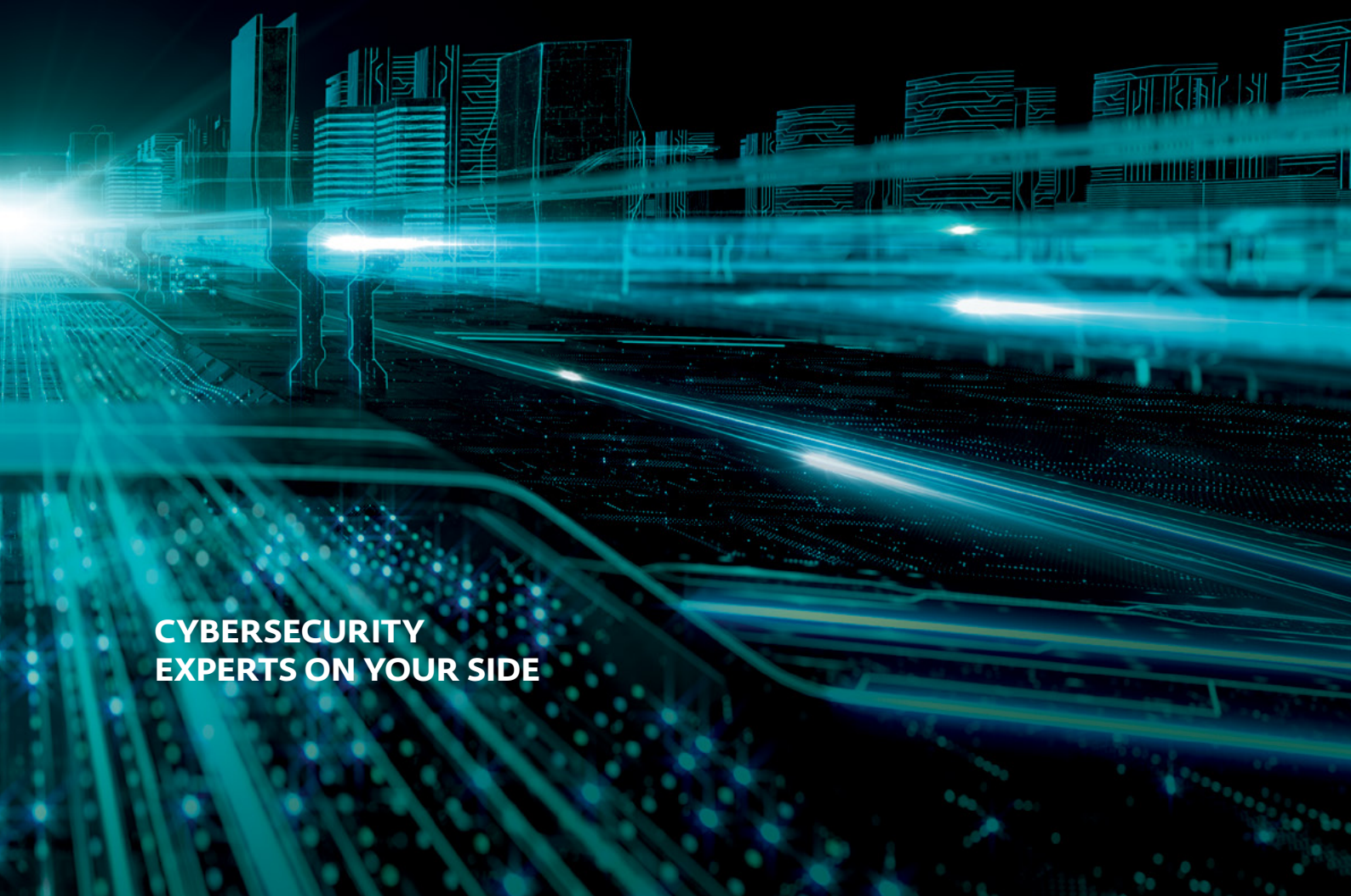
WYPRODUKOWANE
W UNII EUROPEJSKIEJ
ROZWIJANE
W POLSCE

5 MLN+
KLIENTÓW
W POLSCE

ENTERPRISE INSPECTOR

Rozbudowane rozwiązanie typu EDR,
z którym zidentyfikujesz zagrożenia
i ataki w swojej sieci firmowej



**CYBERSECURITY
EXPERTS ON YOUR SIDE**

Czym jest rozwiązanie typu **Endpoint Detection & Response?**

ESET Enterprise Inspector to narzędzie typu Endpoint Detection & Response (EDR), służące do identyfikacji nietypowych zachowań i naruszeń bezpieczeństwa firmowej sieci. Rozwiązanie pozwala reagować na zdarzenia, oceniać ich ryzyko, a także podejmować stosowne do sytuacji działania zaradcze.

Program w czasie rzeczywistym nadzoruje i ocenia wszystkie czynności wykonywane w sieci (np. zdarzenia dotyczące użytkowników, plików, procesów, rejestru, pamięci i sieci), a w razie potrzeby umożliwia podjęcie natychmiastowych działań.

Dlaczego warto wybrać **ESET Enterprise Inspector?**

NARUSZENIA BEZPIECZEŃSTWA DANYCH

Firmy nie tylko muszą wykryć, że doszło do naruszenia bezpieczeństwa danych; muszą także zidentyfikować i wyeliminować przyczynę tego typu incydentów. Wiele przedsiębiorstw nie jest w stanie samodzielnie monitorować swojej firmowej sieci, dlatego zdecydowana większość z nich korzysta w tym celu z pomocy dostawców zewnętrznych. Współczesne organizacje potrzebują coraz lepszego wglądu w swoje sieci i komputery, by mieć pewność, że nowe zagrożenia, ryzykowne zachowania pracowników i niepożądane aplikacje nie stwarzają ryzyka dla zysków i reputacji firmy.

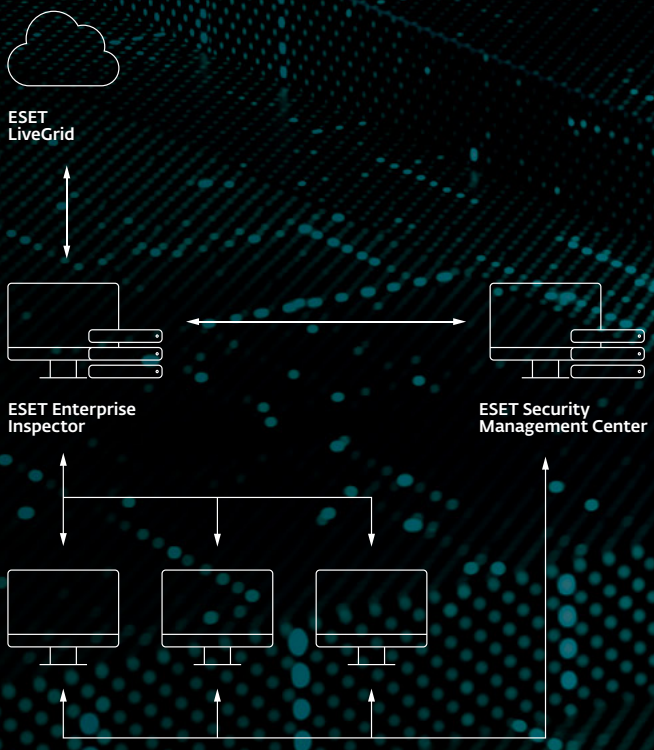
Naruszenia bezpieczeństwa danych dotyczą szczególnie tych branż, które dysponują cennymi dla atakujących informacjami. Należą do nich firmy m.in. z sektora finansowego, publicznego, handlowego, czy też przedstawiciele służby zdrowia. Nie oznacza to jednak, że inne branże są bezpieczne.

ZAAWANSOWANE ZAGROŻENIA APT I ATAKI UKIERUNKOWANE

Systemy EDR wykorzystywane są do identyfikacji zagrożeń APT i ataków ukierunkowanych. Wiele tego typu infekcji może pozostawać niewykrytych przez wiele dni, a nawet miesięcy.

LEPSZY WGLĄD W ORGANIZACJĘ

Systemy EDR zapewniają lepszy wgląd w strukturę IT organizacji, dając dostęp do wyjątkowo szczegółowych informacji nt. działań realizowanych w sieci firmowej. Dzięki temu możliwe jest rozpoznanie i zablokowanie nawet najbardziej wyszukanych ataków i infekcji.



ESET Enterprise Inspector zapewnia unikatowy sposób detekcji zagrożeń w oparciu o **analizę zachowania i reputacji plików**. Wykrywanie zagrożeń jest dzięki temu w pełni transparentne dla zespołów ds. bezpieczeństwa IT.

Endpoint Protection Platform
Wielowarstwowa ochrona stacji roboczych w firmie. Każda z warstw ochronnych przesyła zabrane informacje do ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Wyrafinowane narzędzie typu EDR, analizujące w czasie rzeczywistym ogromne ilości danych. Rozwiązanie pozwala wykryć każdą niepożądaną lub niebezpieczną aktywność w sieci firmowej.

=

Kompletne rozwiązanie do zapobiegania, wykrywania i reagowania na zagrożenia oraz ataki.

Współczesne organizacje potrzebują stałego monitoringu aktywności podejmowanych na firmowych stacjach roboczych. Taka kontrola pozwala na błyskawiczne identyfikowanie **nowych zagrożeń**, niechcianych aplikacji, czy **ryzykownych zachowań** pracowników, mogących negatywnie wpłynąć na zysk czy reputację przedsiębiorstwa.

ESET Enterprise Inspector działa jeszcze skuteczniej w połączeniu z dedykowanymi usługami ESET

Instalacja i aktualizowanie programu ESET

Nasi specjaliści zainstalują i skonfigurują produkty ESET w Twoim środowisku sieciowym, a następnie przeprowadzą szkolenie dla Twoich pracowników. Zyskasz w ten sposób pewność, że programy ESET działają w Twojej sieci dokładnie tak, jak tego oczekujesz.

Monitorowanie zagrożeń (ESET Threat Monitoring)

Usługa, w ramach której eksperci z centrali firmy ESET, nadzorują sieć i punkty końcowe w Twojej firmie, by na bieżąco ostrzegać o podejrzanych zdarzeniach wymagających Twojej uwagi.

Wykrywanie zagrożeń (ESET Threat Hunting)

Usługa ekspercka ESET, która zapewni Ci profesjonalną analizę danych, zebranych przez ESET Enterprise Inspector. Poznasz szczegóły nt. wykrytych zdarzeń i alarmów oraz dowiesz się, jak wyeliminować wskazane problemy.

Poczuj różnicę z ESET

ZSYNCHRONIZOWANA REAKCJA

Produkty ESET stworzono tak, by stosowane razem, tworzyły spójny ekosystem zabezpieczeń. Dzięki temu, w sytuacji ataku lub infekcji, możliwa jest zsynchronizowana reakcja obronna w każdym chronionym elemencie sieci. Zespoły odpowiedzialne za bezpieczeństwo IT mogą zatrzymywać procesy, pobierać pliki, które wywołały alarm lub wyłączyć dany komputer bezpośrednio z konsoli.

OTWARTA ARCHITEKTURA

Zapewnia unikatowy sposób detekcji zagrożeń w oparciu o analizę zachowania i reputacji plików. Dzięki temu wykrywanie złośliwej zawartości jest w pełni transparentne dla zespołów ds. bezpieczeństwa IT. Wszystkie reguły zapisywane są w formacie XML, dzięki czemu można je łatwo edytować i dopasować do potrzeb konkretnej organizacji, np. poprzez integrację z systemami SIEM.

ZDALNY DOSTĘP

ESET Enterprise Inspector został wyposażony w obsługę PowerShella, dzięki czemu osoby odpowiedzialne za bezpieczeństwo sieci mogą zdalnie badać i konfigurować poszczególne komputery w organizacji, w związku z czym możliwa jest sprawna odpowiedź na incydenty, bez zaburzania cyklu pracy użytkowników.

OBSŁUGA WIELU PLATFORM

ESET Enterprise Inspector oferuje wsparcie dla systemów Windows i macOS, dzięki czemu stanowi idealny wybór dla środowisk multiplatformowych.

PUBLICZNE API

ESET Enterprise Inspector został wyposażony w API, które umożliwia dostęp i eksport danych na temat detekcji oraz środków podjętych, by im przeciwdziałać, pozwalając na integrację z zewnętrznymi narzędziami, takimi jak SIEM i SOAR.

CZUŁOŚĆ ALARMÓW

Dzięki możliwości dopasowania czułości reguł detekcji dla różnych grup komputerów i użytkowników, możliwe jest precyzyjne identyfikowanie zagrożeń i unikanie fałszywych alarmów. W połączeniu z takimi kryteriami, jak: nazwa pliku / ścieżka / hash / komenda wiersza poleceń / nazwa wydawcy, możliwe jest precyzyjne określenie warunków uruchamiania alarmów.

MITRE ATT&CKTM

ESET Enterprise Inspector odnosi poszczególne detekcje do struktury MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), umożliwiając zdobycie szczegółowych informacji na temat złożonych zagrożeń za opmocą jednego kliknięcia.

SYSTEM REPUTACJI

Rozbudowane mechanizmy filtrowania ESET dają możliwość szybkiej identyfikacji wszystkich znanych i bezpiecznych aplikacji. Wszystko dzięki systemowi reputacji ESET, który w swoim działaniu wykorzystuje bazę danych, zawierającą informacje o milionach bezpiecznych plików. Dzięki temu pracownicy działów IT, odpowiedzialni za bezpieczeństwo sieci firmowej, mogą skupić się na analizie wyłącznie niebezpiecznej zawartości.

Przykłady

Dogłębne wykrywanie zagrożeń – Ransomware

Oprogramowanie ransomware stara się przedostać do firmowej sieci i pozostać w niej niezauważonym. Po cichu rozprzestrzenia się na tak wiele punktów końcowych, jak to tylko możliwe. Przedostaje się do kopii zapasowych, przez co nawet przywrócenie poprzednich obrazów systemów nie odwróci skutków infekcji.

Agent ESET Enterprise Inspector rozszerza funkcjonalność rozwiązań ESET dla stacji roboczych i umożliwia aktywne wykrywanie złośliwego oprogramowania ransomware. Także tego obecnego już w sieci firmowej. W przykładowym scenariuszu, użytkownik otrzymuje e-mail z załącznikiem. Otwiera dokument i zostaje poproszony o uruchomienie makra. Gdy to zrobi, w systemie umieszczony zostaje plik wykonywalny, który zaczyna szyfrować wszystkie dane, włącznie z tymi zapisanymi na zmapowanych dyskach.

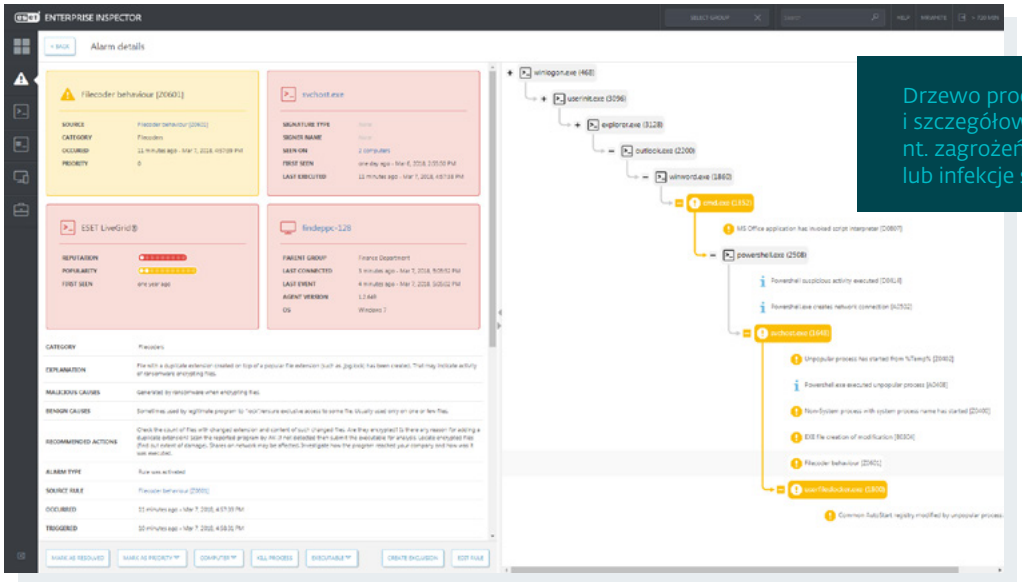
ESET Enterprise Inspector ostrzega o takich sytuacjach. Wystarczy kilka kliknięć, by administrator dowiedział się, co zostało zainfekowane, gdzie i kiedy uruchomiono określony plik wykonywalny/skrypt lub gdzie i kiedy zainicjowano konkretne działanie. Dzięki temu łatwo zidentyfikować źródło infekcji.

PRZYKŁAD

Przedsiębiorstwo chce pozyskać dodatkowe narzędzia do aktywnego wykrywania oprogramowania ransomware. Chce również być błyskawicznie informowane o podejrzanych aktywnościach, podobnych do ransomware.

ROZWIĄZANIE

- ✓ ESET Enterprise Inspector wykryje aplikacje uruchamiane z folderów tymczasowych (temp).
- ✓ ESET Enterprise Inspector wykryje pliki Office (Word, Excel, PowerPoint), które aktywują dodatkowe skrypty lub pliki wykonywalne.
- ✓ ESET Enterprise Inspector ostrzeże w razie wykrycia ransomware na urządzeniu.
- ✓ Z Ransomware Shield zobaczysz wszystkie alerty z rozwiązań ESET nt. oprogramowania wymuszającego okup.



Drzewo procesów i szczegółowe informacje nt. zagrożeń typu Filecoder lub infekcje szyfrujące

Wykrywanie zachowań niebezpiecznych i zagrożeń powtarzalnych

Najsłabszym ogniwem w bezpieczeństwie firmy jest najczęściej pracownik.

ESET Enterprise Inspector z łatwością rozpoznaje pracowników, którzy mogą stanowić zagrożenie dla bezpieczeństwa sieci firmowej. Porządkuje komputery według liczby niepowtarzalnych alarmów, wzbudzonych przez konkretnych pracowników. Jeżeli dany użytkownik generuje dużą liczbę alarmów, jego kontrolą powinien zająć się administrator.

PRZYKŁAD

W Twojej sieci firmowej są użytkownicy, którzy wielokrotnie ulegają działaniu złośliwego oprogramowania? Czy przyczyną tego stanu rzeczy jest ich lekkomyślne zachowanie? A może stają się celem ataków częściej niż pozostali pracownicy?

ROZWIĄZANIE

- ✓ Przeglądaj aktywność problematycznych użytkowników i urządzeń.
- ✓ Przeprowadź szybką analizę i identyfikuj źródła infekcji.
- ✓ Wdróż środki zapobiegawcze - blokuj adresy e-mail, strony internetowe, czy pendrive'y.

Wykrywanie i blokowanie zagrożeń

Charakterystyczną stroną ESET Enterprise Inspector jest wykrywanie trudnych do identyfikacji zagrożeń, ukrytych niczym „igła w stogu siana".

Filtry danych, dostępne w ESET Enterprise Inspector, umożliwiają porządkowanie rekordów na podstawie popularności i reputacji plików, podpisów cyfrowych, zachowania i informacji kontekstowych. Dzięki temu można w łatwy sposób rozpoznać i zbadać każdą złośliwą aktywność w sieci firmowej. Skonfigurowanie kilku filtrów umożliwia automatyzację procesu wykrywania zagrożeń i dostosowanie czułości detekcji do specyfiki danej firmy.

Każdą złośliwą aktywność można łatwo rozpoznać i zbadać.

PRZYKŁAD

System wczesnego ostrzegania lub Security Operation Center (SOC) przysyła Ci nowe ostrzeżenie o zagrożeniu. Co robisz?

ROZWIĄZANIE

- ✓ Wykorzystaj system wczesnego ostrzegania, do zdobycia informacji o nowych i nadchodzących zagrożeniach.
- ✓ Przeszukaj wszystkie komputery pod kątem obecności nowych zagrożeń.
- ✓ Przeszukaj komputery pod kątem wektorów ataku, które wykorzystują nowe zagrożenia.
- ✓ Zablokuj możliwość przedostania się zagrożenia do sieci wewnętrznej. Blokuj także możliwość uruchomienia złośliwego kodu w firmie.

Widoczność sieci

ESET Enterprise Inspector to rozwiązanie bazujące na otwartej architekturze. Oznacza to, że zespół ds. bezpieczeństwa IT może dowolnie dostosowywać reguły detekcji, do specyfiki danej organizacji.

Otwarta architektura zapewnia też elastyczność konfiguracji rozwiązania ESET Enterprise Inspector. Pozwala to na wykrycie użycia aplikacji zabronionych w organizacji, m.in. klientów sieci torrent, dysków chmurowych, przeglądarki Tor, serwerów uruchamianych przez użytkowników lub inne niepożądane programy.

PRZYKŁAD

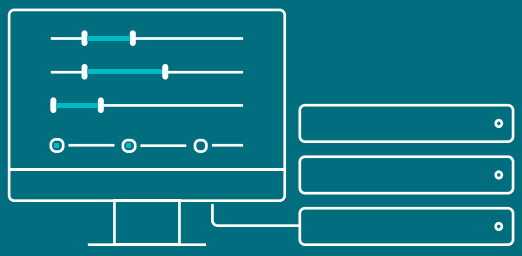
Niektóre firmy martwią się, z jakich aplikacji korzystają ich pracownicy. Dotyczy to tylko programów instalowanych w tradycyjny sposób, ale również aplikacji przenośnych. Jak zachować kontrolę nad wszystkimi aplikacjami, uruchamianymi w środowisku firmowym?

ROZWIĄZANIE

- ✓ Z ESET Enteprise Inspcetor, przeglądaj i filtruj wszystkie aplikacje zainstalowane na komputerach firmowych.
- ✓ Przeglądaj i filtruj skrypty uruchamiane na tych urządzeniach.
- ✓ W prosty sposób blokuj uruchamiane skrypty i aplikacje, które nie posiadają odpowiedniej autoryzacji.
- ✓ Powiadom użytkowników o uruchomieniu aplikacji, która nie posiada odpowiedniej autoryzacji lub usuń ją z sieci firmowej.

Problemem są nie tylko aplikacje instalowane w tradycyjny sposób, ale też aplikacje przenośne (typu portable). Jak zachować kontrolę nad wszystkimi aplikacjami, uruchamianymi w środowisku firmowym?

Zespół ds. bezpieczeństwa IT może dowolnie dostosowywać reguły detekcji do specyfiki danej organizacji.



Analiza danych kontekstowych

Charakter aktywności zależy od jej kontekstu.

Praca wykonywana na komputerach administratorów sieci znacząco różni się od pracy wykonywanej w dziale finansów. Dzięki odpowiedniemu grupowaniu komputerów, zespół ds. bezpieczeństwa IT może łatwo sprawdzić, czy dany użytkownik ma uprawnienia do wykonywania danej czynności na konkretnym urządzeniu. Synchronizacja grup stacji roboczych w ESET Security Management Center i reguł ESET Enterprise Inspector umożliwia uzyskanie niezwykle dokładnych danych kontekstowych.

PRZYKŁAD

Sposób i wynik analizy informacji zależy od jej kontekstu, tzn. od specyfiki jej wykorzystania oraz od tego, kto z niej korzysta.

ROZWIĄZANIE

- ✓ Grupuj komputery i ich użytkowników zgodnie z Active Directory, grupami statycznymi lub dynamicznymi.
- ✓ Przepuść lub zablokuj uruchamiane skrypty lub aplikacje w poszczególnych grupach komputerów.
- ✓ Dopuszczaj lub blokuj aplikacje i skrypty z uwzględnieniem uprawnień konkretnego użytkownika.
- ✓ Otrzymuj powiadomienia dotyczące aktywności wybranych grup.

Łatwa konfiguracja i reagowanie bez angażowania inżynierów

Nawet jeśli firma posiada specjalne zespoły ds. bezpieczeństwa IT, często trudno jest szybko określić priorytety i kroki, które należy podjąć, gdy nagle pojawia się alarm nt. infekcji.

Dlatego przy każdym uruchomionym alarmie ESET Enterprise Inspector wyświetla proponowane działania naprawcze. Gdy rozwiązanie rozpozna zagrożenie, uruchomia funkcję szybkiej reakcji. Poszczególne pliki można wówczas zablokować za pomocą hasha oraz przerwać i poddać kwarantannie poszczególne procesy. Możliwe jest również odizolowanie urządzenia od sieci firmowej lub jego zdalne wyłączenie.

PRZYKŁAD

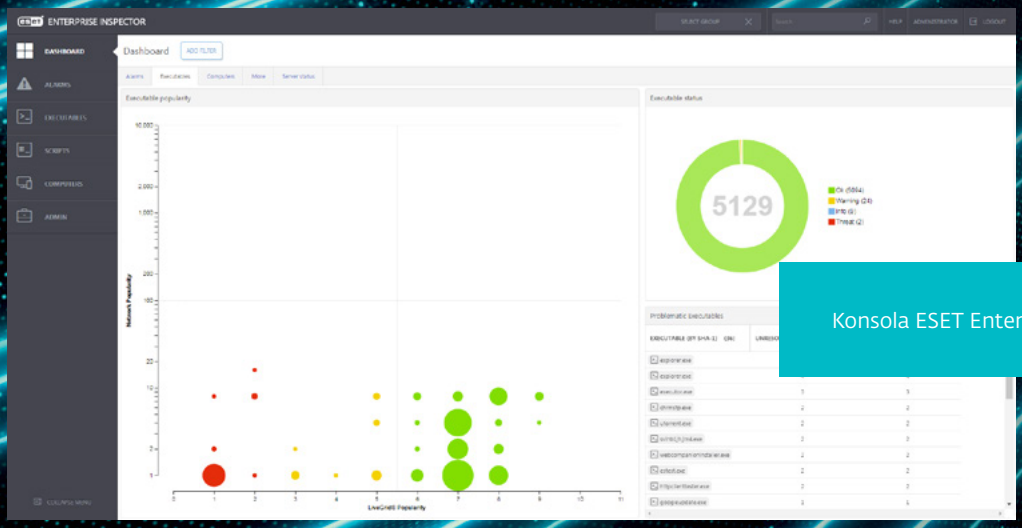
Nie każda firma ma własny zespół ds. bezpieczeństwa IT, a wprowadzanie i stosowanie złożonych reguł detekcji może stanowić dla niektórych przedsiębiorstw spore wyzwanie.

ROZWIĄZANIE

- ✓ Możliwość dostosowania ponad 220 wbudowanych reguł.
- ✓ Łatwa obsługa - jedno kliknięcie blokuje, przerywa procesy i nakłada kwarantannę.
- ✓ ESET Enterprise Inspector podsuwa propozycje dalszego postępowania i środków zaradczych, jakie należy zastosować.
- ✓ Możliwość edycji lub tworzenia nowych reguł za pomocą plików XML.

Charakter aktywności zależy od jej kontekstu. Synchronizacja grup urządzeń w ESET Security Management Center oraz reguł w ESET Enterprise Inspector umożliwia uzyskanie szczegółowych danych nt. pracy użytkownika.

Przy każdym uruchomionym alarmie ESET Enterprise Inspector wyświetla proponowane działania naprawcze.



Konsola ESET Enterprise Inspector

Funkcjonalności

WYKRYWANIE ZAGROŻEŃ

Zastosowanie filtrów pozwala sortować informacje według popularności, reputacji, podpisów cyfrowych, zachowania i informacji kontekstowych. Skonfigurowanie kilku filtrów umożliwia automatyzację procesu wykrywania zagrożeń i dostosowanie go do charakterystyki środowiska danej firmy. Dzięki temu możliwe jest łatwe wykrywanie zagrożeń, w tym również APT i ataków ukierunkowanych. Poprzez odpowiednie skonfigurowanie reguł ESET Enterprise Inspector pozwala również na wyszukiwanie zagrożeń historycznych oraz ponowne „przeskanowanie" całej bazy incydentów.

WYKRYWANIE ZDARZEŃ (ANALIZA ŹRÓDŁA PROBLEMU)

Rozwiązanie pozwala na łatwe przeglądanie wszystkich zarejestrowanych alarmów. Za pomocą kilku kliknięć zespół ds. bezpieczeństwa IT może uzyskać pełną analizę źródła problemu, w tym: co było objęte zdarzeniem, gdzie i kiedy wykonywany był plik, skrypt albo inny kod.

BADANIE I NAPRAWA

Wbudowany zestaw reguł umożliwia tworzenie własnych zasad reakcji na wykryte zdarzenia. Przy każdym uruchomionym alarmie, proponowane jest działanie umożliwiające naprawę wykrytej nieprawidłowości. Funkcja szybkiej reakcji umożliwia blokowanie plików za pomocą hasha lub przerwanie i poddanie kwarantannie poszczególnych procesów. Możliwe jest również odizolowanie urządzenia od sieci firmowej lub jego zdalne wyłączenie.

IZOLACJA ZA POMOCĄ JEDNEGO KLIKNIĘCIA

Definiując polityki dostępu do sieci można w łatwy sposób powstrzymać lateralne ruchy złośliwego kodu. Wystarczy jedno kliknięcie w konsoli ESET Enterprise Inspector, by odizolować wybrane urządzenie od reszty sieci, zatrzymując rozprzestrzenianie się infekcji.

SCORING

System scoringu umożliwia priorytetyzowanie alarmów w oparciu o przyznawaną im wartość liczbową, określającą stopień zagrożenia, jakie stanowią dla organizacji. W ten sposób administratorzy mogą w prosty sposób zidentyfikować komputery, które w pierwszej kolejności mogą stać się źródłem potencjalnego incydentu bezpieczeństwa.

ZNACZNIKI

Dodawanie znaczników do poszczególnych obiektów umożliwia szybkie wyszukiwanie poszczególnych komputerów, alarmów, wyjątków, zadań, plików wykonywalnych, procesów i skryptów. Znaczniki są współdzielone przez wszystkich użytkowników, a po utworzeniu ich przypisanie do obiektu zajmuje tylko kilka sekund.

SZCZEGÓŁOWE INFORMACJE

ESET Enterprise Inspector umożliwia przeglądanie kompletnych danych nt. infekcji i ataków w sieci firmowej, w tym o czasie ich wykonania, użytkownikach, którzy je uruchomili, długości ich trwania oraz urządzeniach nimi dotkniętych. Wszystkie te dane przechowywane są lokalnie, co zapobiega ich wyciekowi.

BEZPIECZNE LOGOWANIE

Funkcja podwójnego uwierzytelniania zapewnia dodatkową warstwę ochrony, która powstrzyma napastnika przed uzyskaniem dostępu do konta adminsitratora, nawet jeśli wejdzie on w posiadanie poprawnego hasła.

WSKAŹNIKI WYKRYWANIA NARUSZEŃ BEZPIECZEŃSTWA

Przeglądanie i blokowanie ataków i infekcji bazuje na ponad 30 różnych wskaźnikach, obejmujących m.in.: hashe, zmiany rejestru, modyfikacjach plików i połączeniach sieciowych.

WYKRYWANIE ANOMALII I ZACHOWAŃ NIEBEZPIECZNYCH

ESET Enterprise Inspector umożliwia kontrolę aktywności plików wykonywalnych i wykorzystanie systemu reputacji ESET LiveGrid do szybkiej oceny, czy wykonywany proces jest bezpieczny, czy podejrzany. Dzięki grupowaniu komputerów według użytkowników, działów i innych kryteriów, możliwa jest szybka weryfikacja, czy dana aktywność była typowa, czy też nie powinna zostać zainicjowana przez konkretnego użytkownika.

NARUSZENIA POLITYKI FIRMOWEJ

Otwarta architektura zapewnia elastyczność konfiguracji rozwiązania ESET Enterprise Inspector. Dotyczy to wykrywania naruszeń polityk użycia pewnych rodzajów oprogramowania w danej organizacji. Obejmuje m.in. torrenty, dyski chmurowe, przeglądarki Tor, serwery uruchamiane przez użytkowników lub inne niepożądane programy.

O ESET

Od ponad 30 lat ESET w swoich centrach badawczo-rozwojowych, m.in. od ponad dekady w Krakowie, rozwija najlepsze w branży oprogramowanie i usługi bezpieczeństwa informatycznego, dostarczając firmom i użytkownikom indywidualnym kompleksowe rozwiązania do ochrony przed stale ewoluującymi zagrożeniami.

ESET jest firmą o wysokiej płynności finansowej, od początku pozostająca w rękach prywatnych przedsiębiorców. Dzięki temu ESET ma pełna swobodę działania i może zapewnić najlepszą ochronę wszystkim swoim klientom.

ESET W LICZBACH

110 mln+
użytkowników na całym świecie

4 mln+
użytkowników w Polsce

400 tys.+
klientów biznesowych

13
centrów badawczo-rozwojowych

WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

Od 2017 roku ESET chroni ponad 14 tysięcy stanowisk.

Canon
Canon Marketing Japan Group

Od 2016 roku ESET chroni ponad 9000 stanowisk.

Allianz Suisse

Od 2016 roku ESET chroni ponad 4 tysiące kont pocztowych.

T-Mobile jest partnerem ISP od 2008 roku. W swojej bazie posiada ponad 2 miliony klientów.

Firma ESET spełnia normę ISO/IEC 27001:2013, czyli międzynarodowy standard zarządzania bezpieczeństwem informacji. Certyfikat został przyznany przez niezależną jednostkę certyfikującą SGS i potwierdza, że ESET realizuje wszystkie najlepsze praktyki w omawianym zakresie.

ESET czynnie wspiera MITRE ATT&CK. Aktualnie firma ESET posiada jedną z największych liczb zgłoszonych zagrożeń wśród dostawców rozwiązań bezpieczeństwa IT, potwierdzając tym samym swoje zaangażowanie w zapewnienie ochrony swoim klientom oraz społeczności.

WYBRANE NAGRODY

UZNANIE EKSPERTÓW

ESET po raz drugi z rzędu jako jedyny uzyskał tytuł „Challenger" w raporcie Gartner Magic Quadrant for Endpoint Protection Platforms 2019.

ESET zdobył tytuł „Strong Performer" w raporcie The Forrester Wave(TM): Endpoint Security Suites, Q3 2019.

W raporcie Radicati Endpoint Security 2019 ESET uzyskał tytuł „Strong Performer" w dwóch kategoriach: funkcjonalności i wizji strategicznej.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. Gartner nie rekomenduje żadnego producenta, produktu ani usługi przedstawionych w swoich publikacjach badawczych. Badania Gartnera zawierają jedynie opinie organizacji badawczej Gartner i nie powinny być interpretowane jako stwierdzenia faktów. Gartner zrzeka się wszelkich gwarancji, wyrażonych lub domniemanych, w odniesieniu do wykorzystania wyników tych badań, w tym wszelkich gwarancji przydatności handlowej lub przydatności do określonego celu.

Gartner Peer Insights to bezpłatna platforma gromadząca recenzje usług i oprogramowania wystawione przez użytkowników biznesowych. Recenzje przechodzą przez szczegółowy proces weryfikacji i moderacji w celu potwierdzenia autentyczności zawartych w nich informacji. Recenzje w ramach Gartner Peer Insights mają subiektywny charakter i stanowią subiektywne opinie użytkowników, poparte ich osobistymi doświadczeniami; nie odzwierciedlają stanowiska instytutu Gartnera oraz powiązanych podmiotów.

CYBERSECURITY
EXPERTS ON YOUR SIDE