Security Operations Center

La gestione delle piattaforme di sicurezza di una rete, come proxy, firewall e sonde di allarme per la previsione delle intrusioni, necessitano giornalmente di attenzioni. La rete comunica messaggi ma amministratori e security manager hanno in genere poco tempo da dedicare alle comunicazioni di allerta che generano tutte le apparecchiature di monitoring.

Sempre più utenti malintenzionati, con connessioni a banda larga e conoscenze tecniche evolute, utilizzano i mezzi a loro disposizione per danneggiare e sottrarre informazioni riservate da sistemi informatici di aziende esposte alla rete Internet, sfruttando vulnerabilità rilevate nei software degli ambienti di esercizio. La soluzione a molti attacchi subiti risiede nei log degli apparati spesso trascurati per ragioni di carico di lavoro.

Una regola di maggior efficacia è la prevenzione, ovviamente accompagnata dal monitoraggio.

Il SOC si propone come obiettivo la totale gestione delle apparecchiature che compongono la sicurezza della rete, dal quotidiano controllo dei segnali di allarme prodotti dalle sonde IDS / IPS a seguito delle intrusioni, al dinamico cambiamento delle politiche di accesso e di filtro sui sistemi firewalls che subiscono attacchi o che dovrebbero proteggere la vostra rete. Il controllo ed il filtro del traffico produce inoltre l'ottimizzazione della banda oltre a ridurre il rischio di sfruttamento delle vulnerabilità non monitorate.

Evitare una violazione del sistema, vuol dire prevenire ogni rallentamento dell'operatività aziendale e annullare le conseguenti perdite finanziarie.

Lo staff di Security Division si preoccuperà di adottare le misure necessarie per ottimizzare i sistemi di controllo e la gestione di tutte le apparecchiature che compongono la sicurezza della vostra rete, il tutto da un centro servizi remoto, semplificando la gestione di sistemi di sicurezza sempre più complessi, trasformando milioni di allarmi di sicurezza in un numero ridotto di eventi di vero interesse, selezionati e gestibili, per la sicurezza proattiva della rete.