Algoritmi di analisi del traffico di rete che riconoscono le anomalie

La problematica

Le grandi aziende ed infrastrutture critiche sono molto sensibili ai temi della sicurezza informatica ed hanno adottato, già da anni a questa parte, tecnologie e sistemi di protezione, per fare fronte ai sempre più numerosi e sofisticati attacchi cibernetici. La maggior parte dei prodotti di mercato è di tipo rule-based: sono cioè disegnati per identificare comportamenti malevoli già noti (es. firme di virus o attacchi conosciuti), ma risultano carenti nell'identificazione di tutto ciò che non è noto (es. attacchi 0-day). Oggi l'interesse e l'obiettivo di molte aziende è quello di superare questo limite evitando, al contempo, di generare eccessivi carichi di lavoro aggiuntivi per gli analisti di sicurezza o impatti sull'infrastruttura.

La Soluzione

Il mezzo più efficace per l'identificazione di comportamenti non noti è rappresentato dal Machine Learning: si tratta tecniche statistiche avanzate che osservano il comportamento degli host di una rete e, senza nessuna conoscenza a priori (ovvero senza regole), stabiliscono quando sono in atto situazioni anomale che meritano l'attenzione degli analisti. Crisma Security ha sviluppato una suite di algoritmi in grado di raccogliere e analizzare il traffico di rete e i log dei sistemi e di produrre score di anomalia al crescere dei quali

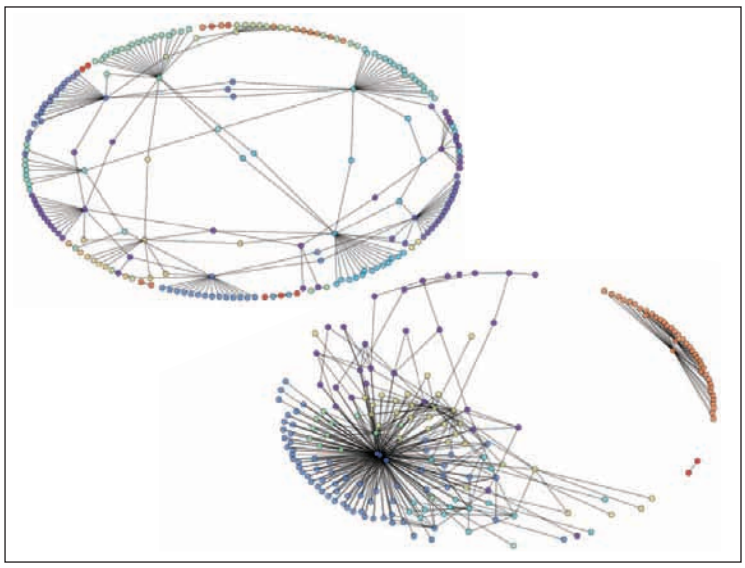
La soluzione Crisma Security è stata implementata in un'importante Utility del settore energia

aumenta il livello di attenzione da dedicare. La soluzione è composta da diversi moduli.
Il modulo BASE agisce al massimo livello di dettaglio: analizza le singole sessioni di traffico scremando decine di milioni di eventi e, tra questi, identificando le poche unità che necessitano di attenzione.
Il modulo OLISTICO, al contrario, osserva il comportamento dei sistemi in toto e solleva allarmi, ad esempio, quando la topologia della rete assume forme inusuali (condizione che si verifica quando sono in corso attacchi di tipo organizzato).
Il modulo Root Cause Intelligence ha l'obiettivo di fornire indicazioni sulle cause più probabili che possono aver scatenato un'anomalia.

I Benefici

Questa soluzione presenta diversi tratti distintivi, la cui somma ne determina il valore. Il primo: non richiede componenti HW aggiuntivi per la raccolta dei dati. Il secondo: non genera sovraccarico per la rete in quanto non vi è duplicazione del traffico. Terzo: non richiede l'ispezione di dati sensibili come, ad esempio, il payload dei pacchetti rendendo agevole il raggiungimento della compliance con le norme attuali di Data Protection. È inoltre concepita su di un'architettura Big Data (è in grado di scalare naturalmente al crescere dei volumi di traffico). Tutto il codice non proprietario è di tipo Open Source: è quindi sicuro e ispezionabile anche dalle realtà più esigenti. Gli algoritmi sono stati disegnati per ridurre al minimo il lavoro aggiuntivo per gli analisti di sicurezza: i moduli generano volumi controllabili di segnalazioni e il Root Cause Intelligence indirizza gli analisti nella ricerca delle cause con l'effetto di ridurre il tempo medio necessario per l'analisi delle anomalie. Questa soluzione è stata installata presso importanti aziende italiane e nel tempo ha permesso di generare diversi incident e ha innalzato i livelli di sicurezza complessivi in azienda. Il tutto senza dover incrementare il numero di analisti al proprio interno.

CRISMA SECURITY
www.crismasecurity.it



Gli algoritmi raccolgono e analizzano il traffico di rete e i log dei sistemi e producono score di anomalia al crescere dei quali aumenta il livello di attenzione da dedicare

Questa soluzione è ideale per qualunque azienda strutturata e di grandi dimensioni

La soluzione non richiede componenti HW aggiuntivi, non sovraccarica la rete, non richiede l'ispezione di dati sensibili ed è concepita su un'architettura Big Data (scala al crescere dei volumi di traffico)