

# The future of enterprise security is here

Next-generation SIEM from Capgemini and IBM



# The cyber threat landscape is growing more complex

---

Malicious attacks can  
take an average of  
**146 days** to identify<sup>3</sup>

---

## No place to hide

While technology's increasing sophistication brings opportunity to unlock business value, it also brings a growing security threat. IBM's latest Intelligence Index<sup>1</sup> showed that cyber attacks are becoming not only more advanced and audacious, but also more varied—from stealing intellectual property to writing malicious code to lodging political protests. No organization is immune. Increasingly, enterprises are finding to their cost that legacy or piecemeal security solutions are no longer adequate. In addition, as the growing demand for cybersecurity expertise far outpaces supply, many enterprises lack the resources in-house to direct, execute and hone cybersecurity strategies.

## A new generation of cyber defense

Many enterprises have already implemented SIEM (Security Information and Event Management) yet have failed to reach the expected benefits because security threats are evolving so quickly in complexity. The lesson is clear: enterprise cybersecurity must also evolve. Enterprises need a solution that is robust, yet not rigid; that is powerful yet intelligent. The new threat landscape calls for a new generation of cybersecurity services that are flexible enough to adapt to the enterprise, yet able to evolve with emerging threats to identify and pre-empt sophisticated attacks.

## Counting the cost of cyber attacks

A recent report<sup>2</sup> into the cost of data breaches—just one of many possible outcomes of a cyber attack—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. With so much at stake, cybersecurity is no longer simply a technology issue—it's a key business challenge. At Capgemini, we believe that enterprise security begins with a holistic view and smart thinking, alongside industry-leading technology. That's why we partner with IBM to offer a new generation of intelligence-driven Multi-Tenant Managed Security Operations Center (SOC) services. Underpinned by the market-leading QRadar Security Intelligence Platform from IBM, it puts control of enterprise security back into your hands.

## The next generation of enterprise security starts here.

<sup>1</sup> <http://public.dhe.ibm.com/common/ssi/ecm/se/en/sej03320usen/SEJ03320USEN.PDF?>

<sup>2</sup> 2015 Cost of Data Breach Study: Global Analysis Ponemon Institute, May 2015

<sup>3</sup> M-Trends 2016 Report, Mandiant Consulting

# Capgemini's Managed SOC: Protecting your business against advanced attacks

Our response to enterprises' rapidly evolving security requirements is a progressive range of end-to-end managed services hosted in India and based on the proven Security Operations Center (SOC) model to enable fast and flexible deployment. Backed by industry-leading SIEM technology from IBM, intelligence-driven Managed SOC from Capgemini brings advanced data analysis to enterprise security, enabling security threats of all types to be identified early and counteracted swiftly, decreasing cost and disruption to the business. What's more, implementations are designed with each client's own set of business risks at the core.

## Partnering for your security

We're harnessing the power of partnership to help you protect your business. Built on IBM's QRadar Security Intelligence Platform with advanced IBM Sense Analytics, Managed SOC enables enterprises to move quickly from being exposed to achieving a high degree of security control, turning from the hunted to the threat hunter. QRadar draws on IBM's strong analytics capabilities to bring deeper-than-ever-before insights and, in turn, enhanced abilities to identify evolving threats from within and from outside the enterprise. Capgemini uses a broad range of threat intelligence sources when allied with QRadar, enabling your organization to take a proactive approach to cybersecurity—and putting you firmly in the driving seat.

## Risk-based security

Enterprises are faced with the complex challenge of avoiding and managing risks. These may be related to regulatory and other compliance, where their license to do business and their reputation is at stake, or they might become liable to fines and other repercussions in case of non-compliance. Complying to laws and framework controls, in and of itself, does not always mean an enterprise is well protected to prevent or counter cyber attacks. Threat landscapes as well as technologies develop at a speed that these laws and frameworks can impossibly keep up with. Managed SOC addresses risk to both compliance and cyber threats, using the intellectual capability of our analysts with the technical power of QRadar and our Golden Hour processes to respond to attacks.

## Deployment flexibility

Multi-Tenant Managed SOC is available as a suite of utility services that can be deployed to integrate with and complement your install-base. Our team of security and cloud specialists works with you to identify the deployment option that meets your organization's needs.

## Meet IBM's QRadar Security Intelligence Platform

IBM has taken SIEM to the next level with QRadar. Together with IBM Sense Analytics, it helps identify threats and eliminate attacks by analyzing security data and matching user behavior with log events, network flows, threat intelligence, vulnerabilities and business context.

- IBM Security named a Leader in Gartner Magic Quadrant for Security Information and Event Management since 2009<sup>4</sup>
- Single platform for analyzing log, flow, vulnerability, risk, user and asset data
- Identifies high risk threats in near real-time, provides quick and easy forensics investigation of security offences and includes ability to rapidly build and execute incident response plans
- High-priority incident detection among billions of data points
- Provides visibility of activity across the network, applications and users
- Addresses regulatory requirements through collection, correlation and reporting capabilities
- Winner of the 2015 SANS Best of Awards in the category 'SIEM'<sup>5</sup>

<sup>4</sup> Gartner\*, Magic Quadrant for Security Information and Event Management 20 July 2015. IBM acquired Q1 Labs in 2011.

<sup>5</sup> <https://www.sans.org/critical-security-controls/best-of-awards>

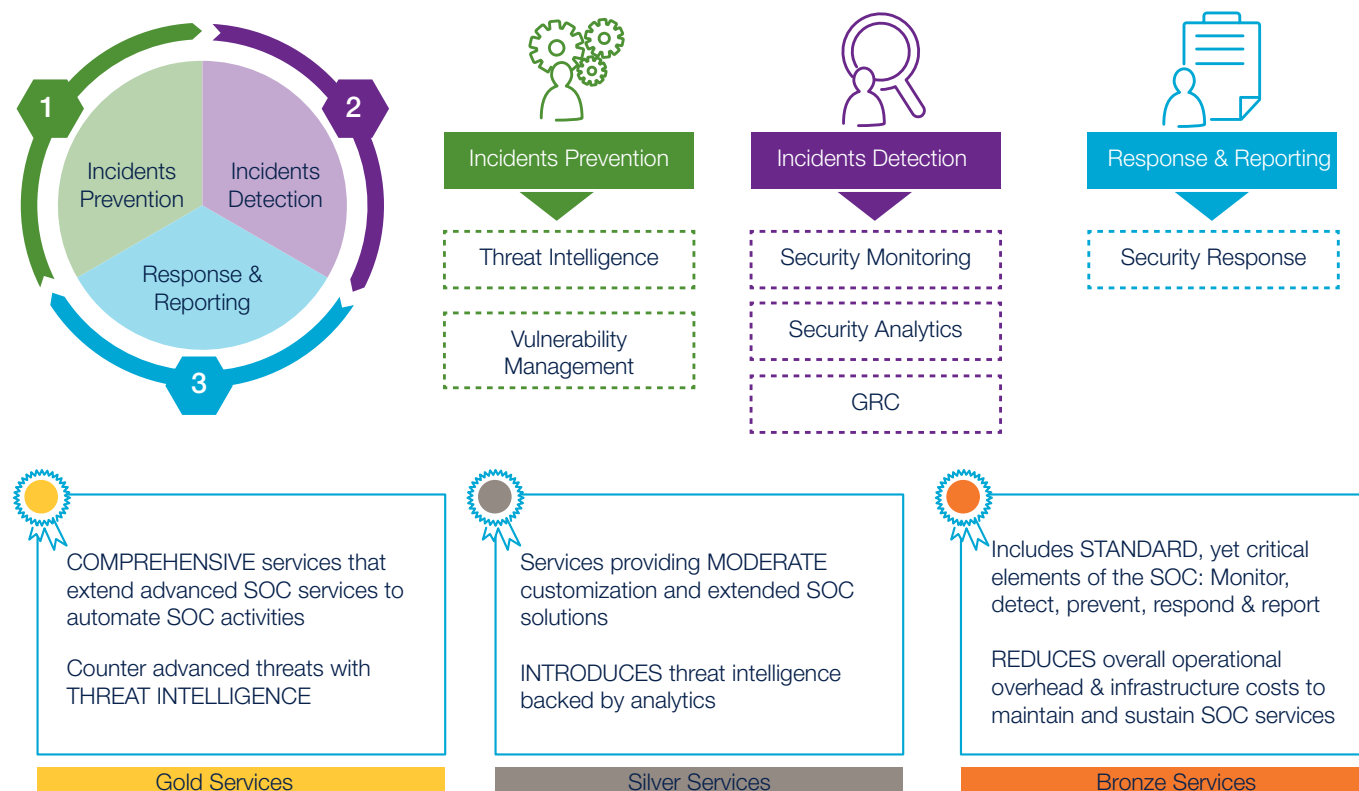
# Discover Managed SOC from Capgemini and IBM

Managed SOC from Capgemini and IBM serves highly scalable end-to-end managed cybersecurity services through a proven, integrated solution that delivers incident prevention, incident detection and response and reporting. Leaving no stone unturned, Managed SOC uses intelligence from multiple sources to uncover new and previously undetected threats while maintaining effective 360° monitoring and protection. Built-in reporting promotes open lines of communication with technical teams and business stakeholders, with systematic follow up in the case of threats being detected.

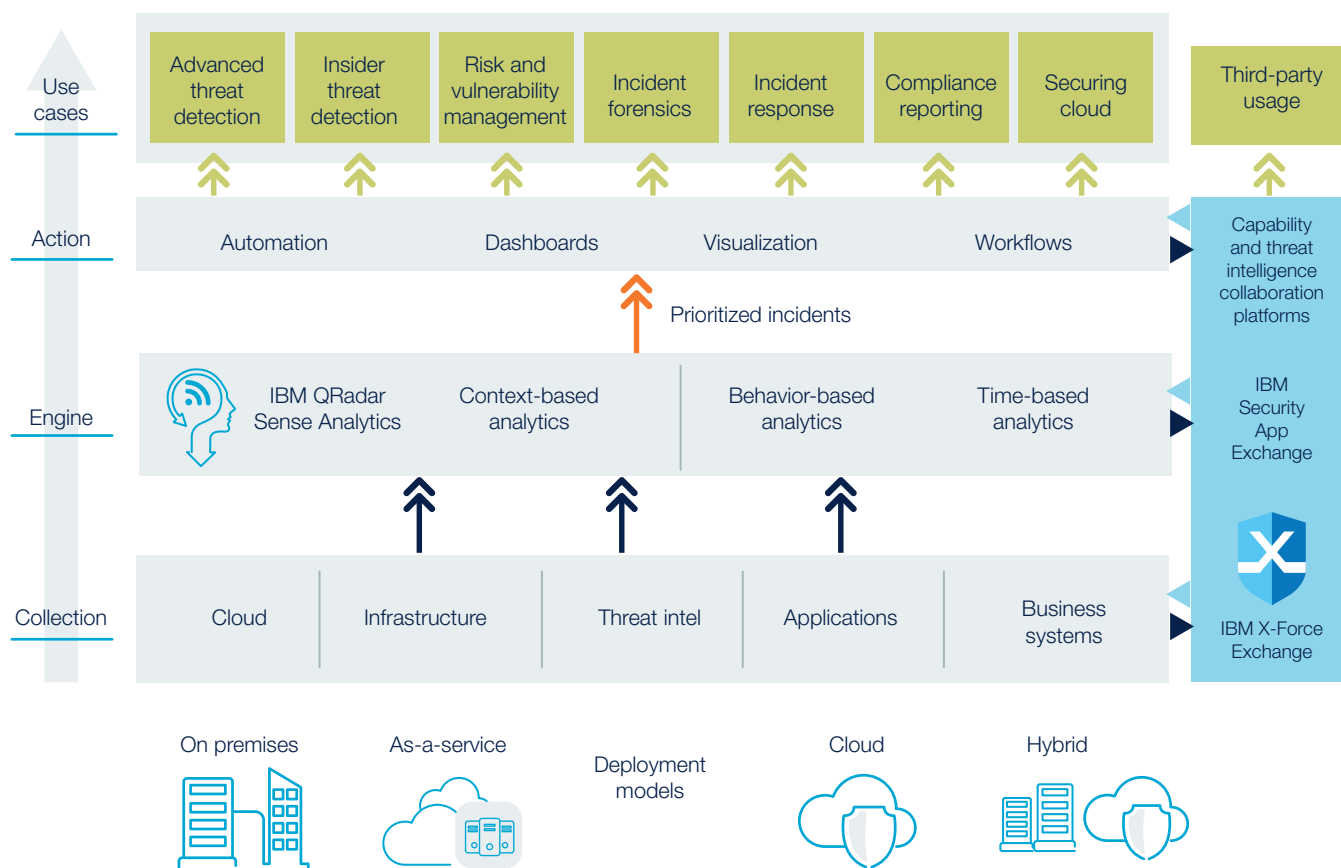
## Powerful computing at the core

QRadar is embedded in the Multi-tenant Managed SOC technology layer at all service levels and supports hundreds of third party software products, meaning that it can adapt to your organization's unique technology landscape. QRadar delivers multiple security capabilities, spanning log management, security intelligence, network activity management, risk management, vulnerability management, network forensics and incident response.

## Managed SOC services – the way we do it



## IBM QRadar Security Intelligence Platform



## Flex it, scale it—your way

The flexible tiered scale of Managed SOC services offers enterprises the opportunity to swiftly establish a highly effective Security Operations Center, out of the box and at low TCO (total cost of ownership). Choose the service level that best suits your business needs and organizational risk profile, and scale up or down at any point if circumstances change.

“

Now more than ever, organizations need advanced behavioral analytics and built-in threat intelligence to detect and stop cyber attacks. QRadar from IBM adds a powerful computing layer to the organization's Security Operations Center to protect more effectively than it was previously possible.”

**Marc van Zadelhoff**  
General Manager, IBM Security






































































# Getting started with Managed SOC

## The right fit for you

Take your first step towards next-generation cybersecurity. We help organizations to identify and quantify their risk profile, enabling them to prioritize and manage threats to their business. Organizations can then select the Managed SOC service level that best fits their needs and deploy. Our Managed SOC offer ranges from standard services that cover the basics across monitoring, detection, prevention and response and reporting to enriched service levels that combine the basics with customized services, analytics-based threat intelligence and advanced SOC automation.

## Delivery that serves you

Managed SOC is backed by Capgemini’s global network of cybersecurity specialists and seven multi-client SOC’s offering remote client support and response. Our industrialized service delivery model uses unified and standardized SOC processes that can be repeated, enabling a low cost of entry and swift deployment.

Managed SOC: Flexible end-to-end integrated services					<div> Gold<div> Silver<div> Bronze</div></div></div>			Common Services
 Incidents Prevention	Threat Intelligence	<ul style="list-style-type: none"><li>Threat intelligence database &amp; feeds</li></ul>				<div> Incident and problem management</div> <div> Device change and configuration management</div> <div> Service &amp; dashboard reporting as defined</div> <div></div>		
		<ul style="list-style-type: none"><li>Threat detection (visibility of unusual patterns within the internal network + reports)</li></ul>						
	Vulnerability Management	<ul style="list-style-type: none"><li>Advanced threat detection (zero-day, malware, APTs etc) + reports</li></ul>						
		<ul style="list-style-type: none"><li>Passive vulnerability scans</li><li>Active vulnerability scans</li></ul>						
 Incidents Detection	Security Monitoring	<ul style="list-style-type: none"><li>Continuous security monitoring</li></ul>						
		<ul style="list-style-type: none"><li>Logs analysis &amp; correlation* (features vary based on service level)</li></ul>						
		<ul style="list-style-type: none"><li>Compliance use cases + reports</li></ul>						
	Security Analytics	<ul style="list-style-type: none"><li>Aggregated data in the analytics engine</li><li>Malware analysis (sandbox): offline &amp; online + reports</li></ul>						
		<ul style="list-style-type: none"><li>User behavior, apps &amp; DNS analysis + reports</li></ul>						
	GRC	<ul style="list-style-type: none"><li>Asset inventory</li><li>Business context / risk management</li><li>Link with IT (e.g. ITSM, CMDB)</li></ul>						
								
 Response & Reporting	Security Response	<ul style="list-style-type: none"><li>Incidents management</li><li>Root cause, follow-up to problem/change management</li></ul>						
		<ul style="list-style-type: none"><li>Technical reports and dashboards* (features vary based on service level)</li></ul>						
								
								
								
								
								
								

# The future of enterprise security is within your reach

## Bringing tangible value

- Intelligence-based threat detection
- End-to-end security service plans that fit your organization
- Decrease CapEx with multi-client set-up
- Customizable and scalable
- Deploy faster with multi-client set-up
- Always-on support from our global SOC network



**Capgemini enables organizations to embed security at the beginning of their digital transformation journey, covering the cybersecurity spectrum from the infrastructure and endpoints right through to the protection of applications, users and data.”**

**Franck Greverie**

Global Cloud & Cybersecurity Lead at Capgemini

## A secure track record

Capgemini's established capabilities in cybersecurity are demonstrated through our Cybersecurity Global Practice, bringing together over 2,500 skilled specialists from consultants and architects through to R&D specialists and ethical hackers. Our deep experience is founded upon years of cybersecurity work with both public sector and private sector organizations around the world.

## Take the next step

The prevalence of sophisticated cyber attacks suggests that every organization will almost certainly be targeted more than once in the coming 12 months. Immunity is not an option, but protection is. In the age of data, always-on connectivity and increased mobility, it's time for organizations to ensure their cybersecurity measures are up to the task.

The next generation of enterprise security is ready—and can be up and running in your organization soon. It's time to get back in the driving seat with advanced enterprise security that's ready for anything.

**Contact us today to find out how you can safeguard your organization against the most advanced of cyber attacks—within days.**

**Geert van der Linden**

geert.vander.linden@capgemini.com

**Bill Millar**

bill.millar@capgemini.com

**Vincent Laurens**

vincent.laurens@sogeti.lu

## About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit [www.ibm.com/security](http://www.ibm.com/security), follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.



## 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 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, seven security operations centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

Find out more:

[www.capgemini.com/cybersecurity](http://www.capgemini.com/cybersecurity) or [www.sogeti.com/cybersecurity](http://www.sogeti.com/cybersecurity)