SECURITY OPERATION CENTER

The Security Operation Center is the place where the trust relationship between Communication Valley and Customer takes place. It is characterized by competences, updates, continuous training and experience. Here, the evolution contributions of each project make up the common Knowledge Base used to produce synergy.

SECURITY OPERATION CENTER (SOC)

The Security Operation Center (SOC) of Communication Valley is a physical and logical structure –the only one in Italy- specialized in providing managed and professional services in the field of IT security. It works for many organizations and is a competence center with more than hundred certifications. It is a real "control tower", guarded 24 hours per day for 365 days per year by a security team composed of analysts, system engineers and testers who specialize respectively in real time monitoring, security device management and security assessment activities. The SOC uses an exclusive infrastructure (Enterprise Security Management), composed of a set of different applications, for security issue management, attack pattern detection, technology maintenance and Knowledge and Asset Management. The SOC interacts with the customer and shares with him the service output through an easy web-based portal which is also rich in contents. The SOC is used to provide the main IT security services which made up the Communication Valley offer.

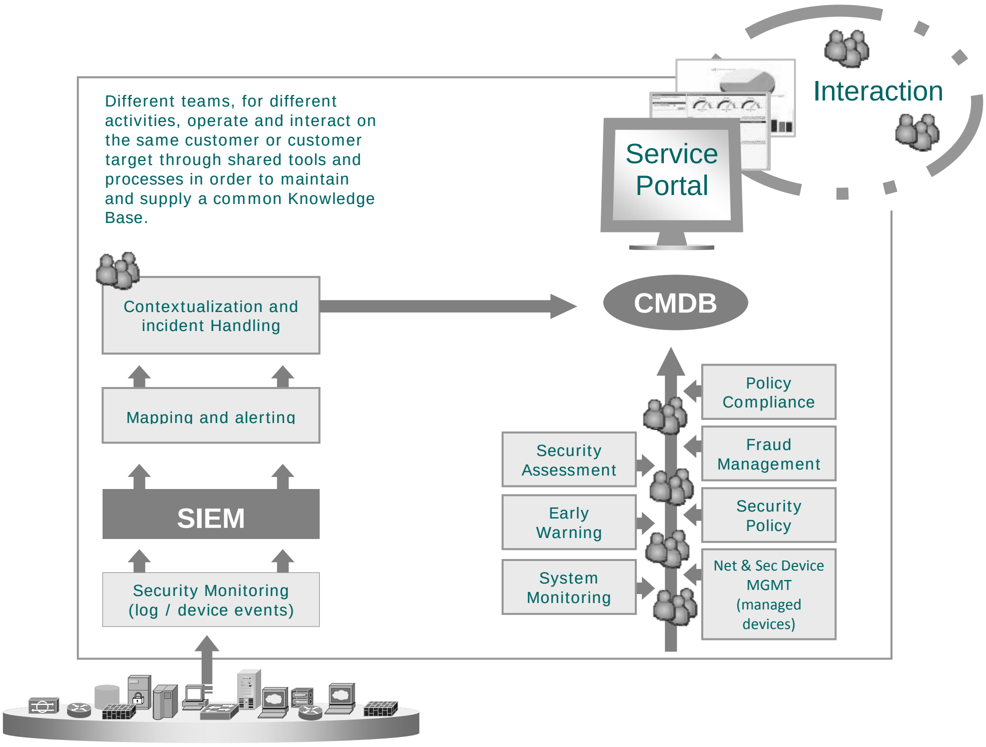
SECURITY MONITORING. The present complexity level of IT systems –determined by the wide use of different interconnected technologies (wireless, VoIP, terrestrial digital technology for TLC, palmtops)- involves the production of many information (log) that must be read, interpreted, managed and maintained. The Monitoring service of Communication Valley acts within control and anomaly detection activities on the networks by detecting, mapping and interpreting the logs generated by any individual component of the network infrastructure being monitored.

The service includes two main components, as follows.

Technological component. It is composed of a SIEM (Security Information and Event Management) platform engineered and implemented with the aim of centralizing log archiving and management and to make these information available for the Security Team. For this purpose, all the information generated by the devices are sent, collected and centralized. A further engine stores the information and makes them available for the Security Team for analysis, mapping, report generation and emergency management, according to defined and signed modes and guarantees.

Analysis component. A fundamental component of the Monitoring service is the analysis of collected data carried out by the analysts working in the Security Operations Center (SOC) of Communication Valley. This activity is not only limited to the activities previous to alarm notifications, real time responses, report preparation and so on; it also includes the implementation of rules, procedures and solutions and the identification, evaluation and suggestion of remedies deemed as both necessary and urgent. This is a value-added activity since it is carried out by highly qualified analysts with acknowledged and certified competences who are in charge of both the preparation and the management of complex security projects.

The distinctiveness of Communication Valley lies in the global approach to the security issue, an approach which integrates in the monitored perimeter the knowledge synergies acquired through heterogeneous services and realities.


Different teams, for different activities, operate and interact on the same customer or customer target through shared tools and processes in order to maintain and supply a common Knowledge Base.

Security Monitoring

NETWORK AND SECURITY DEVICE MANAGEMENT. The Network and Security Device Management handles the operative management of the elements concerning a specific network infrastructure (firewall, IDS, VPN, concentrator, proxy, AAA systems, URL filtering, router, Switch, and so on). The SOC infrastructure –used for device management- has been implemented with the aim of institutionalizing the access and management methods for the service devices operating on the different Communication Valley customers. Using a single management console, the Communication Valley SOC system experts deal in a structured way with all different activities (ordinary maintenance, change, fault management, patching, tuning and so on). The infrastructure has been designed by taking into consideration the following elements: the flexibility for the management of different technologies for different customers; access and management operative methods shared by SOC system experts; isolation and security of different context and SOC network; backup, versioning and maintenance of configurations; high reliability and redundancy.

The following list is a summary of the activities carried out by the Network and Security Device Management service.

- Ordinary management: recommendations, system upgrade and patching due to newly detected vulnerabilities; execution of recursive and agreed operative procedures; system signature update.
- Problem solving: hw, sw and configuration maintenance interventions also concerning security aspects; cooperation with customer's application, system and network administrators; anomaly solving (system and security related).
- Corrective maintenance: planning and execution of ordinary and extraordinary maintenance interventions with corrective actions aimed at increasing and improving the security levels of the managed infrastructure.
- Evolutive maintenance: architecture change activity aimed at upgrading the managed plants (ex. Recommendations for architectural upgrades)
- Change Management: policy and configuration change according to agreed plans; introduction of new physical/logical devices into the infrastructure; user and group policy management.

The service time coverage is decided through SLAs which go from H8x5 Business Day to H24x365 (through availability). Also the interconnection method between the SOC of Communication Valley and the network to be monitored is agreed on. The connection can be made either through a dedicated line or through a simple VPN IPSec on institutional Internet lines.

In particular, for financial institutions, Communication Valley provides an additional module called **System Monitoring** aimed at real time monitoring H24x365dd of the main device parameter availability and performance.

FRAUD MANAGEMENT. The illegal brand use on Internet is an increasing problem that cannot be ignored. Organizations –regardless of industry sector and size- find it difficult to ensure to themselves the exclusive right to use their name. Online brand abuses and attacks are of many different types and sizes and the same happens with counterfeit and domain name property online market. The abuse methods are different, but the aim is always the same: the fraudulent appropriation of the company identity. With the Fraud Management service it is possible to promptly fight the brand illegal use on the whole Web. Through the combination of web monitoring and domain registrations associated to the analysis carried out by the Communication Valley SOC security team, the service carries out a brand protection program the characteristics of which allow for a rapid identification and claim to the lawbreakers of the right to use the brand, ensuring a constant and prompt response. Many different methods can be used to carry out online frauds linked to the company image use. Some are described below, with the indication of what could be done to fight the abuse.

- Improper brand use. The identification and elimination of online counterfeits and sales on the grey market is one of the objectives of the suite of solutions for company identity protection offered by Communication Valley. Damages to brand and image caused by unauthorized product sales (ex. online bids), counterfeits and distractions provoked by the grey market in strongly competitive sectors can be avoided thanks to solutions that increase the visibility on illegal online activities, by simplifying and speeding up abuse identification procedures.
- Phishing. This is an online fraud technique which uses different methods to mislead the user and convince him to give personal and sensitive information (user name, password, credit card number and so on). The most frequent attacks are carried out through false e-mail messages and suggestions of deceptive links to cheat sites. The attackers are most of the time criminal organizations that expect a very high number of users to be caught in the trap so that they can have the desired information.

- Pharming. It is a technique used to support phishing to convince the user of the legality of cheat sites. The attack is on the DNS (Domain Name Server) which is jeopardized by changing the IP addresses associated to company sites. In this case the user cannot be aware of what is happening when he keys in the correct address to connect to the desired site and is diverted to a false site used to steal the user’s credentials.
- Use of expired domains. A brand abuse attempt , as well as phishing and pharming attacks, is often carried out by using a domain name containing the company brand or a variation of it. For this reason, the creation of domains which can be exploited in that way must be always monitored.

The Fraud Management service of Communication Valley is based on a technological infrastructure dedicated to:

- Continuous monitoring -H24x365dd- of a wide range of data to find clues for phishing actions, data obtained from distributed honeypots, email, newsgroups, spam, referrers and registration areas;
- Collection of information concerning the registration of new domains and/or the monitoring of existing domain status with the aim of preventing the use of registered (or expired) domains or domains similar to the brand to be protected from ill-intentioned users;
- Collection and analysis of the actions of spiders launched on the web to search for new Internet pages that use some specific brands in order to identify their illegal (or legal) uses;
- Constant monitoring of any change to authority DNSs for specific Internet domains in order to promptly identify any pharming activity.
- Constant watching of networks and providers of malicious sites (watch-list);
- Management of the activities towards providers, organizations and bodies (ex. CERT) to obtain the closing of clone sites.

In particular, for financial institutions, Communication Valley has created the **Transaction Monitoring** module, a tool used to clearly monitor online activities (both for login and post-login) and to identify high risk actions by signaling the adequate countermeasures to the customer. With reference to Home Banking, different transaction typologies are supported: session logging, money transfer, profile change, operations on securities, card recharges and checks on specific bank web applications.

SECURITY ASSESSMENT. Test and check activities must fill the gap between a state-of-the-art design and the system operative reality. Those activities are also very important to improve the company security position. A complete and effective test and check program integrated into the operative management routine of system and application network allows the user to avoid security incidents. On the other hand, a remediation activity after an adverse event has occurred can be a non-effective effort and cost a lot in terms of money and image. The policies defined by the company have a “baseline” function to be used as a reference to evaluate if the security requirements and position emerged from the operative practice are correct. Testing activities should therefore be fully integrated in the company Risk Management practices. However, it would be limiting to use a model which only uses a “Penetrate&Patch” approach: the evolution of software vulnerability has contributed to highlight its incompleteness and non-effectiveness, therefore the installation of patches without analyzing the problem causes in detail is not considered as a strategic solution for security issues.

In this context, it is very important to setup a correct management of the risks associated to the company IT system. Such a management cannot be effective without cyclic checking activities. These activities must have a complete range of action including: people, who must be adequately trained and aware; processes reflecting policies and procedures in line with the company requirements; technologies which help to implement processes effectively. Test activities are not limited to mere technological aspects, they also must be enabled to detect operational and organizational vulnerabilities that could result into a non-correct security position.

Another very important aspect is the methodology used to execute tests and evaluate results. For its checking activities, Communication Valley uses the OSSTMM and OWASP methodologies which are universally acknowledged and used as a reference point for the execution of complete, accurate, verifiable and repeatable tests.

In order to adapt to multiple requirements, the Security Assessment activity is composed of the following modules.

- *Network & Service Discovery*. Network&Service Discovery activities are introductory to the successive Vulnerability Assessment and Penetration Test stages. They are aimed at collecting as many information as possible on tested applications and systems and on their owners and managers.
- *Network Vulnerability Assessment*. This activity is aimed at identifying all the vulnerabilities of the tested systems mainly by using automatic scanning tools. The use of automatic tools allows for the check of many systems within a limited period of time.
- *Penetration Test*. This activity is aimed at exploiting the vulnerabilities in the systems in order to jeopardize the integrity, confidentiality and availability of information and services: its ultimate aim is that of determining the feasibility degree of an attack and to check its impact in case it is successfully carried out.
- *Web Application Test*. The application security should be guaranteed mainly through a strict software design stage. Unfortunately, many development processes do not imply a standard test stage for security issues before the applications are released. The consequence is that many security issues are identified when the software has already been released into production, so that the process is non-effective and often very expensive in terms of structural remediation implementation. This activity is aimed at detecting and suggesting the changes to be adopted for software development in software engineering.
- *Wireless Assessment*. The extension of the traditional network infrastructure through a wireless component has some advantages such as higher portability and flexibility and a saving on wiring costs for a wide range of portable devices (laptops, PDAs and mobile phones) with possible connections using both Wi-Fi and Bluetooth technologies. Wireless networks are subject to the same vulnerabilities as wired ones; however, in the case of wireless networks the signal cannot be limited within a physical medium such as the cable and therefore some specific vulnerabilities are to be taken into consideration. Specific test activities can be used to highlight a series of vulnerabilities:
- *VoIP Assessment*. VoIP can be considered as one of many applications which use the data network; however, security issues must take into consideration the particular impact it has on the company business. Therefore, a correct evaluation of all possible risks is very important. The main threats are: Denial of Service, tapping, protocol vulnerability, unauthorized access, Vishing, Spit. Communication Valley operates to detect any vulnerability and suggest corrective actions.

- *Telephone Assessment*. This activity is aimed at identifying the possible security breaches generated by the interconnection between traditional telephone networks and data networks through the identification of possible internal and external attacks and abuses. Many of these problems are due to the difficulty of controlling authorized and unauthorized modem use.

EARLY WARNING. Cybercrime activities are often implemented and supported using botnets, that is networks composed of thousands of jeopardized machines geographically distributed and characterized by a high variability in terms of behavior and resistance to the countermeasures adopted to block their use. These botnets are controlled by criminal organizations that have adopted a shared usage model, “Crimeware as a Service” , with high customizing levels associated to service SLAs. It is therefore necessary to collect and process as many information as possible in order to be able to face this business model based on complex and changing scenarios. The Early Warning service provided by Communication Valley SOC has been studied to collect, map and analyze intelligence data concerning scenarios, technologies and methods used in Cybercrime. The information obtained are made available for monitoring and antifraud services to direct and support prevention and management activities concerning customers’ incidents. The same information enrich the knowledge base which is the most important element for an effective and proactive fight to continuously evolving threats.

The latest generation botnets are composed of many jeopardized machines –tens or hundreds of thousand- with a wide geographical distribution. These very dynamic scenarios can be studied only through a constant monitoring of the domains they belong to.

The information obtained in this way can lead to a decisive competitive advantage for example in the field of Security Monitoring and Fraud Management services.

The activities carried out by analysts for the Early Warning service include:

- Rationalization and mapping of intelligence data;
- Evolutive trend analysis in the different security scenarios;
- Identification and analysis of emerging threats;
- Identification and tracing of botnets and fast-flux networks (size, geographic localization, behavior and evolution pattern and so on);
- Collection and analysis of malware;
- reverse-engineering for malicious code disassembling;
- automatic supply of SIEM tools (watchlists, alerts and so on).

Those activities allow for the identification of suspicious and/or “exploit 0-day” domains and/or IP addresses”.

Data collection is carried out using different sources and tools, such as:

- *Blacklist.* Sets of domains and/or IP addresses known as sources of malicious or suspicious activity such as malware distribution, support to spam and phishing campaigns and so on.
- *Spamtraps.* E-mail boxes used only to collect spam. The received messages are analyzed to determine the domains "advertized" in the e-mails. This activity has proved to be the most effective one to collect domains linked to phishing and malware spread.
- *Honeynet.* It is composed of a set of virtual nodes (*Honeypots*) which advertize fake services and can collect both statistic data on network traffic and malicious agents (domains, IPs) and malware samples to be analyzed.
- Intelligence data collection from *non-structured sources* (ex.: RSS feeds, sites, fora, IRC channels, e-mails and so on) for the identification of emerging trends and new threats.
- *Sandbox*es. They are used to automate the collection of malicious codes and the successive analysis with the aim of precisely defining the malware behavior.

POLICY COMPLIANCE. The assurance of the compliance with company policies and standard constraints is a process which safeguards the operability, the image and the legal integrity of the company. Once again, the activity cannot be limited to the implementation of an automated collection and reporting structure (which is deemed as simple by most vendors) but it must include very complex operations:

- Context analysis compared to the reference standard through the definition of a gap;
- Aligning of organization structures and processes with the requirements imposed by the standard;
- Periodic check for constant monitoring and compliance assurance;
- Suggestion of corrective actions aimed at reaching defined thresholds;
- Release of technical and management reports.

Once the policy has been defined by a set of rules, it will be necessary to customize the approach and carry out the activities that make up the Compliance Management of the specific situation. An example list of those activities can be useful to understand the required competences.

- Software development and modification
- Suppliers security requirements
- Necessary resources definition
- Protection from malevolent software
- Log of events
- Network protection
- Privileges management
- Identification and authentication
- Sessions time-out

- Critical services isolation
- System timetable synchronization
- Data validation
- Cryptography
- Source codes protection
- Systems security verifications.

SECURITY POLICY. Experience teaches that crackers, miscreant users and authorized users have got an intrinsic advantage compared to those in charge of protecting a IT system. New vulnerabilities which increase the risk of suffering IT cybercrimes are discovered and published every day. In order to minimize the risks, special efforts must be put on increasing the IT system security level through a constant check of configurations against security. As soon as a new system starts running, a risk exists depending on the gap between its real security level and the ideal situation in which the system is not vulnerable. This risk is due to the vulnerabilities of the operative system and its applications and to the use of unsuitable configurations. It increases with time due to the discovery of new vulnerabilities or attack vehicles. The Security Policy service of Communication Valley, provided by SOC analysts and testers, is aimed at:

- Taking operative systems and applications to a suitable security level by amending the configurations that can lead to vulnerabilities (**hardening** modules);
- Maintaining a high security level for operative systems and applications either through a precise and timely application of the required patches or through configuration tuning in order to eliminate dangerous security breaches (**baseline** module);
- Considering and suggesting alternative solutions if the plant architecture, configurations or policies do not allow for the application of patches or corrective measures.

Hardening allows for the elimination –already during the initial configuration step- of a wide range of known vulnerabilities and default configurations that are not suitable for a specific environment. The hardening operations carried out typically on highly critical systems allow for the definition –at operative system and/or configuration level- the essential components and their most secure configuration.

Later on, it will be necessary to maintain at very low levels the gap between known vulnerabilities and system security level. This aim can be reached by applying the suitable security patches –baseline- periodically released by the reference vendor but it requires precise and timely interventions. The Security Policy service offers the opportunity of exploiting the knowledge base produced and maintained by Communication Valley with the aim of increasing the security level of its network infrastructure by saving time and resources in the search for required information. Part of the daily activities of Communication Valley SOC security team is dedicated to the update of operative and application systems adopted by its customers.

Within the Reply Spa Group, Communication Valley and Spike Reply are companies specialized in the field of Security and Personal Data Protection. Communication Valley is a Managed Service Provider specialized in the security management of complex networks. Its solutions are applied to all types of data and voice networks: wireless and wired, traditional and VoIP. Its portfolio includes security assessment, security device management and real time monitoring activities. Communication Valley can boast a Security Operations Center where security specialists are active H24x365.

Reply developed a comprehensive, integrated and consistent offer, in order to tackle any aspect of risks associated to an information system: from detection of threats and vulnerabilities, to the definition, planning and implementation of technological, legal, organizational, insurance or risk retention counter-measures. The Reply mission is to allow its customers to perform their business in a secure environment, thus supporting them during the development and implementation of adequate strategies and solutions, for an effective management of Information Security.

Communication Valley Reply
www.reply.eu