Capgemini

Threat Intelligence Service

End-to-end visibility and actionable analysis - so you can get proactive about protecting your enterprise.

The surge in cybersecurity threats is well documented. Malware, data breach attacks, phishing exploits, ransomware, cryptojacking, and many other threats are on an upward spiral in sheer volume and level of sophistication. The reasons are also well documented: increased reliance on IT systems and decentralized data make enterprises more attractive and more vulnerable to criminal elements.

The question is, how can you stay a step ahead of malicious actors in this environment? How can you transform everything that's known about specific cyber threats into proactive protection for your enterprise?

Capgemini's Threat Intelligence Service combines granular, continuously updated information about cyber threats with rigorous analysis by experts using AI, analytics, and automation. It detects threats quickly and accurately and delivers early warnings, alerts, and recommended actions for IT and end users--so they can respond effectively and prevent successful attacks.

Our threat intelligence is aggregated and analyzed by experts at our global, connected network of security operations centers (SOCs). The Threat Intelligence Service gives you access to:

• Complete, accurate, up-to-date threat intelligence from many sources

• Specialized intelligence such as dark web and social media hunting to help protect your brand

• Sector-specific threat intelligence and cybersecurity expertise in your industry

• Personalized services and on-call support

Capgemini's Threat Intelligence Service goes beyond the capabilities of competitive offerings because it delivers the end-to-end visibility you need to understand precisely:

• How secure your enterprise is, with attack probabilities and potential impact analysis

• How IT and employees should respond to a detected threat or attack

• How effectively your security budget is being spent and how to optimize spending

Armed with this intelligence, you can protect your users, systems, endpoints, networks, clouds, IoT devices, and industrial systems. Equally important, you can move ahead with your strategic initiatives—quickly and confidently. You can disrupt in the digital arena without fear of being disrupted. You can strengthen your defenses without breaking the budget. And you can transform security from a source of expense and worry into a source of competitive advantage.

Comprehensive threat intelligence requires a global perspective

Threat intelligence is widely available from many sources in many different forms. The key to effective enterprise security is not finding threat intelligence—it is finding the **right** intelligence, from the **right** sources, and using it in the **right** way. That requires access to timely, relevant, accurate, actionable, sector-specific intelligence from around the globe, along with the ability to integrate and rigorously analyze that intelligence.

Capgemini is uniquely capable of delivering on these demands because we bring global capabilities, global resources, and a global scale to the collection and analysis of threat intelligence. We combine:

• **A connected, global network of Security Operations Centers (SOCs)** that give you direct, on-demand access to threat intelligence and expertise on an unprecedented scale. The SOCs bring together the experience of 4000+ security professionals and a set of proven, certified processes and technologies. We monitor clients' environments continuously and completely to provide end-to-end visibility into their security posture, and we harness advanced data analytics to detect and respond to incidents and prevent successful attacks.

USA Foxborough
USA Columbia
USA San Diego
USA Dallas
Brazil Sao Paulo
Netherlands Utrecht
Luxembourg
Germany Frankfurt
UK Inverness
France Paris
Spain Asturias
France Toulouse
India Mumbai
India Bangalore
Australia Melbourne

■ SOC ■ Satellite ■ Opening shortly

Figure no.1 - Capgemini maintains a global network of SOCs that monitor and analyze threats constantly

Cyber threats: more prolific and expensive than ever.

The number, diversity, sophistication and costs of cyberattacks are on the rise. Last year alone:

• 54% of companies experienced one or more successful attacks that compromised data and/or IT infrastructure [1].

• The average cost of a successful ransomware attack was $5 million[2].

• 54% of companies experienced an industrial control system security incident[3]. More than 5,207 data breaches were reported, at an average cost of $3.86 million per data breach incident and $148 per record[4].

• Illicit cryptocurrency mining malware detections rise by 459% over the previous year[5].

• 64% of organizations have deployed IoT devices, and 61% of those have already experienced an IoT security incident[6].

[1]Ponemon Institute, "The 2017 State of Endpoint Security Risk Report."
[2]Ponemon Institute, "The 2017 State of Endpoint Security Risk Report."
[3]Business Advantage State of Industrial Cybersecurity 2017.
[4]Ponemon Institute, "The Cost of a Data Breach," 2018.
[5]Cyber Threat Alliance, "The Illicit Cryptocurrency Mining Threat," August 2018.
[6]Trustwave: IoT Cybersecurity Readiness Report, 2017.

Capgemini maintains a global network of SOCs that monitor and analyze threats constantly.

- **Accurate, timely threat intelligence from multiple sources.** We aggregate threat intelligence from many sources, enabling us to identify and defend against known attacks and attack vectors you may not have seen before. Our threat intelligence includes:
  - **Vendor feeds** from trusted suppliers and third-party partners, such as IBM XForce
  - **Security forums** that tap into the expertise of large communities of cybersecurity analysts and professionals
  - **Social media** such as Facebook, Twitter, Instagram, and dozens of other popular social media platforms
  - **Security events,** which provide analysis of newly discovered attack vectors
  - **Malware research** from our own analysts as well as recognized, respected third-party sources
  - **Sector-specific threat intelligence** for virtually every industry, including banking and financial services, healthcare, government, utilities, oil & gas, manufacturing, retail, and more
  - **Specialized intelligence** such as dark web monitoring, new and trending malware detection, leaked credentials, vulnerability identification enrichment, and brand monitoring
- **Access to our elite R&D team.** The Threat Intelligence Service can connect you to the expertise of our team of professionals who can analyze and reverse-engineer complex malware to support you in case of very severe cyberattacks.

Specialized Intelligence for a more complete picture

Capgemini aggregates specialized intelligence feeds to give you complete visibility, including:

- **Dark Web Monitoring:** Our solution enables you to track indicators of compromise from dark web threat feeds and identify vulnerability information uniquely relevant to your business.
- **New & Trending Malware Detection:** We constantly look for trending malware and help you gain contextual knowledge of the threat.
- **Leaked Credentials:** Our solution can be configured to alert you when a specific set of corporate domains are seen in connection with leaked credentials, dramatically increasing visibility into potential breaches of corporate data and code.
- **Vulnerability Identification Enrichment:** Intelligence from harder-to-reach sources enables you to more rapidly identify emerging threats and make faster, more informed security decisions.
- **Brand Monitoring:** We constantly monitor for threats such as Typo Squatting and Fake Domains that could be a risk to your brand reputation, and we have the capability to strategically monitor, identify and respond to potential risks such as fraudulent domains, fake mobile applications, and other threats to the brand.

Visibility that enables you to respond quickly and intelligently

The result of our global capabilities and diverse range of threat intelligence resources is that you get end-to-end visibility into your security posture, up-to-date assessments of risks, and timely recommendations about how best to respond to attacks.

For example, we constantly monitor your environment not only for known threats such as WannaCry and NotPetya, but also for new and emerging threats such as ransomware attacks or cryptojacking exploits.

With our use of advanced AI, analytics, machine learning, and automation, we also bring situational awareness and context to our assessments, reducing both false alarms and mis-identification of potential new threats.

The result: you experience increased response efficiency against cyber attacks, and you consistently protect your enterprise and your brand against malicious activity that other technologies may have missed.

Flexible subscription tailored to your needs

Capgemini's Threat Intelligence Service is available on a subscription basis and offers multiple options to accommodate your specific requirements.

We can deliver Define Services addressing the full range of cybersecurity strategy, assessment, and deployment needs, as well as Managed Security Services covering your applications, networks, endpoints, data, end users, infrastructure, clouds, perimeters, and more, all with a range of service levels.

Capgemini is the one service provider who can bring everything together for your enterprise: end-to-end

Advanced Services	**Enhanced Services**	**Standard Services**
Focuses on defining a world-class threat intelligence program	Identification of motivations, intentions and capabilities of the actors targeting the business	Building blocks for developing Threat Intelligence practices and capabilities

• Security Alert
• Security News
• Specialized Intelligence
• Personalized Intelligence
  • SOC Integration(with Firewall and SIEM)*
  • Proactive Blocking*
  • Take Down Service*
• Identify Attack Planning (Targeted Attack)
• Major Crisis Support
• Monthly Dashboard
• Proactive event alerting
• 24*7 service support
• 24*7 On call support
	• Security Alert
	• Security News
	• Specialized Intelligence
	  • Leaked Credentials Monitoring`
	  • Dark Web Monitoring
	  • Social Media Monitoring
	  • Vulnerability Identification Enrichment
	  • New & Trending Malware Detection
	  • Industry specific Attack Trends
	  • Infrastructure Risk
	  • Phishing or Spam Campaign Trends
	  • Brand Reputation Risk
	  • Gift cards and Credit Card Monitoring
	  • Targeted Threat Actor Research
	  • Third-Party Supplier and Partner Trends
	  • Undisclosed Vulnerabilities(Zero day)
	• Proactive event alerting
	• 24*7 service support
		• **Security Alert –** Notification related to security vulnerabilities mapped with client technology stack
		• **Security News –** Notification related to global attack campaigns and threat actors
		• **Specialized Intelligence**
		  • Vulnerability Identification Enrichment
		  • New & Trending Malware Detection
		  • Undisclosed Vulnerabilities(Zero day)
		• **9*5 service support**

*License cost for the API feed integration with SOC tools as well as Take Down Service will be separate.

An integral part of our comprehensive cybersecurity capabilities

The Threat Intelligence Service is a core element of our overarching, end-to-end offerings in cybersecurity.

cybersecurity solutions from multiple vendors, coupled with a comprehensive portfolio of consulting and managed service offerings—globally or locally, in virtually every industry and market segment.

We can serve as your single trusted advisor for integrating and orchestrating your cybersecurity solutions globally, and we have many years of experience covering security requirements in virtually every industry and market segment, at a scale that will match your needs today and tomorrow.

Cybersecurity Define Services

Strategy

Strategic Consulting	Operational Consulting

Assessment

IAM Fast Track	End Point Security	GRC Assessment
Cyber Attack Simulation	GDPR Assessment	Cloud Security Assessment
	Vulnerability Scanning	

Deployment

Cryptographic deployment	Endpoint Sec. deployment	IAM Deployment
Network Sec. Deployment	SIEM deployment	GDPR Controls Deployment
Security Platform Service	Security Incident response	

Managed Security Services

- Security Management Services
- Multitenant Managed SOC
- Managed SIEM
- Application Security Testing (AST)
- Endpoint Protection as a Service (EPaaS)
- Data Loss Prevention (DLP)
- Cloud Security
- Identity as a Service (IDaaS)
- Cryptographic Service
- Automotive Cybersecurity
- GDPR Readiness
- Industrial Systems & IoT
- Perimeter Security

Strategy services

- Strategic consulting
- Operational consulting

Assessment services

- Security of endpoints to clouds
- Vulnerabilities
- Compliance assessment
- Overall security posture

Deployment services

- Technologies
- Solutions

Managed security services (MSS)

For details about any of the services above visit **www.capgemini.com.**

Compelling advantages

Our ability to deliver comprehensive threat intelligence and cybersecurity capabilities results in multiple advantages that truly set us apart. These include:

End-to-end and ecosystem expertise.

In an era of disjointed security solutions and increasingly diverse attack vectors, Capgemini is the one service provider who can bring everything together: comprehensive threat intelligence, end-to-end cybersecurity solutions from multiple vendors, coupled with a comprehensive portfolio of consulting and managed service offerings—globally or locally, in virtually every industry and market segment.

A business-focused, collaborative approach.

We start by understanding your specific requirements from a business perspective. Through discussions with your key stakeholders, we tailor a strategy and an approach that aligns with your business objectives, then we recommend services tailored to your specific needs.

IoT and industrial security skills.

Armed with sector-specific threat intelligence, Capgemini Enterprise Operational IoT experts can assess the security posture of your industrial systems and IoT devices, including maturity analysis of industrial information systems, risk analysis of critical systems, and creation of a roadmap to improve the organization's defenses, while delivering quick wins in reducing risk.

Cloud security specialization.

Capgemini has broad and deep expertise in cloud security, enabling you to adopt a range of dedicated and hybrid cloud models safely and cost-efficiently. Capgemini can help you assess your current cloud security maturity level; map your current posture against security services offered in clouds; implement security practices and tools to protect infrastructure, applications, platforms and data in the cloud; provide recommendations to address security compliance gaps; manage security incidents; and more.

Global scale.

We are everywhere you and your networks, devices and users are, worldwide. With a global web of SOCs and research labs, over 4000 security professionals, and presence in over 200 hundred countries, we can deliver the advice, skills and managed services you need, your way, anywhere in the world.

Industry recognition.

Capgemini is recognized as a leading cybersecurity and managed security services provider by analyst firms such Gartner, IDC, NelsonHall, and HfS Research in their respective publications.

Top talent.

Our 4000+ skilled cybersecurity experts hold industry standard certifications such as CISSP, CISM, CISA, CCSP, including ITIL, CEH, CCIE and other technology certifications.

Satisfied clients.

We carefully measure and monitor client satisfaction, and the vast majority of our clients are "highly satisfied" with the services they receive. Just ask us for case studies and a detailed client list in your sector.

Simplicity.

The complexity of cybersecurity can be overwhelming. We extract complexity at every turn, so you can focus on your business goals and strategic initiatives. We're here to make your life simpler while we make your enterprise safer.

Get proactive. Contact Capgemini.

Take the next step toward proactive protection of your enterprise. Contact Capgemini today and learn more about our uniquely effective Threat Intelligence Service.

About Capgemini and Sogeti

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE., listed on the Paris Stock Exchange.

For more information please visit

www.sogeti.com

For further information please contact:

infra.global@capgemini.com