CYBER SECURITY OPERATION CENTER

Reply's new Cyber Security Operation Centre is a structure specialised in the provision of Premium-level security services, tailored to the customer's needs, processes, and the specific threats characteristic of the sector in which it operates.

Communication Valley Reply's Cyber Security Operation Centre, created to meet the security needs of banks and financial institutions, makes its assets and expertise available to companies operating in equally complex environments including the Retail, Manufacturing and Utilities sectors.

SECURE YOUR BUSINESS

24 HOURS A DAY, 365 DAYS A YEAR

CYBER SECURITY OPERATION CENTER

The Cyber Security Operation Centre is a veritable "watchtower" manned 24 x 7 x 365 days a year by a team of Security Analysts, System Engineers, Security Testers and Malware Specialists.
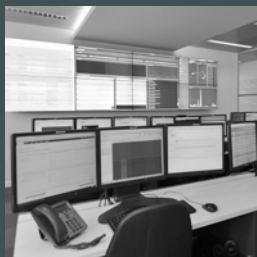
The services offered by the Cyber Security Operation Centre (CSOC) rely on a new security monitoring model based on a first level of highly specialised analysts. From the very first service level, the model reduces reaction times and speeds up the implementation of the necessary countermeasures.

Preventive detection and real time management of security incidents are factors of primary importance for ensuring an adequate level of network, data and services protection for businesses.
The Cyber Security Operation Centre is a space where a team of experts carries out real time monitoring, security assessments and security device management, relying on leading-edge technologies.

THE SERVICES

PROACTIVELY DETECT ATTACKS AND CYBER THREATS

CYBER SECURITY MANAGEMENT

1

FRAUD MANAGEMENT

2

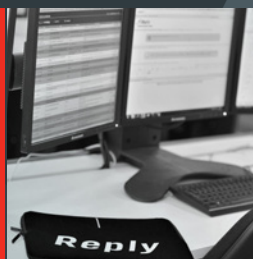DETECT AND MANAGE FRAUDS ACROSS ALL CHANNELS

GUARANTEE SECURE AND EFFICIENT ACCESS TO CORPORATE APPLICATIONS AND DATA ANYTIME AND EVERYWHERE

ENTERPRISE MOBILITY SERVICES

4

MANAGED NETWORK SECURITY

3

SHARE THE RESPONSIBILITY OF KEEPING YOUR NETWORK MANAGED AND SECURE

CYBER SECURITY MANAGEMENT

Cyber Security Management services are designed to guarantee the customer's "core" security management activities. In particular, the Security Monitoring service is the primary tool for detecting and managing security incidents.

This service is based on the collection and correlation of events related to the customer's infrastructure, applications and systems. All the information is collected by the Advanced Security Analytics platform, which facilitates the analysis of events gathered from heterogeneous sources and from different customers.

Based on this approach, the CSOC maximises the ability to identify even the most sophisticated forms of attacks, while ensuring, through the logical separation of data and information relating to different clients, the highest level of privacy.

The same platform is used by System Engineers and by Malware Specialists to provide vertical services such as: Cyber Threat Intelligence, Breach Detection and Domain Monitoring.

CYBER SECURITY MANAGEMENT **1**	SECURITY TESTING ASSESSMENT SERVICES SYSTEM SECURITY POLICY **1,1**	SECURITY DEVICE MANAGEMENT STRONG AUTHENTICATION **1,2**	CYBER THREAT INTELLIGENCE CREDENTIAL / CREDIT CARD MONITORING BREACH DETECTION & EARLY WARNING DARK WEB THREAT MONITORING ANTI DEFACEMENT & DOMAIN MONITORING **1,3**	LOG MANAGEMENT SECURITY MONITORING SIEM MANAGEMENT & CONFIGURATION **1,4**

FRAUD MANAGEMENT

With the widespread use of online and multichannel services, there has been a corresponding increase in fraudulent activity, in terms of both volume and complexity.
These activities are generally aimed at identity and credential theft or the acquisition of other information useful for committing fraud.

CSOC's **Fraud Management** services focus on the identification and analysis of Malware for different types of devices, on the detection and shutdown of clone sites used to conduct phishing campaigns, on the

analysis of fraudulent financial transactions and, in the event of complex fraud scenarios, on security incident investigations including forensic analysis.

The CSOC offers technologies and applications that facilitate the detection of fraud, thanks to analysis and the identification of abnormal behaviour within browsing sessions.

FRAUD MANAGEMENT **2**	ACTIVE FRAUD PREVENTION AND MALWARE INTELLIGENCE **2,1**	MOBILE ROGUE APPLICATION HUNTER **2,2**	ANTIPHISHING SERVICES **2,3**	BRAND ABUSE MONITORING SOCIAL MEDIA THREAT MONITORING **2,4**

MANAGED NETWORK SECURITY

Managed Network Security services are designed to support the unified management of network infrastructure, harmonising access and management systems for service devices operating across CSOC's various customers.

A single management console allows System Engineers to take action in an organised and structured manner, both with regard to incident management, as well as in relation to ordinary and extraordinary management, including patching, tuning and change activities.

The distinctive elements characterising the Centre's infrastructure are:
• Flexibility in managing the different technologies used by our customers.
• Standardisation and sharing of methods for accessing and managing systems.
• Security and compartmental structuring, both with regard to customer environments, as well as CSOC's infrastructure.
• Diligent configuration management, with appropriate storage, backups and versioning. High level of reliability and redundancy.

MANAGED NETWORK SECURITY 3	SECURE NETWORK DESIGN AND IMPLEMENTATION 3,1	NETWORKING REMOTE & ON-SITE SUPPORT SERVICES 3,2	DEVICE & SOFTWARE SUPPLY AND SUPPORT 3,3	NETWORK ENGINEER SUPPORT NOC & COMPLEX NETWORK CONSULTING 3,4

ENTERPRISE MOBILITY SERVICES

The incremental use of mobile devices and related content has fuelled the need for enterprise-specific tools and services aimed at the regulation of mobile applications and associated security.

Today, the growing adoption of personal devices within business contexts (Bring Your Own Device) represents an opportunity for companies, and at the same time, a risk. The CSOC is able to support the customer in developing a strategy designed to maximise the benefits of the BYOD model, without overlooking the necessary adherence to security policies. End User Computing services are used to monitor and manage

workstations, mobile applications and their security, ensuring a specialised contribution for customers based on 8 x 5 or 24 x 7 service models, depending on individual requirements.

CSOC's **Enterprise Mobility Services** support customers in the management of devices and mobile applications, to ensure full compatibility with Mobile Device Management platforms and adherence to core security principles.
The CSOC supports the customer both in the development of secure business applications, as well as in "securing" third party applications.

ENTERPRISE MOBILITY SERVICES 4	END USER COMPUTING 4,1	DEVICE MANAGEMENT 4,2	MOBILE APPLICATION SECURITY 4,3	IDENTITY & SECURITY MANAGEMENT 4,4

REPLY COMMUNICATION VALLEY

COMMUNICATION VALLEY REPLY Communication Valley Reply is the Reply Group company that specialises in providing managed security services. Through its Cyber Security Operation Center – an ISO27001-certified European centre of expertise in the managed security services sector that operates on a 24/7 basis, 365 days per year – the company ensures business continuity and fraud prevention for companies with regard to threat intelligence, fraud detection and management, security monitoring and testing, and managed network security. With more than 15 years of experience, Communication Valley Reply provides specialised services for the finance sector in the identification and analysis of malware, in the detection of websites created for conducting special phishing campaigns, and in the analysis of fraudulent, often highly complex transactions, including forensic analyses.

CYBER SECURITY OPERATION CENTER
Via Robert Koch 1/4, Torre B,
20152 Milano, Italy

COMMUNICATION VALLEY REPLY

ITALY	**GERMANY**	**UK**
Via Robert Koch 1/4, Torre B,	Arnulfstraße 27,	38 Grosvenor Gardens London,
20152 Milano, Italy	80335 München, Germany	SW1W 0EB, United Kingdom

www.communicationvalley.com
csoc@reply.com