Financial Sector

Security Operations Center Transformation

Capgemini helped one of the world's leading financial institutions establish a leading Security Operations Center (SOC) capability on an aggressive deployment schedule.

THE CLIENT

Global financial services firm providing financial service products to hundreds of millions of individual and institutional customers worldwide, with more than a trillion dollars in assets under management.

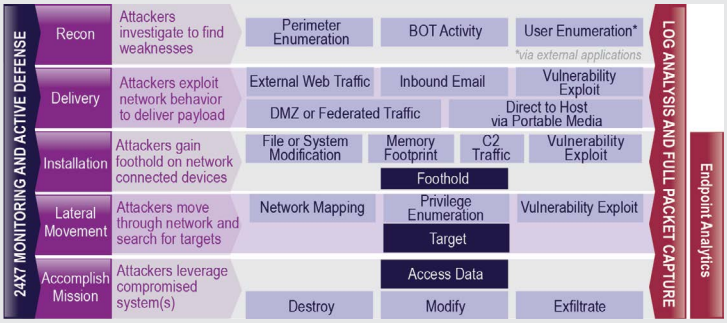
THE CHALLENGE

The client found that its cyber defenses were being challenged by increasingly advanced cyber-attacks. Its Board of Directors required a SOC be built and operational within 12 months, modeled on leading industry cyber operations centers.

CAPGEMINI APPROACH

Capgemini approached this challenge leveraging its decades of experience battling advanced attacks and also using intrusion kill chain methodology. This methodology was used to develop use cases for the client's cybersecurity needs, which then were used to drive the rest of the SOC development program. This program included the following:

- Working with risk management to establish SOC governance
- Managed Detection and Response (MDR) defense capabilities
- SOC operations processes, procedures, metrics, and Key Performance Indicators (KPIs)
- Training for SOC analysts, managers, and Incident Response Teams, including forensics tools and investigations
- Threat intelligence and threat hunting proofs of concepts
- Use cases and playbooks for cyber operations and incident response
- Visibility and monitoring within cloud computing environments



IMPACT OF THE SOLUTION

The client was able to drive immediate improvements to its cyber defense posture, using this new SOC capability. This capability leveraged our approach over decades of experience operating its own Managed Security Service Provider (MSSP) service, along with first-hand experience combating advanced and nation-state attackers. Furthermore, the client was able to position itself to continue evolving its defenses long term against new and emerging cyber threats.

CYBER CASE STUDY

> "They are our **trusted advisor** and an extension to our entire cyber team ...they are all that they were built up to be."
>
> - Client Cyber Executive

About Capgemini

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.

Learn more about us at

www.capgemini.com/cybersecurity

People matter, results count.

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

Capgemini