



Cyber Attack Simulation Services

The future of enterprise security is here



The cyber threat landscape is growing more complex

No place to hide

While technology's increasing sophistication brings opportunity to unlock business value, it also brings a growing security threat. Cyber-attacks are becoming not only more advanced and audacious, but also more varied from stealing intellectual property to writing malicious code to lodge 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 that 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

The 2018 report¹ into the cost of data breaches—just one of many possible outcomes of a cyber-attack—found that for the cross-section of 477 companies interviewed, the average total cost of a data breach in 2017 was \$3.86 million, or \$148 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 Capgemini partners with IBM to offer a new generation of intelligence-driven Managed Security Operations Center (SOC) services. Underpinned by the market leading QRadar Security Intelligence Platform from IBM, it puts control of the enterprise security back into your hands.

Malicious attacks can take an average of 101 days to identify
(M-Trends2018 Report, Mandiant Consulting)

Capgemini's Cyber Attack Simulation: Protecting against advanced attacks

Attack Simulation Services

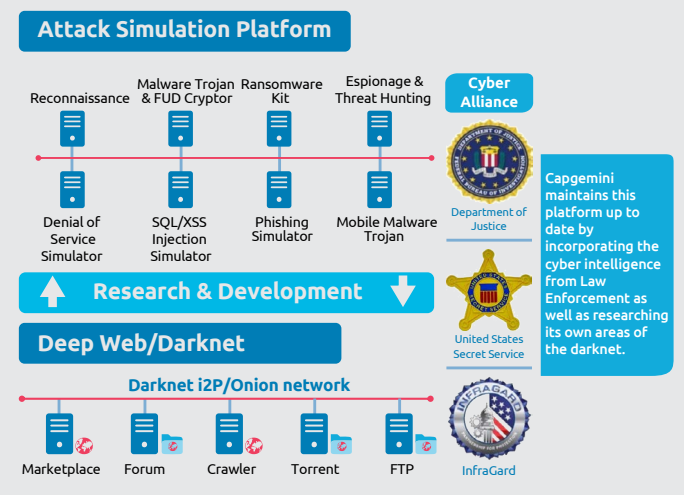
Simply put, Attack Simulation begins where other security testing programs end by taking a hacker view of your target organization. By utilizing years of experience in cyber-attack tools and methodologies, identifies security flaws not detectable to the client organization. The advantage of the simulation is the ability to see the systemic effect that each identified gap or weakness has on other security controls around it and across the enterprise.

Another advantage of incorporating attack simulation into the process is that by loading the Attack Simulation model with current industry data loss values, the assessment process will identify and predict realistic financial losses customers will face from cyber-attacks against their organization.



- The hacker's view on your security posture
- Attack planned and executed the way a hacker would without causing the related damage to your enterprise
- A detailed report of all vulnerabilities and gaps found
- A clear report of next steps and remediations

Capgemini adopts a Hacker's view 'outside-in', coupled with an in-depth view of enterprise security 'inside-out'



Attack Simulation Platform

Capgemini's attack simulation exercise will test the attack surfaces of our client's external facing perimeter. Capgemini's well-refined methodologies span multiple technologies and security control areas, from personnel and procedural security controls, to system and application level penetration. The aim of the simulation is to provide insight into our customer environment from the point of view of an attacker, and to provide that external non-biased view of your estate.

Attack Simulation: Attack Types



Capgemini's approach goes beyond traditional penetration testing, which often excludes the very tactics, assets, or locations most valuable to attackers. Capgemini uses information that is open source and available publicly to understand an attacker's point of view. This enables Capgemini to quickly identify the security gaps in how an organization's most valued assets are being protected.

Benefits

The more you know about the threat's your organization faces, the less vulnerable you are to increasingly sophisticated cyber attacks. Capgemini gives you that knowledge. Our Cyber Attack Simulation exercise simulates phishing, malware compiling & binding, DDOS multi-layer, SQL injection, crime kits and other exploits to give the CISO/CFO/CEO the insights needed to strengthen the security strategy moving forward into digital transformation. A Cyber Attack Simulation exposes both known and unknown vulnerabilities by putting enterprise defenses under the same duress as in the real and evolving threat landscape. Our state-of-the-art Security Operations Centers(SOCs) bring together the combined expertise of our thousands of security professionals and a set of proven, certified processes and technologies to give you complete visibility into your security posture.

- The IT Security posture impacts the reputation of an enterprise in many ways from compliance and visible investment to damage after real attacks
- A realistic "hacker's view" on security
- Cyber Attack simulation provides insights into the Security "unknown unknowns" of digital enterprise
- Insight into preparedness and resilience
- Focus and direction for improvements

Cyber Attack Simulation gives the CXO the insight needed to strengthen their security strategy moving forward

The future of enterprise security is within your reach

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.

¹2018 Cost of a Data Breach Study: Global Overview Benchmark research sponsored by IBM Security | Independently conducted by Ponemon Institute LLC | July 2018



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

This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.
Copyright © 2019 Capgemini. All rights reserved.

For further information please contact:
infra.global@capgemini.com