# Cyber Solution for the Financial Sector

## The Challenge

Financial services, by definition, are a premium target for criminals and malefactors. Financial institutions operate large, mission scale networks that process endless volumes of sensitive information that put them in the crosshairs for cyber-attacks. Such attacks can cause significant loss of business intelligence and intellectual property, drive up security costs, disrupt workflow and harm the company's reputation.

The financial sector is known for innovation and for adapting new technologies to improve customer satisfaction and maintain a competitive edge. However, this innovation may inadvertently expose its systems to attacks. In order to protect themselves and fulfill their ethical and regulatory obligations to protect customers' assets and privacy, financial services companies require constant security improvement and advanced risk management strategies.



THREAT INTELLIGENCE

CYBER SERVICES

CYBER ANALYTICS SOLUTIONS

## Mer Solution - 360° Cyber Protection

Mer is offering a comprehensive solution that concentrates on the big picture and creates tailormade cyber security programs based on vast experience in cyber warfare & Intelligence. Our expert cyber-security team has developed a holistic comprehensive cyber strategy, addressing multiple threats within the financial sector, such as:

- Insider Threats
- Denial of Service Attacks
- Account Takeovers
- Securities and Market Trading Breaches
- Third-Party-Payment Processor Breaches

- Supply Chain Infiltration
- Mobile Banking Breaches
- Payment Card Skimming
- CryptoLocker attacks (also known as "Ransomware")

In order to counter these threats, Mer has developed a strategic portfolio of complementary services to reinforce the organization's security posture and bring it to the forefront of current technology and knowledge.

## Cyber Threat Intelligence – Taking the Initiative

Threat Intelligence helps financial institutions identify and concentrate on real world individuals or groups that are actively trying to undermine them. Mer's multi-lingual team of experts gathers contextual information from open sources and the DarkNet to create a comprehensive review of real life adversaries, their motivations and intended actions. The result is a detailed and prioritized report about existing and potential cyber threats together with recommendations for mitigation.

Mer offers a unique portfolio of services, empowering customers to define the package that optimally fits their specific needs and interests. Mer expert team delivers clear reports, which may include the following components:

- Threat Actors: contextual information on adversaries such as organized crime and activists, their motivations and intents.
- Intelligence about significant threats and attacks within the financial sector.
- Published vulnerabilities and exposures.
- List of malicious indicators for blacklisting, e.g. IP addresses, malware, DDoS infrastructure and more.
- Actionable advice on mitigating the threats.

## Professional Cyber Services – The Human Advantage

A comprehensive package of services that will take the organization from planning to implementing an effective cyber security program.

- **Risk Assessment** - a comprehensive review of the company's security level, listing vulnerabilities and mitigation recommendations.
- **Cyber Security Plan** - A detailed, actionable and optimized cyber security and business continuity plan based on the completed risk assessment.
- **Incident Response Support** - Emergency expert service available 24/7 to handle any case of breach or attack, in order to limit damages and reduce recovery time and costs.
- **Training and Mentoring** - Flexible cyber security training programs from general awareness to advanced cyber security skills.
- **Cyber Security Operations Center (CSOC)** - Establishing on behalf of the customer top of the line intelligence-driven cyber security operation center that monitors the organization's security posture at all times and ensures centralized alerting and investigation. This allows the organization to proactively anticipate threats and breaches and respond accordingly.

## Why Mer?

- Proven track record across the globe in cyber security and complex large scale projects that require a high level of expertise.
- Vast experience in cyber warfare & Intelligence.
- A single, accountable provider responsible for seamless implementation and operation.
- Integration expertise with a diversified portfolio of providers and subsidiaries.
- Local operations around the world for better support and rapid response.
- An innovative company with stable and dependable operations.