Bezpieczeństwo

Sposoby stosowania uczenia maszynowego w zaawansowanych rozwiązaniach bezpieczeństwa Cisco

Ostatnio dużo mówi się o stosowaniu uczenia maszynowego w dziedzinie cyberbezpieczeństwa. Wygląda na to, że obie te kwestie są ze sobą nierozdzielnie powiązane. Wiele organizacji, z którymi rozmawiałem w ciągu ostatnich kilku miesięcy, jest zainteresowanych nauką, ale często po rozpoczęciu badań są jeszcze bardziej zdezorientowane. Na początek proponuję zapoznać się z wpisem Przełamujemy stereotypy: uczenie maszynowe a bezpieczeństwo punktów końcowych.

W Cisco korzystamy z uczenia maszynowego od wielu dziesięcioleci, więc temat ten nie jest dla nas nowy. Tylko w dziedzinie bezpieczeństwa mamy liczne zespoły i ponad 20 doktorów będących specjalistami od uczenia maszynowego. Nasze zespoły wykorzystują je jako metodę wykrywania i analizy zagrożeń. To metoda, a nie efekt. Warto rozróżnić te dwie kwestie, jeśli chodzi o bezpieczeństwo. W ciągu ostatnich kilku lat widzieliśmy wiele firm, które nakłaniają do uczenia maszynowego, ale nie chcą wyjaśnić, co to naprawdę oznacza.

Dlaczego Cisco jest inne?

W 2013 r. przejęliśmy Cognitive Security, firmę całkowicie poświęconą uczeniu maszynowemu. Szybko połączyliśmy ich technologię (nazywaną obecnie Cognitive Intelligence) z naszymi rozwiązaniami w zakresie bezpieczeństwa sieciowego w celu ulepszenia wykrywalności (patrz blogi). Było to pasywne podejście do wykrywania. Dzienniki są wysyłane z serwera proxy do rozwiązania Cognitive Intelligence, gdzie poddaje się je analizie. Analizujemy atrybuty logów, bez konieczności zwracania uwagi na obciążenie, aby wykryć nietypową aktywność w trakcie normalnego działania. Efekt jest prosty: technologia Cognitive Intelligence informuje tylko o naruszeniu zabezpieczeń hostów. Ponieważ ostrzeżenie dotyczy jedynie potwierdzonych infekcji, analitycy nie tracą czasu i od razu przystępują do działań naprawczych i usuwania błędów.

To był dopiero początek osadzania uczenia maszynowego w naszej ofercie zabezpieczeń. Szybko zdaliśmy sobie sprawę z wartości tej technologii i zaczęliśmy wykorzystywać jej ogromne możliwości analityczne w innych częściach zasobów zabezpieczeń. Zastosowaliśmy algorytmy umożliwiające korelowanie ogromnych ilości danych i dostarczanie analiz wykraczających poza to, co można było zobaczyć z jednego wektora. Na przykład dzięki korelacji danych o ruchu sieciowym z zewnętrzną komunikacją proxy dałoby się zidentyfikować zagrożonego hosta, który ma uprawnienia administratora i wykonuje ruchy na boki – nie byłoby to możliwe przy użyciu jednej technologii. Ale jeśli połączy się kilka elementów, już tak. Wtedy właśnie zdaliśmy sobie sprawę z prawdziwej wartości tego, czym dysponujemy.

Zastosowanie uczenia maszynowego w telemetrii sieci

Cisco na całym świecie słynie z innowacyjnych przełączników i routerów. Można powiedzieć, że zbudowaliśmy szkielet infrastruktury internetowej większości organizacji. Ta infrastruktura sieciowa jest bogatym źródłem danych. Na przykład Stealthwatch gromadzi i analizuje telemetryczne dane sieci w celu zidentyfikowania zagrożeń, które mogą kryć się w jej obrębie. Rozwiązanie to integruje się również z mechanizmem uczenia maszynowego zastosowanym w technologii Cognitive Intelligence, który koreluje zachowania wskazujące na zagrożenia obserwowane **lokalnie** w obrębie przedsiębiorstwa z zachowaniami obserwowanymi **globalnie**. Może on wykrywać anomalie, a także jest wystarczająco inteligentny, aby następnie klasyfikować pojedyncze elementy „działań wskazujących na zagrożenia” (ponieważ nie wszystko co nietypowe musi być złośliwe), co prowadzi do precyzyjnych alarmów o kluczowym znaczeniu. Jest to również rdzeń technologii Encrypted Traffic Analytics (ETA), która potrafi – jako pierwsza w branży! – wykrywać złośliwe oprogramowanie w szyfrowanym ruchu danych bez jego *deszyfrowania*.

Uczenie maszynowe a bezpieczeństwo punktów końcowych

Jeśli chodzi o bezpieczeństwo punktów końcowych, powszechnie przyjmuje się, że wykrywanie oparte na podpisie (np. wartości hash plików) to jedynie element rozwiązania, a nie rozwiązanie. Złożoność zmieniających się wartości hash plików lub zakresów adresów IP to kwestia oczywista, co oznacza, że przeciwnicy mogą generować nowe wartości SHA256 dla każdego ataku. Wartość hash może wystarczać do zidentyfikowania pojedynczego złośliwego pliku, ale nie pomaga w wykryciu innych powiązanych ataków polimorficznego złośliwego oprogramowania, powiązanych z tym samym naruszeniem lub nawet z tym samym atakującym. Dana wartość hash po prostu nigdy nie pojawi się po raz drugi.

Gdy zastosujemy do tych plików mechanizm uczenia maszynowego, będziemy w stanie rozdzielić każdy z nich, aby móc analizować je po kawałku. Przypomina to patrzenie na poszczególne elementy składające się na samochód, nie na pojazd jako całość. Tak, auta mają opony, silnik, przednią szybę, szyby boczne, ramę itd. Ale zdecydowanie nie wszystkie samochody są sobie równe. To samo dotyczy złośliwego oprogramowania. Możemy rozbić każde pojedyncze zagrożenie na najdrobniejsze detale (ponad 400 różnych atrybutów). Atrybuty te są wykorzystywane jako dyskretne klasyfikatory w modelu uczenia maszynowego, a większy poziom szczegółowości daje w efekcie inteligentniejszy, skuteczniejszy algorytm, jak również wyższą precyzję. Oznacza to, że nasz mechanizm uczenia maszynowego lepiej sprawdza się przy wykrywaniu tych nowych i zmodyfikowanych zagrożeń. Cyberprzestępcy często zmieniają formaty swoich narzędzi, czego przykładem może być luka Flash z CVE-2018-4878, wykorzystywana w wielu atakach, m.in. ROKRAT i kolejnej kampanii z użyciem tego trojana. Uczenie maszynowe jest jedną z 14 technik wykorzystywanych w rozwiązaniu AMP dla punktów końcowych w celu wykrywania zagrożeń i ochrony przed nimi.

Łączenie kawałków w jedną całość

Jednym ze sposobów, w jaki rozwijamy te technologie w Cisco, jest definiowanie modeli atakujących za pomocą mechanizmu uczenia maszynowego i technologii Cognitive Intelligence. Poprzez korelację telemetrii z dzienników internetowych proxy (Cisco i innych firm), telemetrii sieciowej (Stealthwatch), wartości SHA256 i zachowania plików z AMP można określić, jak działają napastnicy, co robią, a nawet kim są. Gdy wprowadzimy taką ilość danych do naszych algorytmów uczenia maszynowego, uzyskujemy niezrównany poziom wykrywalności, a co ważniejsze blokujemy więcej zagrożeń, zanim staną się one problemem. W kolejnych wpisach będziemy szczegółowo badać poszczególne klasyfikatory.

Możesz bezpłatnie przetestować rozwiązanie AMP dla punktów końcowych tutaj: www.cisco.com/go/tryamp.

Aby dowiedzieć się więcej na temat tego, w jaki sposób wykorzystujemy uczenie maszynowe w rozwiązaniach bezpieczeństwa Cisco, obejrzyj ten film na temat technologii.

Słowa kluczowe:

- zaawansowana ochrona przed złośliwym oprogramowaniem
- zaawansowane zabezpieczenia przed zagrożeniami
- bezpieczeństwo punktów końcowych
- uczenie maszynowe

Aby zachować aktualność rozmów, komentarze na stronie Cisco Blogs są blokowane po 60 dniach. Najnowszą zawartość można znaleźć na stronie głównej Cisco Blogs.

- Subskrybuj sekcję Bezpieczeństwo

Top of Form
Bottom of Form

- Media społecznościowe

- Nasze lektury
  - CERT Vulnerability Analysis
  - Microsoft Security Research & Defense
  - SANS Internet Storm Center
  - Schneier on Security
- Powiązane łącza
  - Porady i odpowiedzi
  - Raporty na temat ryzyka cybernetycznego
  - Najlepsze praktyki w zakresie bezpieczeństwa
  - Działalność Cisco w dziedzinie analiz bezpieczeństwa
  - Produkty w dziedzinie bezpieczeństwa