Odnajdywanie ukrytych zagrożeń

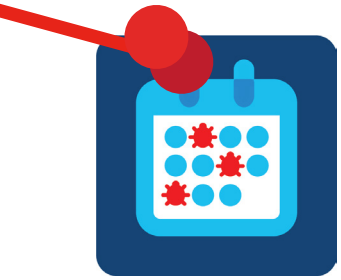
Włączenie aktywnego wyszukiwania zagrożeń do programu bezpieczeństwa

CISCO

Spis treści

Wprowadzenie

Jest godzina pierwsza i wszystko jest dobrze. Wracasz z obiadu, a jako starszy badacz ds. zagrożeń w firmie, właśnie przeglądasz panele SIEM w celu sprawdzenia potencjalnych alertów bezpieczeństwa. Nic niezwykłego nie przykuło twojej uwagi. Niedawny projekt automatyzacji drastycznie skrócił czas potrzebny do wykonania tego zadania, co pozwala zwolnić cenny czas, który byłby wcześniej poświęcony na wykonywanie zadań wykonywanych ręcznie. Co więc można z tym czasem zrobić?



Polowanie na zagrożenia to aktywność, którą celowo planujesz i regularnie realizujesz, aby wzmocnić swoją pozycję w zakresie bezpieczeństwa.

Być może nadszedł czas, aby rozważyć aktywne wyszukiwanie zagrożeń. Polowanie na zagrożenia wykracza poza to, o czym już wiem, lub zostaliśmy powiadomieni. Oprogramowanie zabezpieczające ostrzega nas tylko przed złośliwymi zagrożeniami i zachowaniami, które znamy. Polowanie na zagrożenia jest to wyruszenie w nieznane.

Polowanie na zagrożenia to aktywne ćwiczenie z zakresu bezpieczeństwa, mające na celu znalezienie i wykorzenienie atakujących, którzy niezauważenie przeniknęli do naszego środowiska. Stoi w opozycji dotradycyjnego dochodzenia oraz odpowiedzi na zagrożenia, o których zostaliśmy poinformowani dzięki alertom, pojawiającym się po wykryciu potencjalnie złośliwej aktywności.

Rzeczywistość

Oczywiście scenariusz ten może brzmieć nieco wyidealizowanie. Kto naprawdę ma w dzisiejszych czasach wolne popołudnie? Zawsze jest coś innego, co trzeba zrobić, prawda?

W rzeczywistości, przez większość czasu, polowanie na zagrożenia nie jest czynnością, którą można „po prostu” zrobić w wolnym czasie. Nie jest to również coś, co robisz w toku dochodzenia jako kolejny krok w procedurze. Jest to raczej czynność, którą celowo planujesz i regularnie realizujesz, aby pomóc Ci wzmocnić swoją pozycję w zakresie bezpieczeństwa. Zasadniczo jest to kolejne narzędzie w twoim arsenale bezpieczeństwa.

Wiadomo, harmonogram zawsze jest zapakowany, a lista zadań do wykonania jest tak długa, jak twoja ręka. Istnieje jednak kilka kluczowych korzyści, płynących z aktywnego odnajdywania zagrożeń.

Moment w czasie

Identyfikacja i eliminacja nieznanych i niezauważonych zagrożeń jest zawsze dobra. Nawet wtedy, gdy nie wykryje się konkretnego zagrożenia, ćwiczenia związane z odnajdywaniem zagrożeń często identyfikują zagrożenia w twoim środowisku, które można wyeliminować. Ostatecznie regularne polowanie na zagrożenia może znacząco zmniejszyć możliwości ataku przyszłym, złośliwym podmiotom.

Istnieje także wiele możliwości, które można wykorzystać, aby wykorzystać nauki wyciągnięte z procesu odnajdywania zagrożeń. Ćwiczenia te mogą zidentyfikować obszary, w których mogą być wprowadzane ostrzeżenia o złośliwym zachowaniu, a także obszary, w których można opracować automatyzację, aby powtórzyć określone zadanie wyszukujące zagrożenia. Możesz przeprowadzić dodatkowe zadania związane z polowaniem na zagrożenia, budować i rozszerzać swoje zabezpieczenia i możliwości.

Rozpoczęcie

Celem tego dokumentu jest przyjrzenie się procesowi polowania na zagrożenia. Będziemy badać tajniki polowania na zagrożenia, przyjrzymy się dlaczego warto to robić, kto powinien brać udział oraz czemu, gdzie i kiedy należy zajrzeć.

Istnieje również szereg dyscyplin bezpieczeństwa, z czynnościami, które pokrywają się z polowaniem na zagrożenia. Będziemy porównywać i wyróżniać dyscypliny, pokazując, że polowanie na zagrożenia jest podobne do innych czynności, oraz że zasługuje na miejsce w twoim arsenale bezpieczeństwa.

Na koniec omówimy, w jaki sposób można tworzyć skuteczne kampanie związane z polowaniem na zagrożenia w organizacji. Jedną z najtrudniejszych rzeczy do ustalenia jest to, gdzie zacząć. Zaczyniemy od prostych kroków, które można podjąć, aby zbudować lepszą pozycję wyjściową podczas polowanie na zagrożenia, dodatkowo wzmacniając bezpieczeństwo organizacji.

Aktywne odnajdywanie zagrożeń a _____

Jeśli chodzi o dyscypliny bezpieczeństwa, polowanie na zagrożenia jest stosunkowo młodą specjalnością. Jest więc normalnym, że pewne czynności będą się pokrywać. W rzeczywistości wielu ludzi obecnie biorących udział w aktywnym odnajdywaniu zagrożeń posiada doświadczenie pracy w innych rolach. Poniżej przedstawiono kilka szybkich porównań z innymi dyscyplinami.

Reagowanie na zdarzenia

Doświadczenia w tej roli są prawdopodobnie najbardziej podobne do aktywnego wyszukiwania zagrożeń. Obydwie dyscypliny muszą usunąć bezpośrednie zagrożenie w danym środowisku. Podstawową różnicą jest to, że reakcja na incydenty jest reaktywna – wiadomo, że coś jest w sieci, lub przynajmniej, że coś lub ktoś próbowało uzyskać dostęp do sieci - wiemy to dzięki alertom zabezpieczeń, zachowaniu sieci lub punktu końcowego lub tym podobnym indydentom. Aktywne wyszukiwanie zagrożeń natomiast nie musi posiadać żadnych dowodów na istniejące zagrożenie. To po prostu aktywne wszukiwanie czegoś co potencjalnie istnieje, a nie próba powstrzymania czegoś, o czym wiesz, że istnieje.

Testy penetracyjne

Polowanie na zagrożenia i testy penetracyjnei również mają pewne podobieństwa. W obydwu przypadkach staramy się odnaleźć słabe punkty w sieci. Jednakże testy penetracyjne zazwyczaj szukają problemów z konfiguracją lub znanych luk w zabezpieczeniach w celu uzyskania dostępu do sieci lub poufnych informacji. Celem polowania na zagrożenia nie jest konieczność uzyskania do czegoś dostępu, ale raczej zidentyfikowanie ukrytych zagrożeń występujących w środowisku, wyeliminowanie ich i ustanowienie zasad zapobiegających im w przyszłości.

Zarządzanie ryzykiem

Ideą zarządzania ryzykiem jest określenie słabych punktów w sieci lub w systemach, określenie ich wagi, priorytetyzacja, a następnie podejmowanie odpowiednich kroków w celu ich skorygowania. Może to oznaczać identyfikację źródeł zagrożeń. Polowanie na zagrożenia może pomóc przeprowadzić proces oceny ryzyka. Jednak takie oceny zazwyczaj obejmują znacznie więcej niż samo polowanie na zagrożenia, a jednocześnie uwzględniają wszystkie potencjalne zagrożenia, zarówno znane, jak i nieznane.

Ocena możliwości naruszenia bezpieczeństwa

Podobnie jak w przypadku polowania na zagrożenia, Ocena możliwości naruszenia bezpieczeństwa polega na ustaleniu, czy sieć została naruszona przez nieznane elementy. Jest to jednak znacznie szersze działanie niż polowanie na zagrożenia. Podczas oceny możliwości naruszenia bezpieczeństwa różne narzędzia są instalowane w całej sieci, patrząc przekrojowo w poszukiwaniu czegoś niezwykłego. Natomiast polowanie na zagrożenia zaczyna się od bardzo konkretnego pomysłu lub scenariusza i się na nim skupia.

5 pytań

Podczas ustanawiania ćwiczeń z aktywnego odnajdywania zagrożeń ustalenei punktu wyjścia może być trudne. Zadaj sobie 5 pytań, często stosowanych w dziennikarstwie. To dobry sposób na rozpoczęcie procesu.

Twój zespół odpowiedzialny za polowanie na zagrożenia będzie prawdopodobnie pokrywał się z zespołem reagowania na incydenty, a polowanie na zagrożenia wyostrza umiejętności i czasy reakcji w obliczu rzeczywistego incydentu.

Dlaczego?

Wyższe nakłady finansowe na proaktywne wykrywanie zagrożeń mogą znacząco wzmocnić posturę bezpieczeństwa organizacji. Naprawdę istnieją zorganizowani, wykwalifikowani i dobrze finansowani napastnicy. Czasem grupa taka nie spocznie, dopóki nie znajdzie luki w systemie, którą będzie mogła wykorzystać. Niestety, nie da się odkryć każdej takiej luki, nawet z najlepszymi narzędziami bezpieczeństwa. W tym miejscu aktywne odnajdywanie zagrożeń – jego głównym zadaniem jest znalezienie dokładnie takiego typu ataków.

Dodatkowym elementem jest to, że wykonywanie takich ćwiczeń pozwala lepiej poznać narzędzia i techniki, które są niezwykle ważne w przypadku wystąpienia ataku lub naruszenia bezpieczeństwa. twój zespół odpowiedzialny za polowanie na zagrożenia będzie prawdopodobnie pokrywał się z zespołem reagowania na incydenty, a polowanie na zagrożenia wyostrza umiejętności i czasy reakcji w obliczu rzeczywistego incydentu. Można ją traktować jako ćwiczenia przygotowujące do momentu, gdy coś pójdzie nie tak.

Kto?

Budowanie zespołu zajmującego się polowaniem na zagrożenia może wydawać się uciążliwe, tak samo jak trudnym jest złożenie drużyny superbohaterów w celu pokonania wspólnego „złego". Trzeba zebrać ludzi o różnej przeszłości, umiejętnościach, i możliwościach.

Jeśli pracujesz w dużej organizacji, to pierwszym krokiem może być po prostu ustalenie regularnego spotkania dla całego zespołu, podczas którego odbywać się będzie planowanie, wykonywanie i raportowanie nt. podjętych działań. Jednakże, jeśli pracujesz w małej firmie z tylko kilkoma (być może tylko jednym!) pracownikami działu IT, może się to okazać trudniejsze. Mając to na względzie, warto zwrócić się o pomoc do ekspertów zewnętrznych. Ma to dobre i złe strony. Jako plus zapisać można, że najprawdopodobniej uzyskasz dostęp do umiejętności i osób, które na pewno przydadzą się w procesie aktywnego szukania zagrożeń. Jednakże zewnętrzny zespół zajmujący się polowaniem na zagrożenia nie będzie tak dobrze zaznajomiony z obsługą sieci jak normalny pracownik.

Niezależnie od tego, w celu przeprowadzenia procesu odnajdywania zagrożeń, istnieje mieszanka podstawowych umiejętności niezbędnych w zespole:

- **Znajomość punktów końcowych i bezpieczeństwa sieci**

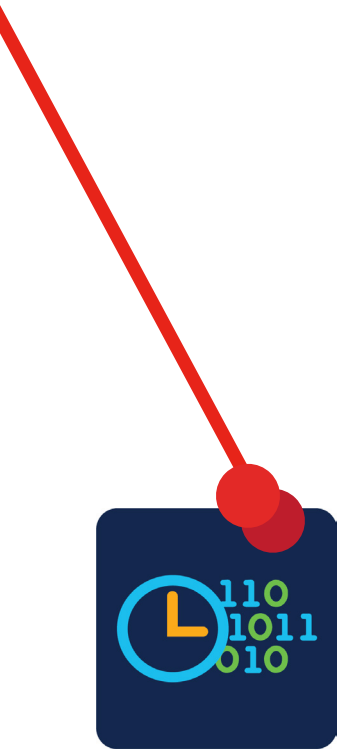
  To oczywiste. Potrzebujesz doświadczonych członków zespołu SOC lub IT, którzy dysponują rozległą i dogłębną wiedzą na temat zagadnień związanych z bezpieczeństwem i najlepszych praktyk.

- **Zrozumienie analityki danych**

  Często polowanie na zagrożenia wymaga wyciągania złośliwych wzorców z nieprzetworzonych danych. Zrozumienie analiz statystycznych pomoże w ustaleniu wzorców danych. Wizualizacja danych jest równie ważna, aby wykrywać i udostępniać znalezione anomalie.

- **Wrodzona ciekawość**

  Aktywne odnajdywanie zagrożeń nie jest działaniem wedle ustalonego wzorca. Czasami można przyrównać je do procesu artystycznego. Wymaga pewnej ilości kreatywnego myślenia, łączącego pozornie niepowiązane elementy lub zadającego sobie pytanie „Co by było, gdyby..."



Zanim można będzie rozpocząć aktywne odnajdywanie zagrożeń, musisz upewnić się, że masz włączone odpowiednie procesy rejestracyjne, niezbędne w tymże procesie.

Jedno jest pewne – z perspektywy specjalisty ds. bezpieczeństwa, aktywne polowanie na zagrożenia to dobra zabawa. Polowanie na zagrożenia daje ludziom w dziale SOC lub IT przerwę od codziennych reaktywnych działań oraz otwiera szansę, aby przejść do ofensywy. Takie aktywne, ciekawe zadania dla pracowników często mogą prowadzić do wyższych wskaźników retencji wśród pracowników SOC, zachowując ich w obszarze, w którym wykwalifikowany personel jest wysoce mobilny i ciężki do znalezienia.

Kiedy wyruszyć na polowanie?

Ostatecznie najbardziej udanym polowaniem jest dobrze zaplanowane. Musisz określić zakres poszukiwań, określić jasne cele i wyznaczyć blok czasu na przeprowadzenie polowania. Gdy skończysz, musisz ocenić kroki, które poprawią twoją pozycję w zakresie bezpieczeństwa oraz rozpisać listy kroków bezpieczeństwa, aby w przyszłości czerpać wiedzę z osiągniętych wyników.

Gdy podejrzewasz, że niebezpieczne zachowanie mogło mieć miejsce, być może przeprowadzenie aktywnego poszukiwania zagrożeń to dobry pomysł.

- **Czy użytkownik pobiera o wiele więcej danych w danym dniu niż zwykle?**
- **Czy użytkownik próbuje zalogować się do systemu, do którego nie ma dostępu?**
- **Czy administrator czyści dzienniki bash?**

Wiele z tych zachowań może wskazywać na działania złośliwego oprogramowania, które zainfekowało urządzenie. Jest to dość dobry punkt wyjściowy na rozpoczęcie polowania na zagrożenia.

Zdarzają się też sytuacje, w których polowanie na zagrożenia może nie być czynnością zaplanowaną. Czy nie zdarzyło się nigdy, aby news dot. bezpieczeństwa cybernetycznego, który przykuł uwagę CIO, sprowokował go do wysłania e-maila lub rozmowy telefonicznej z pytaniem, czy firma jest narażona na ataki? Jest to zasadne pytanie – co więcej, posiadanie wypróbowanego procesu wyszukiwania luk w zabezpieczeniach pozwala zaoszczędzić znaczną ilość czasu i zasobów.

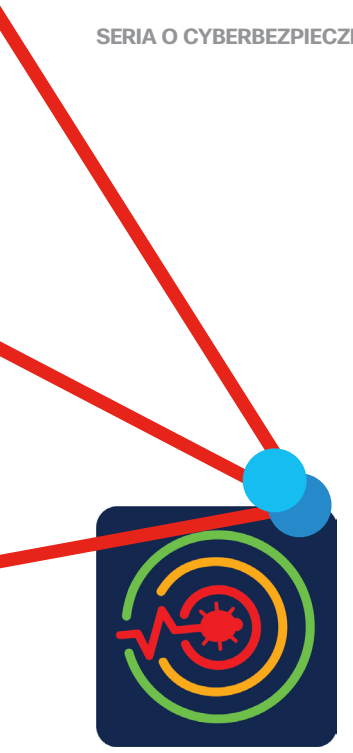
Co i gdzie?

Ostatecznie, to dane mają kluczowe znaczenie. Zanim można będzie rozpocząć aktywne odnajdywanie zagrożeń, musisz upewnić się, że masz włączone odpowiednie procesy rejestracyjne, niezbędne w tymże procesie. Jeśli nie widzisz, co dzieje się w systemach, to nie możesz na to działanie odpowiedzieć.

Wybór systemów do przebadania zależeć będzie od zakresu polowania – jedno polowanie może być skoncentrować się na punktach końcowych w dziale finansów, a inne na serwerach www. W niektórych przypadkach możesz nawet zainstalować narzędzia w środowisku, aby monitorować określone typy ruchu. Dzienniki ściągnięte przez te tymczasowe systemy zostaną wykorzystane w polowaniu.

Oczywiście włączenie rejestrowania może szybko wypełnić zasoby pamięci masowej, a gromadzenie dzienników może łatwo zająć zbyt wiele czasu zaangażowanego zespołu. Może to wymagać oddzielenia zasobów fizycznych do przechowywania dzienników i konfigurowania podstawowej automatyzacji w celu ich wysłania. W perspektywie krótkoterminowej konieczne może być selektywne konfigurowanie systemów, których zapisy będą rejestrowane. Korzystanie z narzędzi, takich jak informacje o zabezpieczeniach i oprogramowanie do zarządzania zdarzeniami (SIEM), może znacznie ułatwić analizowanie dzienników.

Po kilku pierwszych ćwiczeniach związanych z polowaniem na zagrożenia wynik może zawierać listę pytań, na które nie można odpowiedzieć na podstawie dostępnych dzienników. Z czasem wszystko stanie się jaśniejsze. Będzie można powiedzeć, które systemy muszą mieć włączone logowanie i na jakim poziomie, w celu uzyskania pożądanych wyników.



Celem ćwiczenia związanego z polowaniem na zagrożenia powinno być wykrycie wartości TTP ataku. Jest to najbardziej wartościowy element wiedzy o atakującym, najtrudniejszy do zastąpienia.

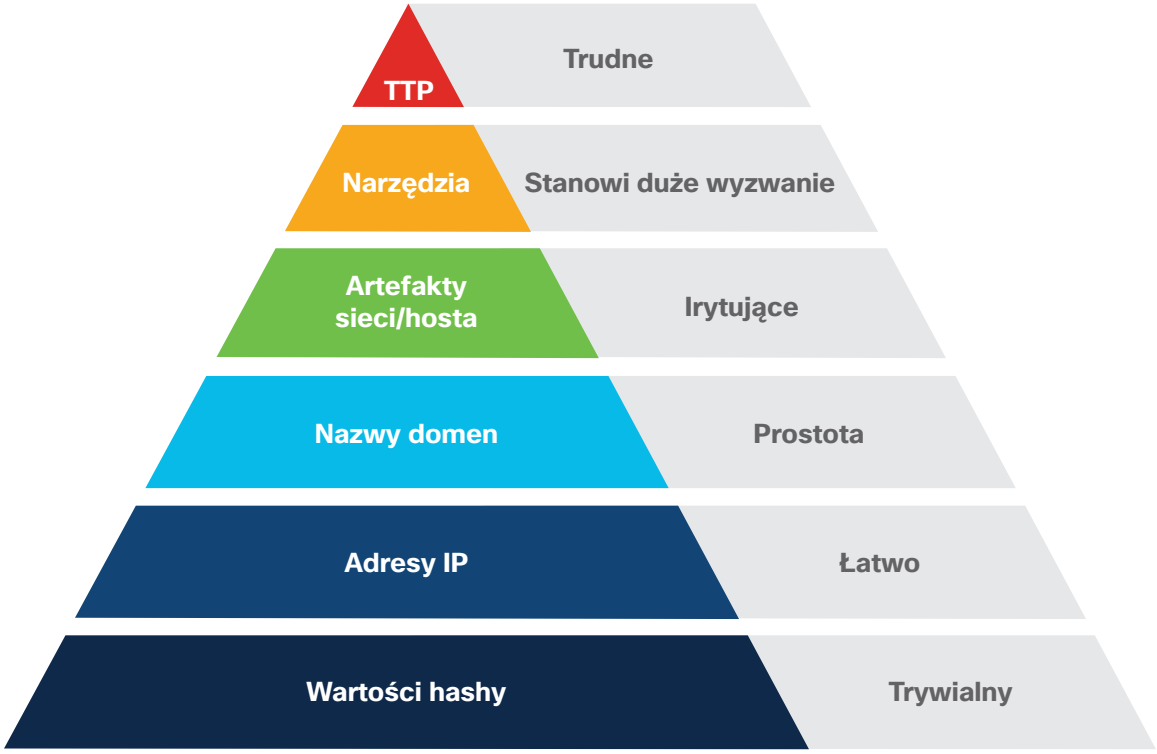
Pyramid of Pain (Piramida bólu)

Badacz bezpieczeństwa David Blanco wymyślił podejście zatytułowane The Pyramid of Pain (Piramida bólu), w którym opisano, jak sprawić, aby cyberprzestępcy mieli jak największe trudności podczas ataku na sieć. Każda z sześciu warstw przedstawia różne podejście, które możesz zastosować, zaczynając od najprostego aż do najtrudniejszych.

Na przykład u podstawy piramidy znajdują się hashe. Pliki opatrzone znanymi złośliwymi hashami są łatwe do wykrycia, a także łatwe do zastąpienia przez cyberprzestępców. To samo dotyczy adresów IP. Zajmuje to jednak trochę więcej pracy (zarówno znalezienie, jak i zastąpienie) stąd fragment piramidy jest mniejszy. Domeny są nieco trudniejsze, a artefakty sieciowe jeszcze trudniejsze itd.

Celem ćwiczenia związanego z polowaniem na zagrożenia powinno być wykrycie taktyki, technik i procedur (TTPs) osoby atakującej. Są one najbardziej cenne, ponieważ są trudne do zastąpienia przez osobę atakującą. To często najtrudniejsze i/lub najbardziej czasochłonne zadanie. Dzieje się tak głównie dlatego, że wymaga ono porównywania punktów danych z różnych zbiorów i wykonania połączeń, w których relacja nie jest widoczna na początku.

W ten sposób możesz zmusić cyberprzestępców do poświęcenia większej ilości zasobów na atakowanie sieci, utrudniając tym samym i zwiększając prawdopodobieństwo, że zostaną schwytani w ten sposób. Ostatecznym celem „piramidy bólu" jest to, żeby postępując zgodnie z zasadami, twoja sieć staje się tak trudna, że cyberprzestępcy przechodzą do innych, prostszych celów.



Źródło: David J. Bianca, blog osobisty

Jak polować

Jeśli chodzi o sposób działania, istnieje wiele sposobów, aby podejść do ćwiczenia związanego z aktywnym wyszukiwaniem zagrożeń. To, jak dokładne będzie wyszukiwanie, zależy od dostępnych zasobów i umiejętności.

W dalszej części zaczniemy od prostych, podstawowych sposobów na rozpoczęcie polowania na zagrożenia, a następnie będziemy zapoznawać się z tymi bardziej złożonymi. Chodzi o to, żeby po każdym ćwiczeniu można było opierać się na tym, czego już się nauczono. Tworzenie list czynności, automatyzacja oraz zmiany zasad w razie potrzeby – wszystko to daje podstawę do przechodzenia na bardziej zaawansowane techniki.

Analizowanie rejestrów

Zdarza się, że najprostsze aktywne wyszukiwanie zagrożeń wynika z badań lub raportów na temat nowo odkrytych zagrożeń. Powszechną praktyką jest uwzględnienie wskaźników naruszenia bezpieczeństwa (IOC) wraz z wykorzystywaniem wyników badań z innych źródeł. Te punkty danych składają się zazwyczaj z adresów IP, adresów oraz URL, hashy, lub innych IOC, które stanowią zagrożenie.

Jednym z najprostszych sposobów na rozpoczęcie ćwiczeń związanych z polowaniem na zagrożenia jest sprawdzenie dzienników z systemów wobec zapisów IOC. Narzędzia wiersza polecenia lub proste skrypty wystarczą do rozpoczęcia pracy. Korzystanie z SIEM jest inną metodą porównania IOC do logów. Istnieje również więcej zaawansowanych produktów z domeny bezpieczeństwa, które mogą pomóc w ułatwieniu polowania na zagrożenia, umożliwiając kopiowanie i wklejanie IOC do pulpitu nawigacyjnego w celu sprawdzenia, czy wystąpiły wcześniej w danym środowisku.

Gdy zapoznasz się już z tymi działaniami, nadejdzie czas, aby zanurkować głębiej w logi i zacząć odkrywać nowe IOC, które mogą się tam znaleźć. W tym miejscu wchodzą w grę umiejętności analizy danych. Zastosowanie modeli statystycznych podczas analizy dzienników, takich jak klastrowanie lub rozkład częstotliwości, może rzucić trochę światła na anomalie. Docelowo chcesz dotrzeć na szczyt Piramidy bólu i zidentyfikować TTP atakującego.

Polowanie na zagrożenia w działaniu

Jeff Bollingera zarządza badaniami bezpieczeństwa dla CSIRT w Cisco. Poniżej znajduje się jego historia związana z polowaniem na zagrożenia, wykonywana przez jego zespół.

„Przeglądając historyczne dane punktów końcowych Cisco AMP dla wskaźników naruszenia bezpieczeństwa, widzieliśmy podejrzany binarny dropper binarny, który został usunięty przez użytkownika.

Udało nam się odzyskać plik binarny poprzez przywrócenie pojedynczego pliku z (korporacyjnego) archiwum kopii zapasowych i udało nam się odwrócić go i wyodrębnić dodatkowe wskaźniki (nazwy hostów C2), które następnie zastosowano do wszystkich naszych telemetrycznych sieci.

Przyniosło to dodatkowe hosty dotknięte problemem, które nie odpowiedziały na pierwotny hash droppera.”

Nawet jeśli jesteś doświadczonym weteranem w zespole, nie myśl, że widziałeś to wszystko wcześniej. Zamiast tego spróbuj udowodnić, że rzeczywiście nie jest to zagrożenie. Jeśli nie możesz tego zrobić od ręki, należy szukać głębiej.

Testowanie teorii

Niektórzy mogą twierdzić, proste sprawdzanie dzienników wobec znanych IOC nie jest prawdziwym polowaniem na zagrożenia. Wedle takich teorii, po prostu dopasowuje się elementy jeden do jednego. W takich przypadkach, aby zakwalifikować działanie jako polowanie na zagrożenia, trzeba kopać głębiej.

Właśnie tam kreatywność odgrywa ważną rolę. Musisz wydedukować, gdzie może znajdować się zagrożenie, jakie będą wektory ataku oraz jakie techniki wykorzystano.

- **Przeczytaj informacje o bezpieczeństwie**

  Najnowsze informacje na temat zagrożeń mogą być pełne materiałów pomagających rozpoczęcie poszukiwań. Na przykład, jeśli w niedawno ujawnionym procesie systemu Windows wystąpiła Krytyczna luka w zabezpieczeniach, sprawdź, czy wokół tego procesu nie wystąpił jakiś dziwny rodzaj działalności. Oczywiście należy zwrócić szczególną uwagę na wiadomości dot. branży, w której się obracasz. Na przykład, jeśli pracujesz w lotnictwie, oprogramowanie kradnące numery kart kredytowych nie będzie miało wysokiego priorytetu. Z drugiej strony, jeśli pracujesz w bankowości, zagrożenie atakujące ICS nie będzie mieć pewnie zastosowania.

- **Zapoznaj się z raportami o dziwnym zachowaniu**

  Badaj nietypowe raporty o aktywności pracowników. Czy śpiące systemy budzą się nagle w nocy? Zbadaj, czym jest to spowodowane. Czy któryś dział poinformował cię, że znaleziono dane wewnętrzne na zewnętrznym źródle? Idź za tropem wycieku danych.

- **Przyjrzyj się temu co normalne, aby odnaleźć to, co nienormalne.**

  Nietypowa aktywność jest dobrym punktem wyjścia, ale nie zawsze jest łatwa do wykrycia. Czasami trzeba przekopać się przez stertę danych, aby ją wytropić. Zapoznaj się z konkretną aktywnością pod kątem użycia jej w nieodpowiednim celu. Na przykład:

  - Szukaj długich połączeń sieciowych, które mogą być oznaką wycieku danych. Odfiltruj wyniki spodziewane i sprawdź, czy któryś z tych, którzy zostały, wygląda podejrzanie.
  - Spójrz na zwiększenie obłożenia procesora i na procesy, które to spowodowały, co może wskazywać na kopalnie kryptowalut czy logowanie zapisów przez złośliwe oprogramowanie. Odsiej wyniki spodziewane, a przyjrzyj się tym, których nie powinno być.
  - Jakiego rodzaju pliki są pobierane przez narzędzie BITSAdmin? Może ono zostać wykorzystane do znalezienia złośliwych narzędzi, ponieważ wiele zagrożeń wykorzystuje narzędzia lokalne do maskowania swoich działań. Odsiej te pobrane pliki, których się spodziewasz, a przyjrzyj się pozostałym.
  - Zapoznaj się z zaplanowanymi zadaniami. Cyberprzestępcy mogą dodawać własne zadania w celu rozpoczęcia niektórych złośliwych działań. Czy są jakieś działania, które nie są uruchamiane przez administratorów systemu? Zbadaj wszystkie, które wydają się podejrzane.

Wszelkie przypadki, w których zachowanie wydaje się niezwykłe, są głównymi obszarami, które trzeba zbadać i znaleźć ich przyczynę. Jednak ważne jest, aby badać znalezione dane ostrożnie. Tylko dlatego, że coś wygląda dziwnie, niekoniecznie oznacza, że jest złośliwym oprogramowaniem. Przed wyciągnięciem wniosków należy porównać wyniki z innymi źródłami danych. Nawet jeśli jesteś doświadczonym weteranem w zespole, nie myśl, że widziałeś to wszystko wcześniej. Zamiast tego spróbuj udowodnić, że rzeczywiście nie jest to zagrożenie. Jeśli nie możesz tego zrobić od ręki, należy szukać głębiej.

Pójście do źródła

Udało Ci się zidentyfikować zagrożenie w sieci, wskazać, co pozwoliło mu uzyskać dostęp i podjąć środki, aby zapobiec jego ponownemu wystąpieniu. Jednak podczas kolejnego wyszukiwania, okazuje się, że cyberprzestępcy znaleźli już inny sposób.

Jeśli twoja organizacja jest stale atakowana, warto przeanalizować, kto atakuje, jaka infrastruktura jest używana oraz spróbować zakończyć działalność grupy.

Nie jest to jednak sugestia, aby samemu przeprowadzać ofensywne działania hakerskie. Zostanie hakerem może być kuszące, ale istnieje wiele problemów związanych z przejściem na ciemną stronę.

Jeśli zaatakujesz złośliwą infrastrukturę, istnieje duża szansa, że cyberprzestępcy zauważą twoje działanie i wyprowadzą kontratak. Jednak ich nową motywacją może już być nie kradzież informacji, ale raczej zemsta – wyłączenie lub zniszczenie systemów.

Innym powodem, dla którego nie należy się włamywać, jest to, że w większości lokalizacji na świecie jest to działanie nielegalne. Pomimo faktu, że teoretycznie atakowano by osoby prowadzące nielegalne działania, nadal mówimy o odpowiadaniu wetem za wet.

Dobrą wiadomością jest to, że jest jeszcze mnóstwo innych rzeczy, które można zrobić. IOC ataku może ujawnić wiele informacji o cyberprzestępcach, nawet bez konieczności podłączania się do ich sieci.

Najlepszym podejściem do zwalczania złośliwych podmiotów jest zebranie wszelkich danych IOC, które można zdobyć, od hashy aż po TTP, stworzenie profilu atakującego, a następnie przekazanie tych danych odpowiednim organom ścigania. Organy ścigania mają najlepsze możliwości na zakończenie atak.

Najlepsze podejście aby pokonać złośliwe oprogramowanie: zbierz wszystkie IOC, które możesz odkryć, zbuduj profil atakującego i przekaż te dane odpowiednim organom ścigania.

Dla większości podmiotów nie jest to jednak proces, który da się łatwo uruchomić. W rezultacie, lwia część organizacji może i powinna opierać się na zespołach zajmujących się badaniem bezpieczeństwa zewnętrznego, które przeprowadzą śledztwo, gdy będzie to potrzebne. Organizacje zajmujące się informacjami o zagrożeniach, takie jak Talos Intelligence Cisco Incident Response, są pomocne w takich przypadkach.

Wykorzystanie polowanie na zagrożenia

Sean Mason, dyrektor ds. zarządzania zagrożeniami w Cisco Security Advisory Services, zastanawia się nad tym, jak jego zespoły wykorzystują polowanie na zagrożenia w firmie Cisco.

„Naprawdę zacząłem rozumieć i doceniać aktywne odnajdywanie zagrożeń podczas RSA Hack w 2011 roku. Brałem udział w spotkaniu, rozmawiając o tym, jak możemy wykryć tego typu zagrożenia. Pozwoliło nam to uzyskać nową perspektywę. Zdaliśmy sobie także sprawę z tego, czego wcześniej nie widzieliśmy. Z biegiem lat różne zespoły, w których byłem, korzystały z polowania na wiele różnych sposobów: albo proaktywnie po niekreślonym przeczuciu, reagując na incydent lub po zapoznaniu się z najnowszymi wiadomościami dotyczącymi bezpieczeństwa w IT. Mogę szczerze powiedzieć, że po ponad ośmiu latach wykorzystania procesu polowania na zagrożenia w różnych możliwościach, uważam ten proces za kluczowy element każdego skutecznego programu bezpieczeństwa”.

Następstwa

Ważne jest, aby identyfikować i eliminować zagrożenia ukryte w twojej sieci, dowiedzieć się, w jaki sposób przestępca dostał się do sieci, oraz podjąć kroki, aby zapobiec przyszłym atakom. Zaplanuj spotkanie po zakończeniu działania, aby omówić wyniki. Pokaż, co zostało znalezione i omów, co należy zrobić, aby naprawić sytuację. Następnie wdróż zmiany zasad sieciowych.

Niekiedy nawet najlepsze działania mające na celu identyfikację zagrożeń okażą się nieskuteczne. Korzyścią jest wtedy wiedza o tym, że zagrożenia zostały zanalizowane i twoja organizacja jest bezpieczna.

Czasami nie chodzi o znajdowanie zagrożenia, ale raczej o ujawnianie słabych punktów organizacji. Skuteczna kampania dotycząca aktywnego odnajdywania zagrożeń może ujawnić nieprawidłowo skonfigurowany serwer lub naruszenie zasad, które wymaga skorygowania. Jak dziwne mogłoby się to wydawać, niekiedy najlepsze działania mające na celu identyfikację zagrożeń okażą się nieskuteczne. Korzyścią jest wtedy wiedza o tym, że zagrożenia zostały zanalizowane i twoja organizacja jest bezpieczna.

Dodanie automatyzacji to kolejny krytyczny krok do poszukiwań zagrożeniach. Po zakończeniu procesu ważne jest, aby sprawdzać okresowo, czy działania, które zostały odkryte, ponowiły się. Zamień odkryte informacje w proces, który można uruchomić ponownie. Skonfiguruj pułapkę z alertami. Z biegiem czasu działania zostaną dodane do listy bezpieczeństwa.

Wnioski

Nie ma możliwości dowiedzenia się, czy twoja sieć jest całkowicie wolna od zagrożeń. Nie oznacza to jednak, że poszukiwanie luk w zabezpieczeniach nie ma sensu. Zaletą polowania na zagrożenia, oprócz wykorzenienia samych zagrożeń, które uda się odkryć, jest to, że można rozbudowywać swoje bezpieczeństwo.

Spójrz na polowanie na zagrożenia tak, jak na budowanie ściany. Budując dom, zaczynasz od pierwszego pierścienia z cegieł. Następnie dodajesz: zaprawę aby pozostały na swoim miejscu. Potem dodajesz kolejną warstwę. Nakładasz warstwę po warstwie, aby stworzyć ścianę.

W przypadku aktywnego odnajdywania zagrożeń, pierwszym pierścieniem mogłyby być np. procesy rejestrowania i zapisywania ataków. Zaprawa to automatyzacja, która sprawi, że rejestry działań spływać będą regularnie. Kolejną warstwą jest porównywanie dzienników z IOC. Zautomatyzuj te procesy, aby utrzymać cegły na miejscu. Kontynuuj naukę dzięki warstwom analityki danych, testowaniu teorii itd.

Wkrótce uda Ci się zbudować silny i stabilny proces polowania na zagrożenia, który da Ci pewność, że Twoja organizacja jest wolna od zagrożeń.

Narzędzia do polowania na zagrożenia

Poniżej przedstawiono kilka zalecanych narzędzi, które można wykorzystać do polowania na zagrożenia. Nie jest to kompletna lista, ale pomoże Ci zacząć.

Cisco Threat Response

Rozwiązanie Cisco Threat Response automatyzuje integrację niektórych informacji od Cisco Security, wykorzystuje analizę zagrożeń od Cisco Talos oraz z innych źródeł, analizując zdarzenia w domenie bezpieczeństwa, aby automatycznie badać wskaźniki zagrożenia (IOCs) i szybko potwierdzać (bądź nie) samo zagrożenie. Cisco Threat Response umożliwia zbieranie i przechowywanie najważniejszych informacji dotyczących dochodzeń, a także zarządzanie i dokumentowanie postępów oraz wniosków.

Cisco Threat Grid

Rozwiązanie Threat Grid łączy zaawansowaną piaskownicę (tzw. sandbox) z informacjami o zagrożeniach w jednym ujednoliconym rozwiązaniu chroniącym organizację przed złośliwym oprogramowaniem. Dzięki solidnej, bogatej w kontekst bazie wiedzy o złośliwym oprogramowaniu zrozumiesz, jak działa złośliwe oprogramowanie, jak duże stanowi zagrożenie i jak się przed nim chronić.

Cisco Stealthwatch

Cisco Stealthwatch to kompleksowy wgląd w informacje oraz rozwiązania w zakresie ruchu sieciowego i analizy bezpieczeństwa w chmurze. Wykrywa złośliwe oprogramowanie w szyfrowanym ruchu danych bez konieczności deszyfracji. To zaawansowane wykrywanie i szybsza reakcja na zagrożenia, a także uproszczona segmentacja sieci za sprawą wielowarstwowego uczenia maszynowego i zaawansowanego modelowania zachowań na przestrzeni całej sieci. Dzięki zaawansowanym analizom behawioralnym możesz dowiedzieć się, kto znajduje się w Twojej sieci lub w infrastrukturze chmury publicznej oraz co robi.

Rozwiązanie Cisco Advanced Malware Protection for Endpoints

Rozwiązanie AMP zapewnia nie tylko ochronę punktów końcowych, ale także pomaga w analizie złośliwego oprogramowania i proaktywnym odnajdywaniuzagrożeń. Niezawodne funkcje wyszukiwania AMP umożliwiają odnajdywanie różnych informacji, takich jak plik, hash, adres URL, adres IP, klucze rejestru, użytkownicy, procesy, aplikacje i wiele innych. Może również pokazać cykl życia pliku w Twoim środowisku, pod pierwszego wystąpienia do tego, co z nim zrobiono w punkcie końcowym oraz inne informacje.

Umbrella Investigate

Badanie zapewnia najbardziej pełny wgląd w relacje i ewolucję domen, adresów IP, systemów autonomicznych (ASN) i hashy plików. Dostępne za pośrednictwem konsoli internetowej i interfejsu API, bogate analizy Investigate zwiększają kontekst zabezpieczeń potrzebny do wykrycia i przewidzenia zagrożeń.

Zarządzanie informacjami i zdarzeniami bezpieczeństwa (SIEM)

Posiadanie SIEM jest kluczowym krokiem w zakresie prowadzenia działań związanych z polowaniem na zagrożenia, zwłaszcza gdy zaczynamy. Dobrze skonfigurowany SIEM może znacznie skrócić czas poświęcany na gromadzenie plików dziennika i przeprowadzać podstawową analizę. Przykłady znanych SIEMs to Splunk, IBM QRadari Exabeam.

Narzędzia do monitorowania punktów końcowych

Istnieje wiele dostępnych narzędzi do gromadzenia szczegółowych dzienników z punktów końcowych. Wbudowany w system Windows dziennik zdarzeń to dobry start, a bardziej złożone narzędzia, takie jak Sysmon i Process Monitor, mogą rozszerzyć możliwości rejestrowania. (Istnieją nawet wstępnie zbudowane konfiguracje, które pomogą Ci rozpocząć pracę). Na komputerach Apple Mac zapoznaj się z konsolą, aby wyświetlić dzienniki.

Analizatory pakietów

Są to narzędzia, które można wykorzystać do monitorowania ruchu sieciowego. Aplikacje, takie jak Wireshark i tcpdump oraz interfejsy API, takie jak PCAP, to popularne narzędzia do gromadzenia informacji o przesyłanych danych w całej sieci.

O serii o cyberbezpieczeństwie Cisco

W ciągu ostatniej dekady Cisco opublikowało wiele informacji na temat bezpieczeństwa i zagrożeń dla specjalistów zainteresowanych stanem globalnego cyberbezpieczeństwa. Te kompleksowe badania dostarczają szczegółowych danych na temat zagrożeń i ich następstw dla firm, a także wielu dobrych praktyk, mających na celu ochronę przed niepożądanymi skutkami wycieków danych.

W ramach nowego podejścia kierownictwo Cisco Security publikuje serię publikacji opartych na badaniach i danych pod nazwą Seria o cyberbezpieczeństwie Cisco. Rozszerzyliśmy liczbę tytułów, aby zawrzeć różne raporty dla specjalistów do spraw bezpieczeństwa o różnych zainteresowaniach. Wcześniejsza seria raportów z 2019 roku skupia się na dogłębnej ekspertyzie badań dotyczących zagrożeń i innowacji w branży bezpieczeństwa i zawiera Analizę porównawczą ochrony danych, Raport na temat zagrożenia i Analizę porównawczą Cisco, a także inne, które ukażą się w ciągu roku.

Aby uzyskać więcej informacji i dostęp do raportów oraz zarchiwizowanych wersji, odwiedź www.cisco.com/go/securityreports.

Centrala w Ameryce Północnej i Południowej
Cisco Systems, Inc.
San Jose (Kalifornia, USA)

Centrala dla krajów Azji i Pacyfiku
Cisco Systems (USA) Pte. Ltd.
Singapur

Centrala w Europie
Cisco Systems International BV, Amsterdam, Holandia

Firma Cisco ma ponad 200 biur na całym świecie. Pełną listę adresów, numerów telefonów oraz faksów można znaleźć na stronie internetowej firmy Cisco pod adresem: www.cisco.com/go/offices.

Opublikowano w sierpniu 2019 roku

THRT_05_0819_r1