Contribution ID: **372** Type: **Poster**

Prototipo di SOC minimale per la rilevazione delle minacce sul traffico DNS

Un Security Operations Center (SOC) è un insieme di processi, tecnologie e persone qualificate che monitorano, rilevano e analizzano in tempo reale la presenza di anomalie o minacce sulle reti informatiche. All' interno dell'INFN si stanno progressivamente adottando degli strumenti utili a creare una solida piattaforma SOC a protezione dell'infrastruttura di calcolo nazionale distribuita e federata dell'ente. Tra questi strumenti si sta testando un prototipo del software pDNSSOC, un SOC minimale che analizza il traffico DNS e vi cerca correlazioni con domini e IP malevoli forniti da una piattaforma di intelligence e condivisione delle minacce. Ciò permette di identificare tracce di infezioni sulle macchine client che hanno fatto richieste al server DNS e di allertare gli amministratori di tali macchine affinché'analizzino le minacce rilevate e vi pongano rimedio.
Il pDNSSOC opera attraverso diverse componenti software open-source che comunicano tra loro. Una coppia di collettori DNS passivi ad alta velocità, go-dnscollector, è installata sul server DNS e sulla macchina ospitante il pDNSSOC con una pipeline configurata per la raccolta e il trasferimento dei dati di log del DNS verso il pDNSSOC. La pipeline consente diverse modalità di anonimizzazione dei dati relativi alle macchine client da cui sono partite le richieste al DNS. Questi dati vengono analizzati dal servizio pDNSSOC, che funziona da motore di correlazione dei dati del DNS con gli indici di compromissione (IOC) ricevuti tramite REST API da un'istanza del MISP, la piattaforma open-source standard delineata dalla comunità internazionale di cibersicurezza per la raccolta e lo scambio delle informazioni. Ogni qual volta che il pDNSSOC trova una correlazione con un IOC del MISP, riporta i dati relativi all'incidente di sicurezza rilevato in un file in formato json e in un messaggio di posta elettronica inviato a un indirizzo e-mail preimpostato.
Lo sviluppo del prototipo di pDNSSOC è attualmente in fase avanzata all'interno della piattaforma INFN DataCloud. È prevista anche l'implementazione della raccolta e della visualizzazione dei dati relativi alle minacce rilevate tramite il servizio OpenSearch di INFN DataCloud, per consentire un monitoraggio ottimale tramite creazioni di apposite dashboard. Successivamente si procederà con l'implementazione del pDNSSOC su una o più infrastrutture di sezioni pilota, per proporre infine una messa in produzione guidata e testata anche su tutte le altre infrastrutture di calcolo dell'ente.

Primary author: LENNI, Alex (Istituto Nazionale di Fisica Nucleare)

Session Classification: Poster

Track Classification: Security e compliance