NSOC

Is time to rethink security concept!

A great cyber security and development company

Network & Security Operation Center

NSOC

Network & Security Operation Center

COS'E' UN NSOC?

E' un centro di controllo e monitoraggio in cui vengono forniti servizi finalizzati alla al monitoraggio infrastrutturale di reti e sistemi e relaitivi sicurezza.

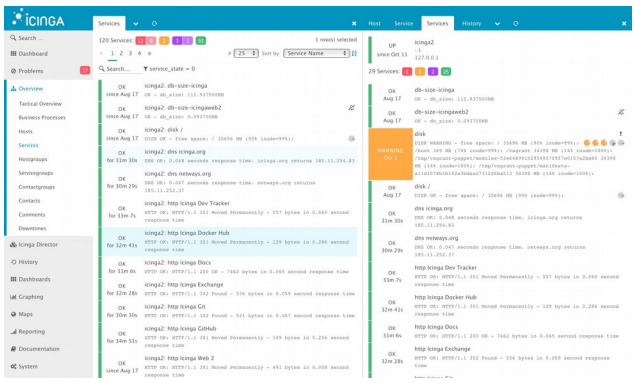
Un NSOC fornisce tre diverse tipologie di servizi:

- ✔ servizi di gestione: tutte le attività di gestione dele funzionlità di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni) sono centralizzate dal SOC;
- ✔ servizi di monitoraggio: l'infrastruttura IT e di sicurezza vengono monitorate in tempo reale al fine di individuare tempestivamente tentativi di intrusione, di attacco o di abuso delle risorse;
- ✔ servizi proattivi: sono servizi finalizzati a migliorare il livello di protezione dell'organizzazione (security assessment, vulnerability assessment, early warning, security awareness).

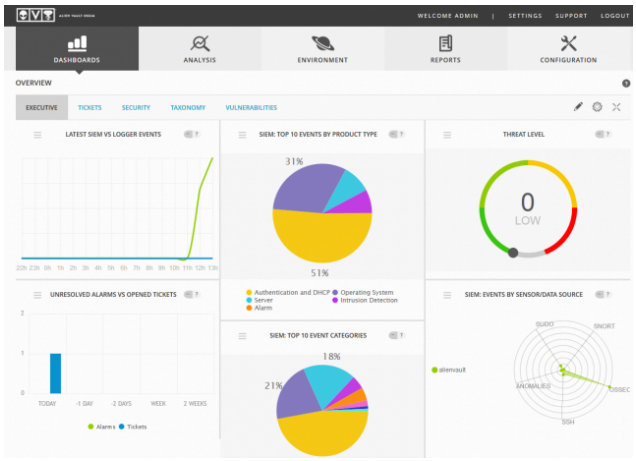
IL NSOC DI SEC4U

Il NSOC di SEC4U è fondato su tre diversi elementi tra loro correlati:

- un sistema di monitoraggio ed alerting degli eventi di networking e di sistema, che analizza diverse metriche provenienti dagli agents in modalità passiva oppure attraverso query attive sui sistemi; il sistema consente di creare dei business process relativi ai processi aziendali e di generare dei report di SLA che è possibile condividere con i propri clienti;



- un sistema di monitoraggio ed alerting degli eventi di sicurezza, che offre al proprio interno moduli di vulnerability assessment, intrusion detection, behavioral monitoring, event correlation. Questo modulo permetterà di essere compliance con quanto stabilito in materia dal General Data Protection Regulation (GDPR), che indica la necessità di adottare software sentinella che verifichino e segnalino eventuali attacchi esterni o accessi interni non autorizzati;



- un modulo di UIDAPO che mette a disposizione dei nostri clienti i servizi di early warning, Vulnerability and Threat Finder personalizzata sui software presenti all'interno dell'infrastruttura del cliente, gestione centralizzata degli incidenti di sicurezza, repository delle configurazioni dei dispositivi aziendali critici (switch, router, firewall) ed un modulo interattivo per la segnalazione del data breach (che il GDPR obbliga a rendere noto entro 72 ore) al Garante per la protezione dei dati personali.