MER Cyber Solution for the Telecommunication Industry

The Challenge

The telecommunication industry is a prime target for cyber attacks from diverse sources. Telecom companies store valuable information about their customers, billing data and usage records that are sought after by foreign nation states, terrorists, hacktivists, and commercial companies looking for business intelligence.

Furthermore, the communications services provided by telecom companies form a critical infrastructure that serves millions of people, first responders and homeland security services. Damage to this infrastructure will affect daily life, business operations and may even put lives in danger. A successful attack may also seriously harm the company's reputation and raise serious concerns about customer privacy.

Therefore, the telecom industry requires a comprehensive cyber security strategy that brings together highly trained personnel, up-to-date technological solutions and the right tools and capabilities to detect, analyze and respond to threats.

The MER Solution - 360° Cyber Protection

MER Cyber and Intelligence team has developed a dedicated comprehensive solution for the telecommunication sector, based on thorough experience in cyber warfare and Intelligence. The solution focuses on the specific cyber threats relevant for the telecom sector, including:

- Application security
- Third-Party suppliers and vendors
- Insider Threats
- Denial of Service Attacks
- CryptoLocker attacks (also known as "Ransomware")

Cyber Threat Intelligence – Taking the Initiative

The security paradigm is changing from reaction to breaches as they happen, to a pro-active approach that collects intelligence on possible threats to keep one step ahead of hackers and malefactors.

According to a new Kaspersky lab intelligence report about the security threats facing the telecommunication industry, cybercriminals are recruiting disaffected employees or blackmailing staff through underground channels to gain access to networks and subscriber data. This combined external-internal mode of operation is impossible to stop without prior intelligence about those criminal intents.

MER's multi-lingual team of experts gathers contextual information from open sources and the Dark Net 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 will provide the organization with a tailor-made report according to its specific needs which may include:

- Threat Actors: contextual information on adversaries such as organized crime and hacktivists, their motivations and intents.
- Intelligence about significant threats and attacks within the telecommunications 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 Services – The Human Advantage

MER works with internet and telecom providers to define the important assets they need to protect. Based on this definition of scope, MER provides the customer with a versatile package of services that will enable the organization to effectively counter relevant risks.

- **Risk Assessment** - A comprehensive review of the company's security level, resulting in a detailed report of 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 and ensures centralized alerting and investigation.

Orchestrating Cyber Solutions

Cyber-attacks have become ever more frequent, targeted and sophisticated. Millions of warnings are produced by platforms, applications and numerous point solutions, making it almost impossible to uncover information that truly indicates a potential for real attack.

Current technology offers a wealth of cyber security products with various purposes and capabilities to counter cyber challenges. The MER team is constantly monitoring the market to find the best offerings at the forefront of security knowledge about defense capabilities. These are being used in integrated solutions that deliver a high ROI through an emphasis on analytical cyber products, which allows cyber specialists to address the main issues and real threats.

In order to implement a security operation that will best suit the customer's cyber security needs, the MER team surveys existing defenses, replaces and upgrades existing products and adding an analytical layer. MER also provides tailored professional training to ensure a seamless operation of the organizational cyber security solution.

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

MER Group
5th Hatzoref St., Holon 58856, Israel | T+972-3-5572555 | F+972-3-5580282 | www.mer-group.com | info@mer-group.com