LEONARDO CYBER & SECURITY SOLUTIONS

MANAGED SECURITY SERVICES

LEONARDO

Cyber-attacks are exponentially growing in terms of involved subjects, reasons, strategies and methodologies increasing the asymmetry between attackers and victims. Attackers are more and more often organized groups that conduct large scale, territorial and target independent actions aiming to maximize profit.
Technological investments in protection tools are in many cases not very effective in defending the corporate perimeter as they are often not focused on minimizing the real risks to which the organization is exposed.
The rapid evolution of threats and the lack of skilled resources make this scenario even worse.
Another critical problem is represented by the response times to cyber incidents, almost always too long in a fast-paced world, generally much more than security departments.

In this scenario, partnering with a Managed Security Service Provider (MSSP) can be enormously helpful to empower enterprises' and organizations' cyber resilience in terms of people, processes and technology.
MSSPs offer a superior protection as they leverage on experience gained from managing cyber security issues for a large number of companies operating across different industries.
In addition, they allow businesses both to employ up-to-date cybersecurity tools, technologies and capabilities with predictable, ongoing operational costs and to focus executives and employees onto core business needs.

LEONARDO MANAGED SECURITY SERVICES

Leonardo provides intelligence-driven managed security services designed to configure and continuously monitor Customers' systems, promptly identify breaches in security policies and apply immediate and appropriate remediation actions.
Close collaborations with top security players, universities, supranational organizations and research centres as well as the experiences gained in various market sectors, including **Defence and Critical National Infrastructures**, enable us to develop solutions tailored on Customers' needs that combine advanced technology with skilled resources to manage cyber risks and prevent cyber threats.

THE NEXT GENERATION SECURITY OPERATION CENTER

Leonardo's **Next Generation Security Operation Centre (Next Gen SOC)** provides managed security services 24x7x365 in order to improve the cyber awareness and resilience of our Customers. It is organized in five operational units:

- **Front End** receives intervention requests from customers, manages trouble ticketing process, provides basic support or sends the most complex requests to the other operating units.
- **Security System & Device Management** configures and manages security systems and devices of Customers.
- **Real Time Monitoring & Analysis** monitors in real time the Customer's security infrastructure, correlates the detected events to identify anomalies, unauthorized access attempts and cyber-attacks being launched.
- **Computer Security Incident Response Team** provides ex post analysis and incidents' remediation and prevention activities including malware analysis, vulnerability identification and resolution, digital forensics.
- **Threat Intelligence** monitors open sources in real time to predict and prevent cyber threats and to support the identification of cyber-attacks, their sponsors and their motivations.

Threat Intelligence Services are based on 500 TFlops High Performance Computing resources enabling analysts to collect, correlate and analyse huge amount of data.

APPROACH AND SKILLS

Leonardo's approach to managed security is based on the native integration of threat intelligence services, aimed at predicting and preventing cyber threats, with services designed to proactively detect security incidents and with activities aimed at the remediation and prevention of cybernetic attacks.

- **Prediction:** open and multiple sources, including deep and dark web, are continuously monitored and analysed to predict and prevent cyber-attacks taking advantage of customer's IT/OT vulnerabilities and detect proprietary information illegally stolen and published on the web.
- **Proaction:** the information gathered by the continuous monitoring of the client's infrastructures and acquired by intelligence activities, allows the timely identification of security policies' violations and address the configuration of IT/OT systems reducing the risk of cyber-attacks or interruption of the operations.
- **Reaction:** once a cyber-attack has been detected, Leonardo's Computer Security Incident Response Team (CSIRT) is immediately involved to limit the operational and economic impacts of the security incident as effectively as possible by defining and implementing the best incident response strategy.
- **Prevention:** preventive services are aimed at verifying the customers' security posture identifying and managing any vulnerabilities before an attack occurs.

PREDICTIVE SERVICES

- **Cyber Threat Intelligence:** services designed to detect new vulnerabilities, cyber-attacks being prepared and proprietary information or sensitive data illegally stolen and posted on the Internet.
- **Social and Security Threat Intelligence:** services aimed at offering a complete overview of the online sentiment related to events or topics of interest improving the awareness of imminent potential threats against the customers' assets.
- **Fraud Detection Threat Intelligence:** services designed to prevent internet frauds realized through phishing campaigns, domain hijacking and theft of digital identities, support attackers identification and protect customers' digital frauds.

PROACTIVE SERVICES

- **Security Device Management:** services designed to manage customers' security infrastructures, in terms of systems' configuration and maintenance such as firewalls (FW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), etc.
- **Security System Management:** managed security services aimed at commissioning, managing and maintaining security applications in terms of configuration and maintenance of systems such as Antivirus, SIEM, Identity Access Management (IAM), etc.
- **Real Time Security Monitoring:** the service is aimed at the continuous monitoring and analysis of security reports provided by the correlation of the logs generated by the Customer's equipments/systems in order to quickly identify potentially harmful events, anticipating attack attempts as much as possible.

PREVENTIVE & REACTIVE SERVICES

- **Offensive Security Services:** focused on finding security flaws that can be exploited by malicious attacks, these services aim to test in advance the measures already adopted by enterprises and organizations. Offensive security activities can be carried out periodically, as vulnerability management, or on demand such as vulnerability assessment and penetration testing.
- **Incident Response:** services aimed to the best cyber incidents strategy management. Through a careful in-depth analysis of Customer's systems, these services identify and respond to the cyber threat, in order to limit its impacts on assets and business processes.

ARTIFICIAL INTELLIGENCE AND SOC PROCESS AUTOMATION

Artificial Intelligence supports the activities of Leonardo's Next Gen SOC analysts, contributing to augment their analytical skills.
The predictive services provided by Leonardo employ AI techniques to support intelligence analysts' activities in order to identify attack patterns for which there is no direct evidence through the correlation and integration of available information. In addition, AI-based virtual assistants automate escalation procedures further reducing response times.
Advanced Security Orchestration, Automation and Response (SOAR) systems further increase Leonardo's response and efficiency levels, as it unburdens analysts of manual and low level tasks and allowing them to focus on more complex and value-added activities.

LEONARDO'S OFFER PORTFOLIO

Leonardo protects Governments, National Critical Infrastructures and National Strategic Industries against cyber threats and attacks using its technology and experience in cutting-edge cyber security and critical IT systems, all crucial for the operation and service continuity for citizens and countries.
Organized into two different lines Business-driven Cyber Security and Critical Information Systems, Leonardo's Portfolio leverages the main emerging technologies and the most up to date technological paradigms to offer solutions, platforms and services able to support customers' secure digital transformation.
The Managed Security Services are part of the Business-driven cyber security offer, including:

- **Cyber Protection & Resilience** for governments and critical infrastructures through services, tools and methodologies for the management of the entire threat life cycle and for the resilience of systems and services against cyber-attacks.
- **Intelligence & Investigation** in order to support Law Enforcement Agencies, Blue Lights e and Defence in the research, the collection and the analysis of relevant information for investigation activities, strategic intelligence and preventing crime.
- **Cyber Training** for the creation and simulation of complex cyber-warfare scenarios aiming at training analyst in charge of IT/OT system security, both in the civil and military sector.

BENEFITS

- Unrivalled cyber protection leveraging on experience gained from managing cyber security issues for a large number of companies operating across different industries including Critical National Infrastructures and Defence.
- Services based on leading-edge technologies including artificial intelligence, machine learning and natively integrated with threat intelligence.
- Extensive Cybersecurity Knowledge thanks a team of cyber security experts with the top international certifications in information security guaranteeing the highest international standards for privacy, integrity and availability of data.
- Significant cost reduction and extended efficiency thanks to the adoption of the "as a service" model, externalising the acquisition of both infrastructures and specialized skills.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber and Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM09027 06-22