

CYBER SECURITY OPERATION CENTER

Il nuovo Cyber Security Operation Center di Reply è una struttura specializzata nell'erogazione di servizi di sicurezza di livello Premium, personalizzati in base ai processi del cliente, ai suoi bisogni e alle specifiche minacce del settore in cui il cliente opera.

Il team del Cyber Security Operation Center di Communication Valley Reply, nato per rispondere alle richieste di sicurezza di banche e istituti finanziari, mette a disposizione i propri asset e le proprie competenze per aziende che operano in ambienti altrettanto complessi, come i settori Retail, Manufacturing e Utilities.



METTI AL SICURO LA TUA AZIENDA

**24 ORE SU 24
365 GIORNI ALL'ANNO**

CYBER SECURITY OPERATION CENTER

Il Cyber Security Operation Center è una vera e propria "torre di controllo", presidiata 24 ore su 24, 365 giorni all'anno, da un team composto da Analisti di Sicurezza, System Engineer, Security Tester e Malware Specialist.

I servizi del Cyber Security Operation Center (CSOC) utilizzano un nuovo modello di monitoraggio della sicurezza che si basa su un primo livello di analisti altamente specializzati. Questo modello, già al primo livello di assistenza, consente di ridurre i tempi di reazione e di accelerare l'applicazione delle contromisure necessarie.

L'individuazione preventiva e la gestione real time degli incidenti di sicurezza sono fattori di primaria importanza per garantire alle aziende un adeguato livello di protezione delle reti, dei dati e dei servizi. Il Cyber Security Operation Center è uno spazio dove, con le più evolute tecnologie, un team di esperti svolge attività di monitoraggio real time, security assessment e gestione degli apparati di sicurezza.

I SERVIZI



CYBER SECURITY MANAGEMENT

I servizi di **Cyber Security Management** nascono per garantire le attività “core” di gestione della sicurezza del cliente. In particolare, il servizio di Security Monitoring rappresenta il mezzo principale per la rilevazione e la gestione degli incidenti di sicurezza.

Questo servizio è basato sulla raccolta e correlazione degli eventi provenienti dall’infrastruttura, dai sistemi e dagli applicativi del cliente. Tutte le informazioni sono collezionate dalla piattaforma di Advanced Security Analytics che consente l’analisi degli eventi provenienti da fonti eterogenee e da diversi clienti.

In questo modo il CSOC massimizza la possibilità di individuare anche le forme di attacco più sofisticate, pur garantendo, attraverso la separazione logica delle informazioni relative ai diversi clienti, il massimo livello di privacy.

La medesima piattaforma è utilizzata dai System Engineer e dai Malware Specialist per l’erogazione di servizi verticali come: Cyber Threat Intelligence, Breach Detection e 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

Con la diffusione dei servizi online e multicanale si è assistito ad un incremento di attività fraudolente, sia in termini di volume, che di complessità. Queste attività sono in genere finalizzate al furto di identità, credenziali o altre informazioni utili a perpetrare le frodi.

I servizi di **Fraud Management** del CSOC si focalizzano sull’individuazione e l’analisi di Malware per diverse tipologie di device, sulla rilevazione e chiusura di siti clone utilizzati per veicolare campagne di phishing, sull’analisi di transazioni finanziarie fraudolente e, in caso di frodi complesse, sulla risposta a incidenti di sicurezza comprensiva di analisi forensi.

Il CSOC dispone di tecnologie e applicazioni che consentono di individuare le frodi grazie all’analisi e alla rilevazione di comportamenti anomali all’interno delle sessioni di navigazione.

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

I servizi di **Managed Network Security** permettono una gestione unificata delle infrastrutture di rete, uniformando i sistemi di accesso e di gestione per gli apparati di servizio operanti presso i diversi clienti del CSOC.

Un'unica console di gestione consente ai System Engineer di intervenire in maniera organizzata e strutturata sia per la gestione di incident, così come per attività di gestione ordinaria o straordinaria, come il patching, il tuning e i change.

Gli elementi distintivi dell'infrastruttura del centro sono:

- Flessibilità nella gestione delle diverse tecnologie utilizzate dai nostri clienti.
- Standardizzazione e condivisione dei metodi per l'accesso e di gestione dei sistemi.
- Sicurezza e strutturazione a comparti separati sia per gli ambienti dei clienti, sia nell'infrastruttura stessa del CSOC.
- Attenta gestione delle configurazioni che vengono memorizzate e per le quali si mantengono versioning e opportuni backup.
- Alta affidabilità e ridondanza.

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

ENTERPRISE MOBILITY SERVICES

L'uso incrementale dei dispositivi mobili, e dei contenuti in essi ospitati e veicolati, ha alimentato la necessità di strumenti e servizi enterprise specifici per la regolamentazione delle applicazioni mobili e della sicurezza associata.

La crescente adozione dei dispositivi personali all'interno dei contesti aziendali (Bring Your Own Device) rappresenta oggi per le aziende un'opportunità ed un rischio allo stesso tempo. Il CSOC è in grado di supportare il cliente nello sviluppo di una strategia BYOD al fine di massimizzare i benefici senza dimenticare l'aderenza alle pratiche di sicurezza. Servizi di End

User Computing sono erogati per monitorare e gestire le postazioni di lavoro, le applicazioni mobili e la loro sicurezza, garantendo un contributo specialistico ai clienti in modalità 8x5 o 24x7, a seconda delle diverse esigenze.

Gli **Enterprise Mobility Services** erogati dal CSOC

supportano i clienti nella gestione dei device e delle applicazioni mobili, al fine di garantire la piena compatibilità con le piattaforme di Mobile Device Management e l'aderenza ai principi di sicurezza.

Il CSOC sostiene il cliente sia nello sviluppo sicuro di applicazioni aziendali, sia nella "messa in sicurezza" delle applicazioni di terze parti.

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



COMMUNICATION VALLEY REPLY è la società del gruppo Reply specializzata nell'erogazione di servizi di sicurezza gestita. Attraverso il proprio Cyber Security Operation Center certificato ISO27001 con un presidio 24x7, 365 giorni l'anno, assicura continuità di business e prevenzione dalle frodi ad aziende di medie e grandi dimensioni. I servizi di Communication Valley Reply comprendono System & Security Monitoring, Remote SIEM Management & Optimization, Log Management, Security Device Management e Network Device Management. Communication Valley Reply fornisce inoltre servizi altamente specializzati di Banking Fraud Detection che permettono di individuare frodi online e di attivare le necessarie azioni di contrasto, e di IT Operation che permettono di gestire interi sistemi in outsourcing in modalità H24.

Communication Valley Reply collabora con i principali istituti di ricerca, con università internazionali e con i principali partner tecnologici del settore per diventare il punto di riferimento in Europa per i Managed Security Services.

CYBER SECURITY OPERATION CENTER

Via Robert Koch 1/4, Torre B,
20152 Milano, Italy

www.communicationvalley.com
csoc@reply.com