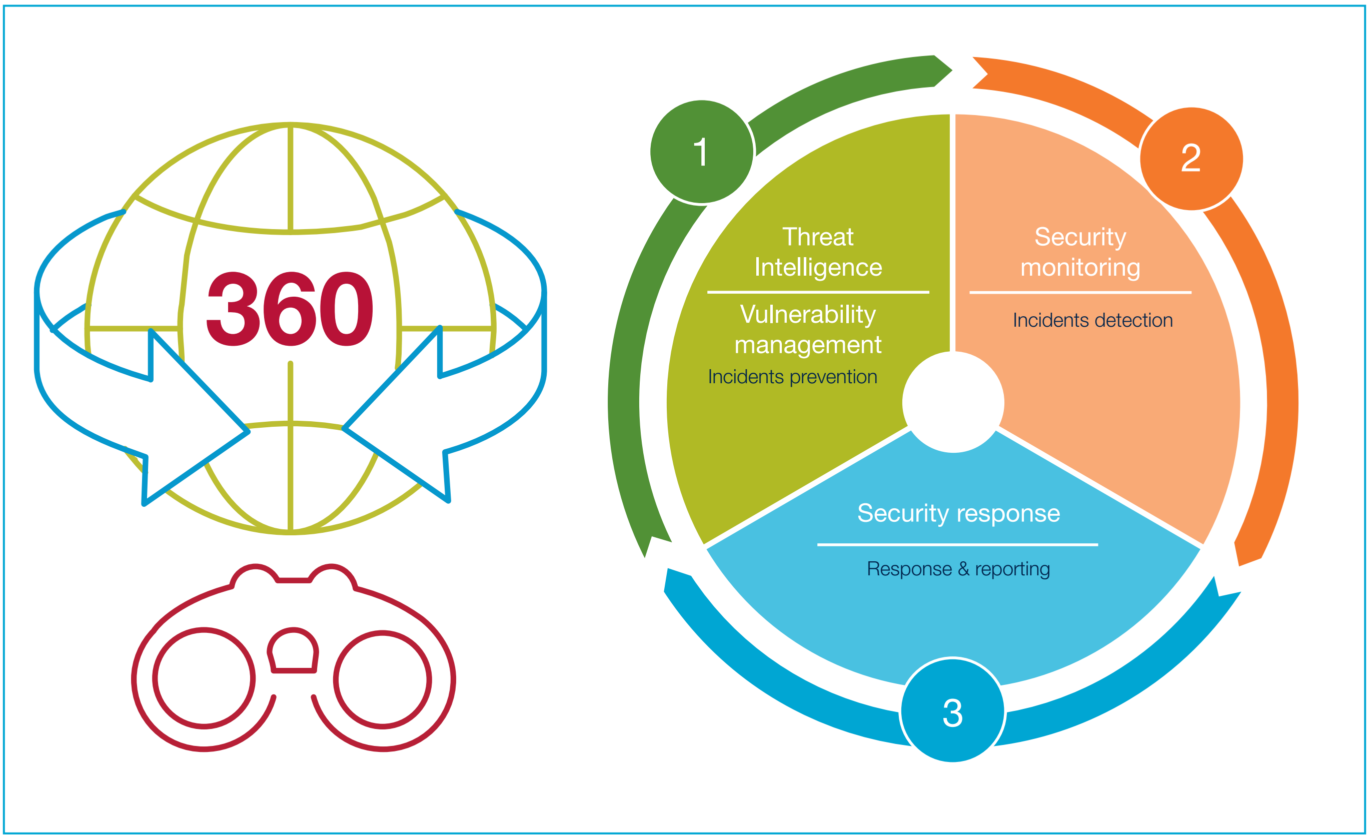
Gain complete visibility of your IT and security system with our Security Operation Center (SOC). It enables you to detect, analyze and respond to cyberattacks.

The SOC is comprised of three elements:

- **Incident prevention:**
  - Threat intelligence
  - Vulnerability management
- **Incident detection and analysis:** detect and analyze even the most advanced attacks before they damage the business
- **Incident response:** take targeted action against the most serious incidents..

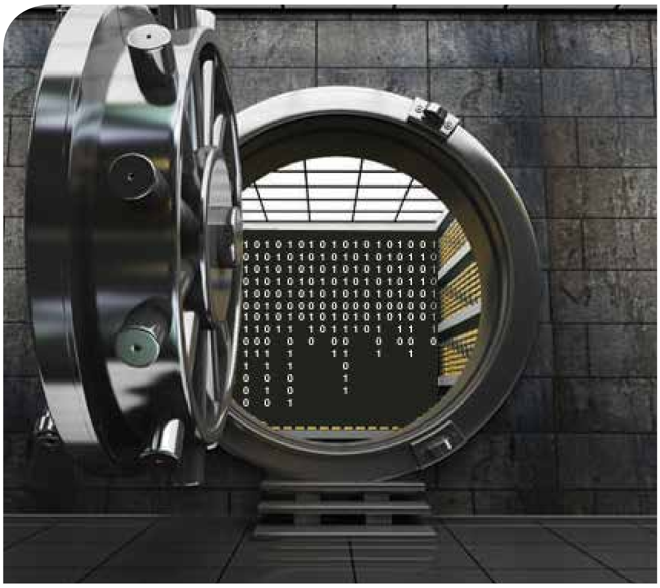
A SOC is the centralized incident-response team reporting through the Chief Security Officer/Chief Information Security Officer (CSO/CISO). It consists of **people, process and technology.**

The SOC orchestrates the multiples roles, processes and technology to enable efficient incident detection and response.

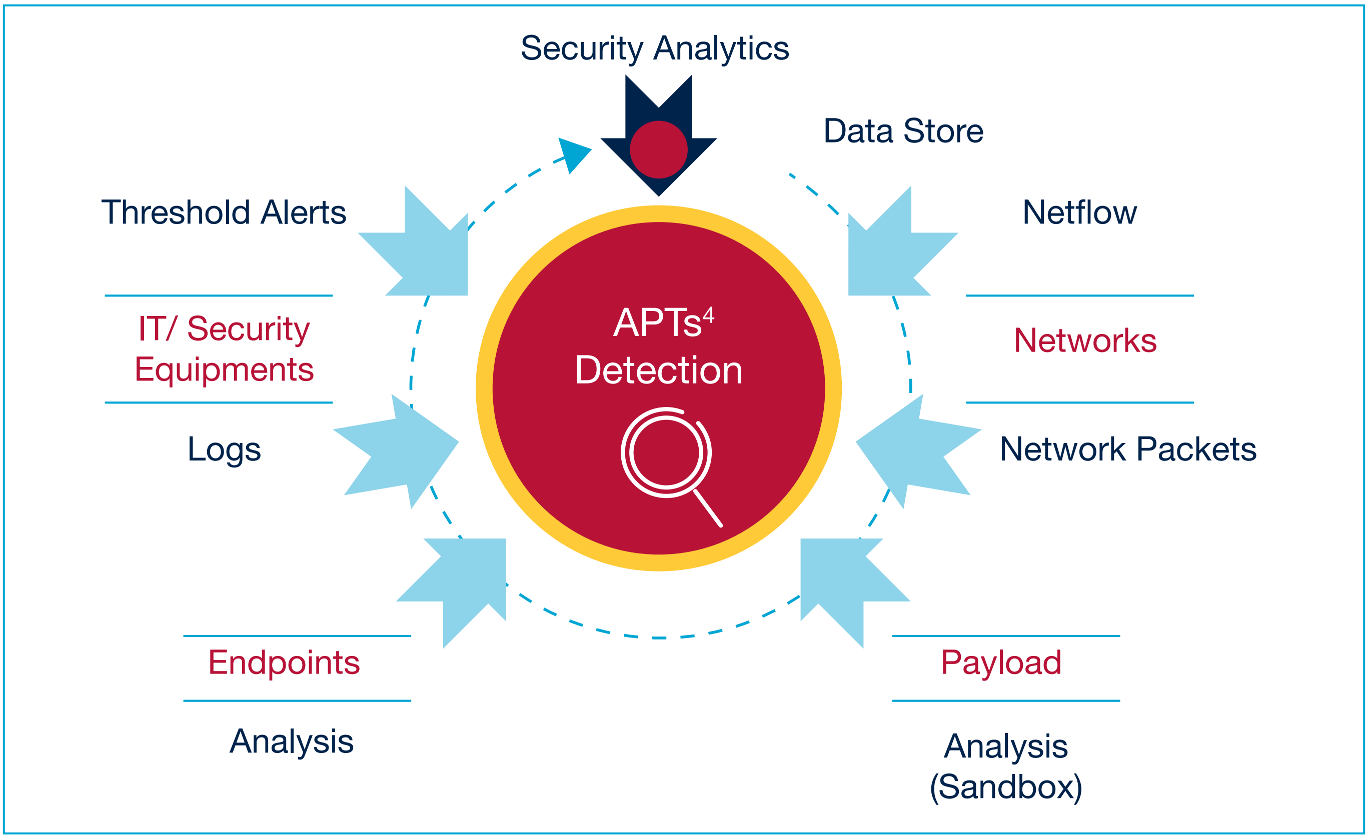


A more determined adversary means more data is needed to identify cyberattacks. More complex IT environments make it possible for even a simple cyberattack to hide in plain sight.

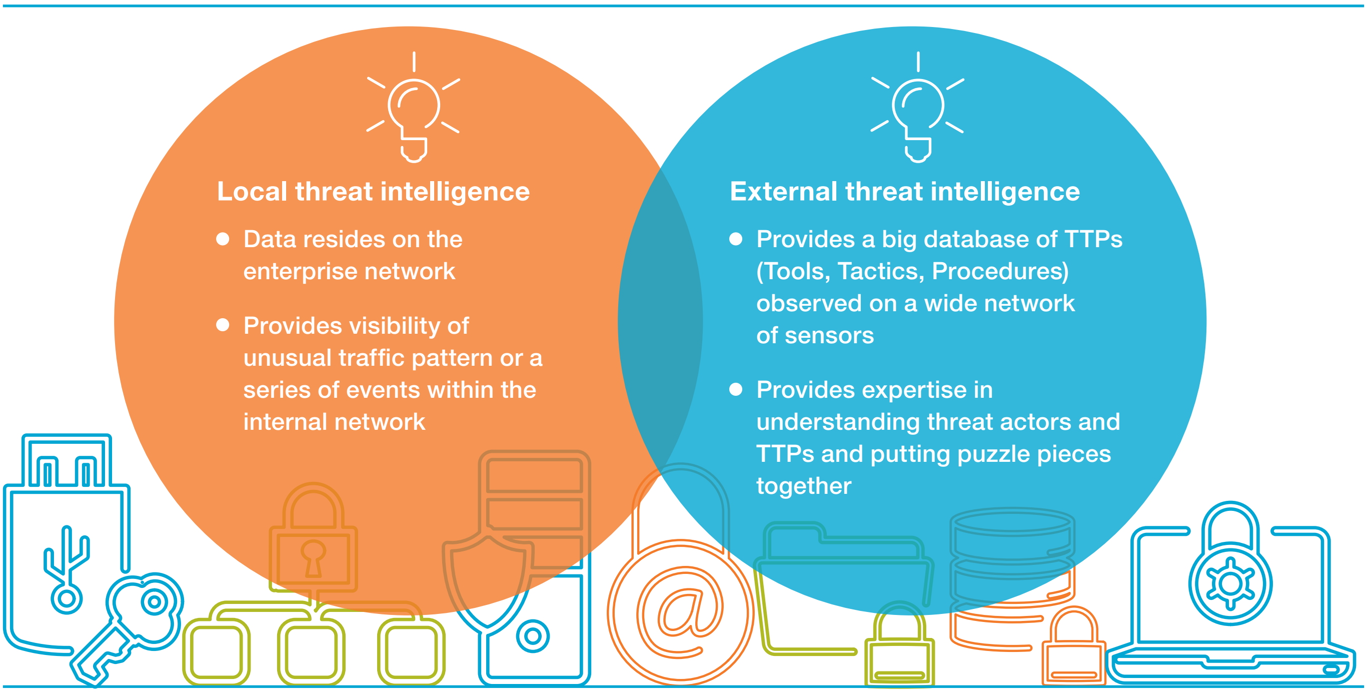
Such is the complexity of today's digital world that security professionals are struggling to keep up. That's why the early, 1st generation SOC is no longer up to the task. It met – and continues to meet – the basic need for a low cost solution enabling regulatory compliance and log monitoring.



Insights never seen before



[4] Advanced Persistent Threats



Local threat intelligence

- Data resides on the enterprise network
- Provides visibility of unusual traffic pattern or a series of events within the internal network

External threat intelligence

- Provides a big database of TTPs (Tools, Tactics, Procedures) observed on a wide network of sensors
- Provides expertise in understanding threat actors and TTPs and putting puzzle pieces together

But this isn't enough! Compliance is not security.

More data is needed to identify cyberattacks.

The 2nd generation SOC enables you to combat advanced threats by bringing together security information and event management (SIEM), network security monitoring, endpoints monitoring, payload analysis and offline big data analytics.

To manage the huge amount of data available in a 2nd generation SOC, our analysts use a unified workflow to:

- Focus on their most critical tasks and complete end-to-end incident management in minutes, not hours;
- Do more with same amount of people by spending their time on the incidents that have the biggest risk to the organization and completing them as fast as possible;
- Use a single tool to perform actions currently only possible within a disparate set of interfaces.

A new generation of detection and response

That's not all. We are now able to offer our clients a new, 3rd generation SOC – the 1st Advanced Data Analysis SOC. This improves still further both the capacity to detect the most sophisticated Advanced Persistent Threats and the incident response. Our 1st Advanced Data Analysis SOC adds four services to those already offered within the 2nd generation SOC:

1. More focused detection rules
   - We integrate our team of analysts with the client organization, enabling us to define more focused, accurate detection rules corresponding to the client's IT environment. We have defined a methodology enabling efficient cooperation without diluting responsibilities. This methodology ensures that our customers can achieve exactly the right balance of accountability and responsibility with their managed security service provider.
2. Deeper understanding of the context
   - Threat intelligence
     - The SOC collects and analyzes cyber threat intelligence to gain insight into adversaries and their motivations, intentions, and methods.

This knowledge is disseminated to help security and business staff at all levels protect critical enterprise assets.

- Understanding the applications included in the attack perimeter

See Data You Didn't See Before
Understand Data As Quickly As Possible

3. More efficient response
   - Creating a strong link with the IT Service Management (ITSM)

To Define Efficient Remediation Actions

- Creating a security dashboard highlighting both technical and business risks.

4. Security analytics
   The 1st Advanced Data Analysis SOC has three key focus areas for its security analytics:
   - **User:** provides visibility of user behavior to detect malicious or negligent users, or identify external attacks that compromise user accounts across the enterprise;
   - **Applications :** this combines analytics with our cloud-based application security testing offer. The SOC processes an organization's growing collection of historical application security scan results to reduce the number of issues that require an auditor's review. This enables our clients to focus resources on fewer, higher priority tasks.
   - **DNS Malware :** identifies malware-infected hosts, such as servers, desktops and mobile devices, so that they can be contained before gaining access to the network. We analyze a high volume of DNS records to detect new, unknown malware. This saves valuable IT time and resources, enabling clients to prioritize and remediate based on the highest risk devices.

Our 3rd generation SOC proposition embraces 1st and 2nd generation SOCs, as well as the 1st Advanced Data Analysis SOC. It is tailored according to a client's individual needs.

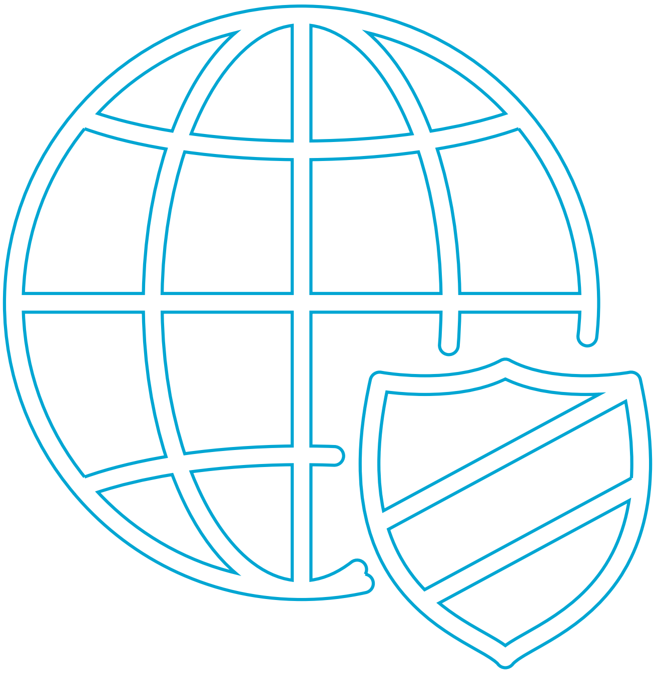
We can deliver security monitoring services though a dedicated customer SOC or through a multi-tenant platform from Europe or India.

Assurance and trust with 1st Advanced Data Analysis monitoring capabilities

A SOC is a set of processes, technologies and a team: a team of trusted security analysts trained to be efficient and on top of its game.

In addition to security analysts, we have an **elite R&D team:**

- able to analyze and reverse engineer the most complex malware;
- able to support you in in the event of severe cyberattacks;
- able to perform deep security tests on security products (for example data sources: sandbox, IPS, etc.) to identify their weaknesses (zero days) or backdoors.



In summary

The 1st Advanced Data Analysis SOC brings a new approach to security that addresses critical challenges:

- Despite increasing investments in security, breaches are still occurring at an alarming rate. Traditional security protection is far from sufficient to secure your enterprise's most valuable assets;
- Traditional SIEMS have not evolved sufficiently to meet the security challenge and combat sophisticated cyberattacks. Log-centric SIEMs cannot defend against attacks. While they connect the dots between security incidents to give security analysts some level of visibility of what is going on across the enterprise, the logs lack the detail needed to understand what is truly happening in the IT system. In fact, 99% of successful attacks were undiscovered by logs (source: Verizon breach report 2014).

New Approach to **security :**

Real-Time and Offline Analysis of Multiple Data Sources

Enhanced by a Good Understanding of the Context

Capgemini and Sogeti – keeping your systems, applications and data protected day and night. Find out more at **www.capgemini.com/soc** and **www.sogeti.com/soc**

About Capgemini and Sogeti

With 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 2014 global revenues of EUR 10.573 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 20,000 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 2,500 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 multi-tenant security operation centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

For more information, please visit:

www.capgemini.com/cybersecurity or www.sogeti.com/cybersecurity