

SECURITY OPERATION CENTER

Il Security Operation Center è il luogo dove si realizza il rapporto fiduciario tra Communication Valley ed il cliente, un luogo fatto di competenze, aggiornamento, formazione continua ed esperienze, dove i contributi evolutivi di ciascun progetto confluiscono nella Knowledge Base comune per produrre sinergia.

SECURITY OPERATION CENTER (SOC)

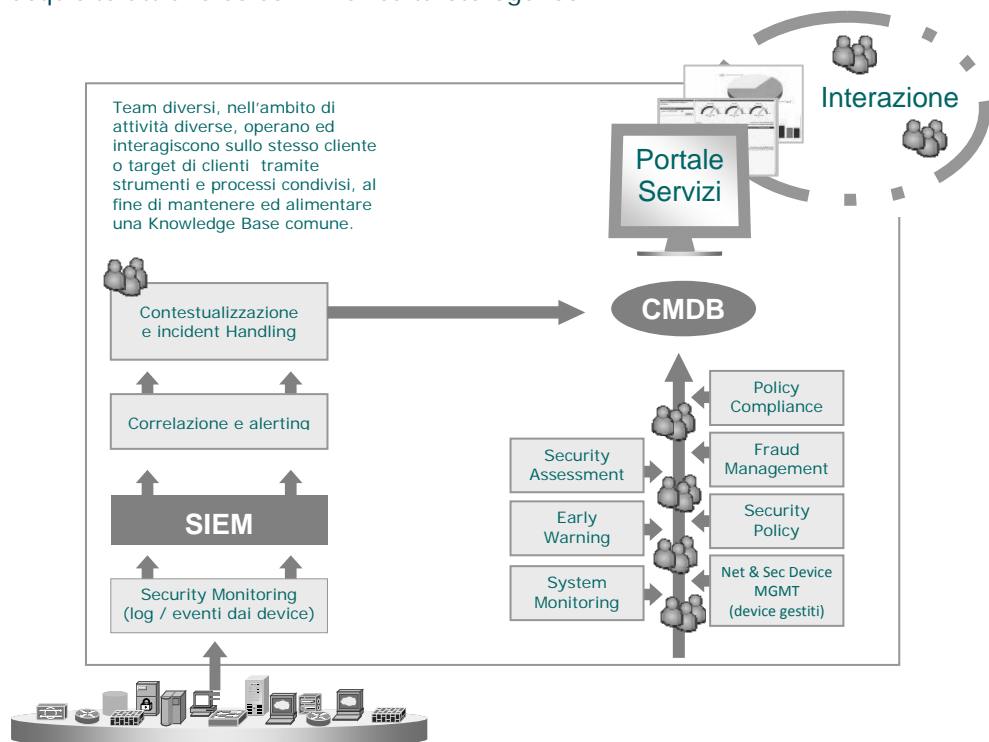
Il Security Operation Center (SOC) di Communication Valley è una struttura fisica e logica, l'unica in Italia, specializzata nell'erogazione di servizi gestiti e professionali di sicurezza informatica, che lavora per una pluralità di organizzazioni e che come centro di competenza vanta più di cento certificazioni. Si tratta di una vera e propria "torre di controllo", presidiata H24x365gg da un security team composto da analisti, sistemisti e tester, specializzati rispettivamente in attività di monitoraggio real time, gestione degli apparati di sicurezza e security assessment. Il SOC si avvale di una infrastruttura esclusiva (Enterprise Security Management), costituita da un insieme di applicazioni, per la gestione di eventi di sicurezza, il riconoscimento di pattern d'attacco, il mantenimento delle tecnologie ed il Knowledge and Asset Management. Il SOC interagisce e condivide con il cliente gli output dei servizi attraverso un portale web-based facile e ricco di contenuti. Dal SOC vengono erogati i principali servizi di sicurezza informatica che compongono l'offerta di Communication Valley.

SECURITY MONITORING. L'attuale livello di complessità raggiunto dai sistemi informatici, determinato dall'impiego su ampia scala di diverse tecnologie interconnesse (wireless, VoIP, digitale terrestre per le TLC, computer palmari), comporta la produzione di un gran numero di informazione (log) che deve poter essere letta, interpretata, gestita, mantenuta. Il servizio di Monitoring di Communication Valley agisce nel contesto delle attività di controllo e di rilevazione delle anomalie nella rete sulla base della raccolta, della correlazione e dell'interpretazione dei log generati da ogni singolo componente dell'infrastruttura di rete monitorata.

Il servizio è costituito da due componenti fondamentali, come di seguito esposto.

- Componente tecnologica. Costituita da una piattaforma SIEM (Security Information and Event Management) ingegnerizzata ed implementata allo scopo di centralizzare l'archiviazione e la gestione dei log, ma anche di mettere queste informazioni a disposizione del Security Team. A questo scopo, tutte le informazioni generate dagli apparati vengono inviate, raccolte e centralizzate. Un ulteriore motore archivia queste informazioni e le mette a disposizione del Security Team per l'analisi, la correlazione, la generazione di report e la gestione delle emergenze, secondo modalità e garanzie definite e sottoscritte.
- Componente di analisi. Componente fondamentale del servizio di Monitoring è l'attività di analisi dei dati raccolti svolta dagli analisti del Security Operations Center (SOC) di Communication Valley. Tale attività viene intesa non solo come quella che precede la notifica degli allarmi, le risposte in tempo reale, la costruzione di report ecc., ma anche come quella che si spinge fino all'implementazione di regole, procedure e soluzioni, passando per l'individuazione, la valutazione e la proposta di rimedi ritenuti necessari e urgenti. Questa attività ha valore aggiunto perché svolta da analisti altamente qualificati con un capitale di competenze riconosciuto e certificato al quale viene affidato sia il concepimento che la gestione di progetti di sicurezza complessi.

Elemento distintivo dell'offerta Communication Valley è l'approccio globale al problema sicurezza, un approccio che integra nel perimetro monitorato, le sinergie di conoscenza acquisite attraverso servizi e realtà eterogenee.



Security Monitoring

NETWORK AND SECURITY DEVICE MANAGEMENT. Il servizio di Network and Security Device Management consiste nella gestione operativa degli elementi riguardanti una determinata infrastruttura di rete (firewall, IDS, VPN concentrator, proxy, sistemi AAA, URL filtering, router, Switch, ecc.). L'infrastruttura del SOC, utilizzata per la gestione degli apparati, è stata implementata con lo scopo di istituzionalizzare le modalità di accesso e gestione dei dispositivi oggetto dei servizi in essere sui diversi clienti di Communication Valley. Attraverso un'unica console di gestione, i sistemisti SOC di Communication Valley affrontano, in maniera strutturata, le diverse attività (manutenzione ordinaria, change, fault management, patching, tuning, ecc.). L'infrastruttura è stata progettata considerando fattori quali: la flessibilità nella gestione di tecnologie diverse su differenti clienti; le modalità operative di accesso e gestione condivise dai sistemisti SOC; l'isolamento e la sicurezza dei diversi contesti e della rete SOC; il backup, versioning e mantenimento delle configurazioni; l'alta affidabilità e ridondanza.

Di seguito viene fornito un elenco schematico delle attività previste dal servizio di Network and Security Device Management.

- Gestione ordinaria: raccomandazioni, upgrade e patching dei sistemi a seguito di nuove vulnerabilità emerse; esecuzione di procedure operative ricorrenti concordate; aggiornamento delle firme del sistema.
- Problem solving: interventi di manutenzione hw, sw e configurazioni, anche relativamente agli aspetti di sicurezza; collaborazioni con gli amministratori delle applicazioni, sistemi e reti del cliente; risoluzione di eventi anomali (sistemistici e di sicurezza).
- Manutenzione correttiva: pianificazione ed esecuzione degli interventi di manutenzione ordinaria e straordinaria con azioni correttive atte ad elevare e migliorare i livelli di sicurezza dell'infrastruttura gestita.
- Manutenzione evolutiva: attività di modifica dell'architettura atta ad evolvere gli impianti in gestione (es: raccomandazioni per evoluzioni architetturali)
- Change Management: modifica delle policy e delle configurazioni secondo piani concordati; inserimento di nuovi dispositivi fisici o logici all'interno dell'infrastruttura; gestioni delle user e group policy.

La copertura del servizio, in termini di orari, è concordata attraverso SLA che partono da H8x5 Business Day fino a H24x365 (attraverso servizio di reperibilità). Viene anche concordata la modalità di interconnessione tra il SOC di Communication Valley e la rete da monitorare. Il collegamento potrà essere costituito da linea dedicata o da semplice VPN IPSec su linee Internet istituzionali.

In particolare, a complemento del servizio per le istituzioni finanziarie, Communication Valley dispone del modulo **System Monitoring** atto al monitoraggio real time H24x365gg della disponibilità e delle performance dei principali parametri dei dispositivi.

FRAUD MANAGEMENT. L'uso illecito del marchio su Internet rappresenta un problema crescente che non può essere ignorato. Le organizzazioni, a prescindere dal settore di appartenenza e dalle dimensioni, faticano a garantirsi l'esclusività del diritto all'uso del proprio nome. La casistica degli abusi e degli attacchi al brand online è differenziata e di proporzioni enormi, così come lo è quella del mercato online delle contraffazioni e della proprietà dei nomi di dominio. Le modalità di abuso sono diverse ma l'obiettivo è lo stesso, l'appropriazione fraudolenta dell'identità aziendale. Il servizio di Fraud Management permette di combattere tempestivamente l'uso illecito del marchio sull'intera rete Internet. Attraverso una combinazione di monitoraggio sul web e sulle registrazioni di domini, associate alle analisi del security team del SOC di Communication Valley, il servizio attua un programma di protezione del marchio le cui caratteristiche consentono di identificare e rivendicare velocemente ai trasgressori il diritto all'uso del brand, garantendo un monitoraggio costante e una pronta risposta. Diversi sono i metodi utilizzati per effettuare frodi online legate all'utilizzo dell'immagine aziendale. Alcuni sono esposti di seguito, con l'indicazione di quanto è possibile fare per arginare l'azione malevola.

- Uso improprio del brand. Identificare ed eliminare le contraffazioni online e le vendite nel mercato grigio è uno degli obiettivi della suite di soluzioni per la protezione dell'identità aziendale offerte da Communication Valley. I danni al marchio e all'immagine causati da vendite non autorizzate di prodotti (es: aste online), da contraffazioni e distrazioni causate dal mercato grigio in settori fortemente concorrenziali si possono evitare con soluzioni che aumentino la visibilità sulle attività illecite online, semplificando e velocizzando le procedure di identificazione degli illeciti.
- Phishing. Si tratta di una tecnica di frode online che si avvale di vari metodi per ingannare l'utente e indurlo a fornire informazioni personali e sensibili (nome utente, password, numero di carta di credito ecc.). Gli attacchi più frequenti si realizzano attraverso l'invio di false mail e la proposta di link ingannevoli che portano a siti truffa. Gli esecutori di questi attacchi, più spesso organizzazioni criminali, si aspettano che un numero considerevole di utenti cadano nel tranello per poi carpire le informazioni desiderate.
- Pharming. Si tratta di una tecnica utilizzata a supporto del phishing per rafforzare nell'utente la convinzione della legittimità dei siti truffa. Ad essere attaccato è il server DNS (Domain Name Server) che viene compromesso modificando gli indirizzi IP associati ai siti aziendali. In questo caso l'utente non può avvedersi di cosa gli stia capitando quando, digitato correttamente l'indirizzo per connettersi al sito desiderato, viene deviato su un sito falso utilizzato per sottrarre le credenziali dell'utente.
- Uso di domini scaduti. E' molto frequente che un tentativo di abuso del marchio, così come avviene per gli attacchi di phishing e pharming, venga effettuato utilizzando un nome di dominio che contiene il marchio dell'azienda o una sua variante. Per questo motivo è necessario monitorare costantemente la creazione di domini sfruttabili in tal senso.

Il servizio di Fraud Management di Communication Valley è basato su una infrastruttura tecnologica che, in breve, è dedicata a:

- monitorare continuamente, H24x365gg, una grande mole di dati per ricercare indizi che facciano risalire ad azioni di phishing, dati ottenuti da honeypot distribuiti, email, newsgroup, spam, referer e aree di registrazione;
- raccogliere informazioni inerenti la registrazione di nuovi domini e/o ad effettuare il monitoraggio sullo stato dei domini in essere, allo scopo di prevenire l'utilizzo di domini registrati (e scaduti) o simili al marchio da proteggere da parte di utenti malintenzionati;
- raccogliere e analizzare il lavoro di spider lanciati sul web alla ricerca di nuove pagine Internet che utilizzano determinati brand allo scopo di identificarne gli utilizzi illeciti (o leciti);
- monitorare costantemente eventuali cambiamenti a DNS autoritativi per determinati domini Internet allo scopo di identificare tempestivamente attività di pharming in atto.
- osservare continuativamente reti e provider di siti malevoli (watch-list);
- gestire le attività verso provider, organizzazioni ed enti (es: CERT) per l'ottenere la chiusura dei siti clone.

In particolare, a complemento del servizio per le istituzioni finanziarie, Communication Valley dispone del modulo **Transaction Monitoring** come strumento per monitorare le attività online in maniera trasparente (sia in fase di login, sia di post-login) e individuare le azioni ad alto rischio, segnalando al cliente le contromisure appropriate. Con riferimento all'Home Banking vengono supportate diverse tipologie di transazioni: logging di sessione, trasferimento di denaro, cambio profilo, operazioni sui titoli, ricariche carte, oltre ai controlli per le specifiche web application bancarie.

SECURITY ASSESSMENT. Le attività di test e verifica devono colmare le lacune tra una progettazione, allo stato dell'arte, e la realtà operativa dei sistemi. Tali attività sono inoltre fondamentali per capire, documentare e migliorare la postura di sicurezza dell'azienda. Un programma di test e verifica completo ed efficace, integrato nella routine di gestione operativa della rete dei sistemi e delle applicazioni, consente in primo luogo di evitare incidenti di sicurezza, mentre rimediare ad un evento avverso dopo che si è verificato potrebbe rivelarsi uno sforzo inefficace e molto oneroso dal punto di vista economico e di immagine. Le politiche stabilite dall'azienda hanno funzione di "baseline" a cui fare riferimento per valutare se i requisiti e la postura di sicurezza riscontrati nella pratica operativa sono corretti. Le attività di testing dovrebbero pertanto essere integrate a pieno titolo nelle pratiche di Risk Management aziendale. Sarebbe però limitativo affidarsi unicamente ad un modello che si limita ad un approccio "Penetrate&Patch": l'evoluzione delle vulnerabilità nel software ha contribuito a evidenziarne l'incompletezza e l'inefficacia, installare le patch di sicurezza senza approfondire le cause dei problemi non è quindi considerata una soluzione strategica alle problematiche di sicurezza.

In questo contesto, è di primaria importanza impostare una corretta gestione dei rischi associati al sistema informativo aziendale, gestione che non può prescindere da attività cicliche di verifica. Queste attività devono avere uno spettro di azione completo, che comprenda: persone, a cui vanno garantite sufficienti preparazione e consapevolezza; processi, che riflettano politiche e procedure adeguate alle necessità aziendali;

tecnologie, che consentano di implementare i processi in modo efficace. L'attività di test non si limita agli aspetti puramente tecnologici, ma deve poter rilevare anche le vulnerabilità di tipo operativo ed organizzativo che potrebbero risultare in una scorretta postura di sicurezza.

Un aspetto di fondamentale importanza è anche la metodologia utilizzata per l'esecuzione dei test e la valutazione dei risultati. Communication Valley ispira le sue attività di verifica alle metodologie OSSTMM e OWASP, globalmente riconosciute e adottate come punto di riferimento per l'esecuzione di test completi, accurati, verificabili e ripetibili.

In modo da potersi adattare a molteplici esigenze, l'attività di Security Assessment è composta dai seguenti moduli.

- *Network & Service Discovery.* Le attività di Network&Service Discovery sono propedeutiche alle successive fasi di Vulnerability Assessment ed eventualmente Penetration Test e si prefiggono l'obiettivo di raccogliere il maggior numero di informazioni possibili sui sistemi e le applicazioni oggetto del test, nonché sui proprietari e gli eventuali gestori.
- *Network Vulnerability Assessment.* In questa attività si cerca di individuare tutte le vulnerabilità presenti sui sistemi oggetto del test utilizzando principalmente scanner automatici. L'uso di strumenti automatici consente di eseguire la verifica di un grande numero di sistemi in un lasso di tempo limitato.
- *Penetration Test.* In questa attività, si cerca di sfruttare le vulnerabilità presenti sui sistemi per compromettere l'integrità, la confidenzialità e la disponibilità delle informazioni e dei servizi: lo scopo ultimo è quello di determinare il grado di fattibilità di un attacco e di verificarne l'impatto nel caso venga portato a termine con successo.
- *Web Application Test.* La sicurezza degli applicativi dovrebbe essere garantita principalmente attraverso una rigorosa fase di progettazione del software. Sfortunatamente, molti processi di sviluppo non prevedono ancora una fase standard di test relativa agli aspetti di sicurezza, prima che gli applicativi vengano rilasciati. La conseguenza è che molti problemi di sicurezza vengono individuati quando il software è già in produzione, rendendo il processo inefficace e spesso proibitivo dal punto di vista dei costi necessari per implementare rimedi strutturali. Questa attività è mirata a rilevare e proporre le modifiche da adottare nello sviluppo del software nell'ingegnerizzazione del software.
- *Wireless Assessment.* I vantaggi di estendere la tradizionale infrastruttura di rete con una componente wireless sono essenzialmente la superiore portabilità e flessibilità unite al risparmio sul costo dei cablaggi, di cui beneficia una vasta gamma di apparati portatili, quali laptop, PDA e telefoni cellulari, con capacità di interconnettersi utilizzando non solo la tecnologia Wi-Fi ma anche quella Bluetooth. Le reti wireless sono soggette alle medesime vulnerabilità delle reti cablate, però diversamente dalle reti tradizionali non è possibile confinare il segnale all'interno di un mezzo fisico come il cavo, e questo comporta l'esistenza di possibili vulnerabilità specifiche. L'insieme delle attività di test consente di evidenziare una serie di possibili criticità, come elencato di seguito.

- *VoIP Assessment*. Nonostante il VoIP possa essere considerato come una delle tante applicazioni che si appoggiano sulla rete dati, gli aspetti legati alla sicurezza devono tenere conto del particolare impatto dello stesso nel business aziendale, e assume quindi grande importanza la corretta valutazione dei possibili rischi. Le minacce principali sono: Denial of Service, intercettazione, vulnerabilità dei protocolli, accesso non autorizzato, Vishing, Spiti. Communication Valley opera al fine di rilevare eventuali vulnerabilità e proporre azioni correttive.
- *Assessment telefonico*. Questa attività ha lo scopo di individuare le possibili falle di sicurezza generate dalle interconnessioni tra reti telefoniche tradizionali e reti dati, individuando possibili attacchi ed abusi sia dall'interno che dall'esterno. Buona parte di questi problemi sono legati alla difficoltà del controllo dell'utilizzo di modem, autorizzati o meno.

EARLY WARNING. Le attività di cybercrime vengono spesso implementate e supportate utilizzando botnet, ovvero reti composte da migliaia di macchine compromesse, geograficamente distribuite e caratterizzate da una estrema variabilità di comportamento e resistenza alle contromisure adottate per bloccarne l'utilizzo. Queste botnet sono controllate da organizzazioni criminali che hanno adottato un modello di utilizzo condiviso, "Crimeware as a Service", con elevati livelli di personalizzazione associati a veri e propri SLA di servizio. E' necessario quindi raccogliere ed elaborare il maggior numero di informazioni possibili per poter contrastare questo modello di business basato su scenari complessi e mutevoli. Il servizio di Early Warning, erogato dal SOC di Communication Valley, è studiato per raccogliere, correlare e analizzare i dati di intelligence relativi a scenari, tecnologie e metodi utilizzati nell'ambito del Cybercrime. Le informazioni ottenute vengono messe a disposizione dei servizi di monitoraggio e antifraud al fine di indirizzare e supportare le attività di prevenzione e gestione degli incidenti dei clienti. Le stesse informazioni arricchiscono, di volta in volta, la knowledge-base, che costituisce la chiave per poter contrastare efficacemente e in modo proattivo le minacce in continua evoluzione.

Le botnet di ultima generazione sono costituite da un numero di macchine compromesse molto elevato, nell'ordine delle decine o centinaia di migliaia, con una geolocalizzazione molto distribuita. Questi scenari estremamente dinamici possono essere studiati solo attuando un costante monitoraggio dei domini che ne fanno parte.

Le informazioni che si possono ricavare possono prefigurare un vantaggio competitivo determinante nell'ambito dell'erogazione ad esempio dei servizi di Security Monitoring e Fraud Management.

Le attività svolte dagli analisti nel servizio di Early Warning comprendono:

- la razionalizzazione e correlazione dei dati di intelligence;
- l'analisi dei trend evolutivi nei vari scenari di sicurezza;
- l'individuazione ed analisi delle minacce emergenti;
- l'individuazione e tracciamento di botnet e reti fast-flux (dimensioni,

- geolocalizzazione, pattern di comportamento ed evoluzione, ecc.);
- la raccolta ed analisi di malware;
- reverse-engineering per disassemblare codice malevole;
- l'alimentazione automatica degli strumenti SIEM (watchlist, alert, ecc.).

Queste attività permettono l'individuazione di domini e/o indirizzi IP sospetti e/o "exploit 0-day".

La raccolta dei dati è effettuata sfruttando diverse fonti e strumenti. Alcuni esempi.

- *Blacklist* insiemi di domini e/o indirizzi IP noti come sorgenti di attività malevola o sospetta, quali la distribuzione di malware, il supporto a campagne di spam e phishing, ecc..
- *Spamtrap* sono caselle di posta elettronica utilizzate unicamente per raccogliere spam. I messaggi ricevuti vengono analizzati per determinare i domini "pubblicizzati" all'interno delle email. Questa attività si è rivelata la più proficua in assoluto per collezionare domini legati a fenomeni quali il phishing o la diffusione di malware.
- *Honeynet* è costituita da un insieme di nodi virtuali (*Honeypot*) che espongono servizi fittizi e sono in grado di raccogliere sia dati statistici sul traffico di rete e sugli agenti (domini, IP) malevoli, che campioni di malware da analizzare.
- raccolta dati di intelligence da *fonti non strutturate* (es.: feed RSS, siti, forum, canali IRC, email, etc.) per l'individuazione dei trend emergenti e la comparsa di nuove minacce.
- *Sandbox* utilizzati per automatizzare la raccolta dei codici malevoli e la successiva analisi con lo scopo di definire con precisione il comportamento dei malware.

POLICY COMPLIANCE. La realizzazione della conformità rispetto a policy aziendali e vincoli normativi è un processo che tutela l'operatività, l'immagine e l'incolumità legale dell'impresa. Ancora una volta non si tratta solo di implementare una struttura automatizzata di raccolta e reportistica, cosa dichiarata semplice dalla maggior parte dei vendor, ma di effettuare una più complessa operazione di:

- analisi del contesto rispetto allo standard/norma di riferimento definendo un gap;
- allineamento delle strutture e dei processi organizzativi ai requisiti imposti dallo standard/norma;
- controllo periodico che consenta di monitorare e mantenere la compliance;
- proposizione delle azioni correttive pesate per il raggiungimento alle soglie definite;
- rilascio di report tecnici e direzionali.

Dato un insieme di regole che definiscano la policy sarà necessario contestualizzare l'approccio e di volta in volta eseguire l'insieme delle attività che, per una specifica realtà, costituiscono il Compliance Management. Un elenco, esempio di tali attività, è utile per comprendere il necessario apporto di competenze.

- 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. L'esperienza insegna che cracker, utenti malintenzionati e utenti autorizzati, hanno un vantaggio intrinseco rispetto a chi ha il compito di difendere un sistema informatico. Quotidianamente vengono scoperte e divulgate nuove vulnerabilità che aumentano il rischio di subire reati informatici.

Allo scopo di minimizzare tale rischi è necessario concentrare gli sforzi sull'aumento del livello di sicurezza dei sistemi informatici utilizzati tramite un controllo continuo delle configurazioni in ottica di sicurezza.

Sin dal primo momento in cui viene messo in esercizio un nuovo sistema, esiste un rischio legato al gap tra il suo livello di sicurezza effettivo e la situazione ideale in cui il sistema stesso non è vulnerabile. Questo rischio è dovuto alle vulnerabilità che affliggono il sistema operativo e le applicazioni presenti sul sistema, nonché all'applicazione di configurazioni non idonee, e cresce nel tempo a causa della scoperta di nuove vulnerabilità o vettori di attacco. Il servizio di Security Policy di Communication Valley, curato dagli analisti e tester del SOC, permette di:

- elevare ad un adeguato livello di sicurezza i sistemi operativi e le applicazioni correggendo le configurazioni che introducono vulnerabilità (modulo **hardening**);
- mantenere nel tempo un elevato livello di sicurezza dei sistemi operativi e delle applicazioni tramite una puntuale applicazione delle patch necessarie o attraverso tuning delle configurazioni al fine di eliminare pericolose falle di sicurezza (modulo **baseline**);
- valutare e suggerire alternative nel caso l'architettura, le configurazioni o le policy dell'impianto non permettano l'applicazione di patch o misure correttive.

L'hardening permette di eliminare, già in fase di configurazione iniziale, una vasta gamma di queste vulnerabilità note e di configurazioni di default che non sono corrette relativamente ad uno specifico ambiente. Le operazioni di hardening, realizzate

tipicamente sui sistemi ritenuti ad alta criticità, permettono di definire, a livello di sistema operativo e/o configurazione, i soli componenti essenziali e la loro più sicura configurazione.

Successivamente, sarà necessario mantenere a livelli minimi il gap tra vulnerabilità note e livello di sicurezza del sistema. Tale scopo è raggiungibile applicando le adeguate patch di sicurezza, baseline, rilasciate periodicamente dal vendor di riferimento ma richiede interventi precisi e tempestivi. Il servizio di Security Policy offre la possibilità di sfruttare la knowledge-base prodotta e mantenuta da Communication Valley, allo scopo di aumentare il livello di sicurezza della propria infrastruttura di rete, risparmiando tempo e risorse nella ricerca delle informazioni necessarie. Parte delle attività quotidiane del security team del SOC di Communication Valley è dedicata all'aggiornamento dei sistemi, operativi e applicativi, adottati dai suoi clienti.



All'interno del Gruppo Reply SpA, Spike Reply e Communication Valley sono le società specializzate sulle tematiche relative all'area della Sicurezza e della tutela dei Dati Personali. Communication Valley è un Managed Service Provider specializzato nella gestione della sicurezza di reti complesse. Le soluzioni offerte si applicano alle reti dati e voce, in tutte le loro modalità: wireless e wired, tradizionali e VoIP. Il portafoglio comprende attività di security assessment, gestione di apparati di sicurezza, monitoraggio in tempo reale. Communication Valley vanta un Security Operations Center presidiato H24x365 da specialisti di sicurezza.

Reply ha definito un'offerta completa, integrata e coerente per affrontare ogni aspetto del rischio associato ad un sistema informativo: dall'individuazione delle minacce e delle vulnerabilità, alla definizione, progettazione e di implementazione delle relative contromisure tecnologiche, legali, organizzative, assicurative o di ritenzione del rischio. La missione di Reply è di permettere ai propri clienti di effettuare il loro business in condizioni di Sicurezza, supportandoli nello sviluppo delle idonee strategie e nella implementazione delle appropriate soluzioni per una gestione efficace della Sicurezza delle Informazioni.