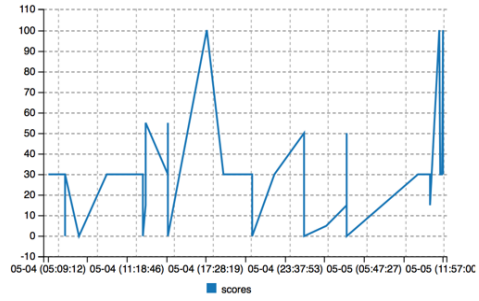
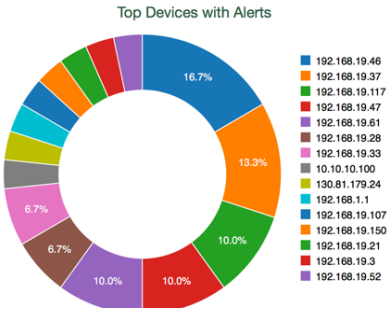
Dlaczego Seceon OTM?

- Dzięki wykorzystaniu przepływów sieciowych (netflow/sflow) Seceon daje wgląd w każdy obszar Data Center i to przy zaledwie 1,5% dodatkowym obciążeniu sieci. System jest skalowalny i działa w czasie rzeczywistym.
- Seceon wykrywa zaszyfrowane ataki na serwery webowe (SQL Injection, XSS i inne) dzięki analizie logów serwerów Apache/IIS i aktywnemu wyszukiwaniu wzorców takich ataków. Zarówno firewalle, jak i sieciowe IDS'y przepuszczają zaszyfrowany ruch, a deszyfracja wprowadza opóźnienie i zabija wydajność, dlaczego więc nie pozwolić końcówce na deszyfrację i dopiero wtedy wysłać log?
- Seceon dostarcza informację o dokładnej lokalizacji zainfekowanego urządzenia na podstawie analizy przepływów sieciowych (Layer 2 Switch i jego ifindex), podczas gdy firewall (ze swoim Layer 3) gubi informacje o źródle sfałszowanego IP.

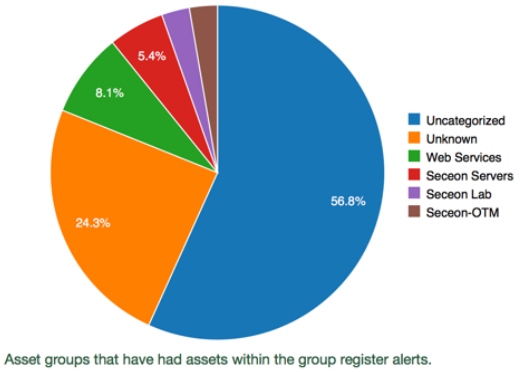


Alert trends are how we determine when unusual network behavior happens. This chart shows the trend for the selected time period.



- Seceon wykrywa malware już w fazie rekonesansu (zgodnie z Malware Kill Chain) dzięki analizie behawioralnej, szerokiemu wglądowi w wewnętrzny ruch sieciowy i logi oraz identyfikacji podejrzanych działań. Zarówno firewall, jak i sieciowy IDS mogą wykryć i zablokować komunikację z Command&Control, ale dlaczego nie mielibyśmy podjąć działań wcześniej, kiedy malware po zainfekowaniu serwera wykonuje dopiero rekonesans w postaci skanowania, podejrzanych działań czy zmiany zachowań ruchu sieciowego itp.? Seceon OTM potrafi wykryć takie zachowania i powiadomić Klienta nie czekając na ustanowienie komunikacji z C&C.
- Seceon Intensywnie wykorzystuje algorytmy kwantowe Abramsa-Lloyda oraz analizę behawioralną do wykrywania ataków typu Zero Day. Obserwuje logi i przepływy sieciowe dla całego Data Center i na tej podstawie tworzy wzorce zachowań zarówno dla użytkowników jak i dla serwerów/stacji. Zidentyfikowana zmiana zachowań jest korelowana z przepływami, logami i wiedzą o zagrożeniach, co pozwala na wykrycia ataków Zero Day.
- Koncepcja działania Seceon OTM ucina zabawę „w kotka i myszkę" twórców malware'u z producentami zabezpieczeń / zespołami ds. bezpieczeństwa IT (malware przyczajony w sandbox).

- Seceon został zaprojektowany, aby chronić, wykrywać i reagować na ataki. Pozwala on klientowi na definiowanie polityk takich jak np.: ruch DNS/Mail zawsze przechodzi przez serwery DNS/Mail. Definiowanie polityk pozwala na wykrywanie malware'u z działaniami rozciągniętymi w czasie. Seceon pełni rolę skutecznego środka ochrony przed atakami dzięki wymuszaniu polityk na firewall'u i zamykaniu kanałów komunikacji.
- Seceon pracuje w architekturze rozproszonej; wymaga jednego APE (Analytics & Policy Engine) w centrali i jednego lub więcej CCE (Collection & Control Engine) w wielu lokalizacjach Data Center. APE instaluje się na fizycznym sprzęcie, CEE wymaga 2-4 rdzeni VM.
- Seceon zapewnia Zero Trust Security; po identyfikacji alertu na poziomie „ważny/krytyczny" – udostępnia rekomendację i daje możliwość wykonania określonej polisy na kontrolerze domeny lub firewall'u w celu powstrzymania malware'u.



Asset groups that have had assets within the group register alerts.

- Seceon rośnie wraz z rozwojem firmy, jest elastyczny i zapewnia wysoki zwrot z inwestycji (ROI). Można zacząć od wysyłania przepływów i logów z krytycznej części Data Center, a potem rozbudowywać platformę o kolejne części DC. Architektura oparta jest na Big Data i może być rozszerzana horyzontalnie, co gwarantuje ochronę początkowej inwestycji.
- Seceon wykrywa pełzające, długotrwałe ataki typu APT dzięki skuteczności własnej techniki przetwarzania, wszechstronnemu wglądowi w to co dzieje się w Data Center i architekturze Big Data. Ponieważ obrona brzegowa jest nieskuteczna dla ataków celowych, Seceon OTM kontroluje przepływy sieciowe bez konieczności utrzymywania informacji o stanie każdego przepływu. Dla ataków APT Seceon utrzymuje wskaźniki kompromitacji (IOC) w szybkiej, skalowalnej, elastycznej i rozproszonej bazie danych.
- Seceon jest zdolny do identyfikacji zagrożeń wewnętrznych i wykrywania skompromitowanych uwierzytelnień.

Partner Seceon w Polsce:

Orion Instruments Polska

05-082 Latchorzew, ul. Warszawska 164

tel. 22 638 31 45, e-mail orion@orion.pl

więcej informacji: www.orion.pl