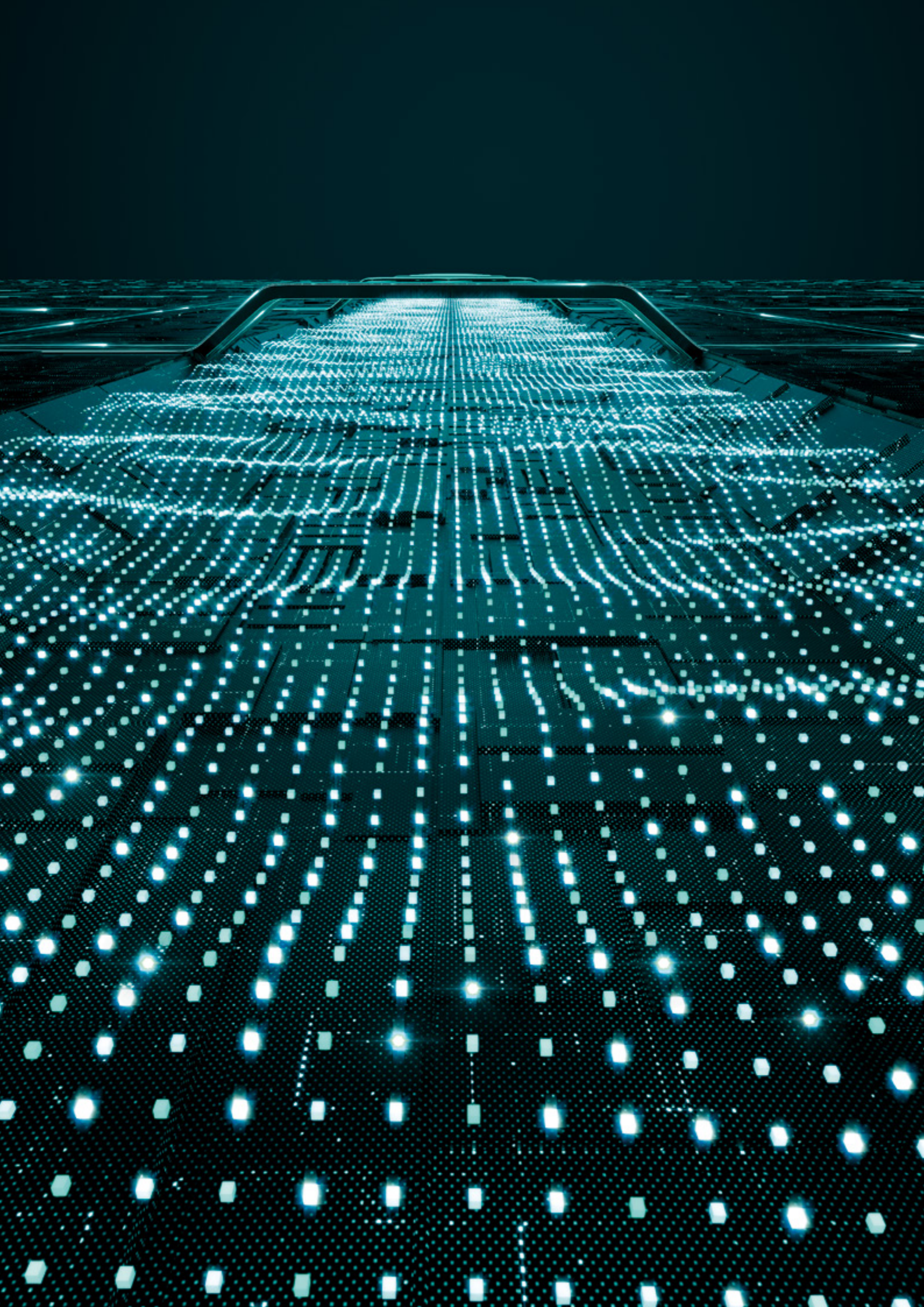
OMÓWIENIE ROZWIĄZANIA

INSPECT

Rozbudowane rozwiązanie XDR,
część pakietu ESET PROTECT,
z którym zidentyfikujesz zagrożenia
i ataki w swojej firmie.

Progress. Protected.



Czym jest **rozwiązanie XDR (Extended Detection & Response)?**

ESET Inspect, komponent pakietu ESET PROTECT oferujący funkcjonalność XDR, to zaawansowane narzędzie pozwalające na identyfikacji nietypowych zachowań, naruszeń bezpieczeństwa i anomalii w firmowej sieci. Rozwiązanie pozwala reagować na zdarzenia, oceniać ich ryzyko, a także podejmować stosowne do sytuacji działania.

ESET Inspect pozwala osobom nadzorującym na monitorowanie, jak również kompleksową ocenę aktywności w sieci i podłączonych do niej urządzeń. Pozwala także na automatyzację i natychmiastowe działanie odpowiednie do zaistniałej sytuacji. Przeszło 800 reguł opracowanych przez ESET umożliwia kompleksowe wykrywanie zagrożeń.

Dlaczego **warto stosować rozwiązania XDR?**

NARUSZENIA BEZPIECZEŃSTWA DANYCH

Firmy nie tylko muszą wykryć, że doszło do naruszenia bezpieczeństwa danych; muszą także zidentyfikować i wyeliminować przyczynę tego typu incydentów. Wszystkie tego rodzaju działania należy realizować z najwyższą precyzją i bez zakłócenia działalności przedsiębiorstwa. 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 m.in. firmy z sektorów finansowego, publicznego, handlowego, czy też przedstawiciele służby zdrowia. Nie oznacza to jednak, że inne branże są bezpieczne – hakerzy po prostu oceniają wysiłek włożony w atak i porównują go do możliwych do uzyskania korzyści.

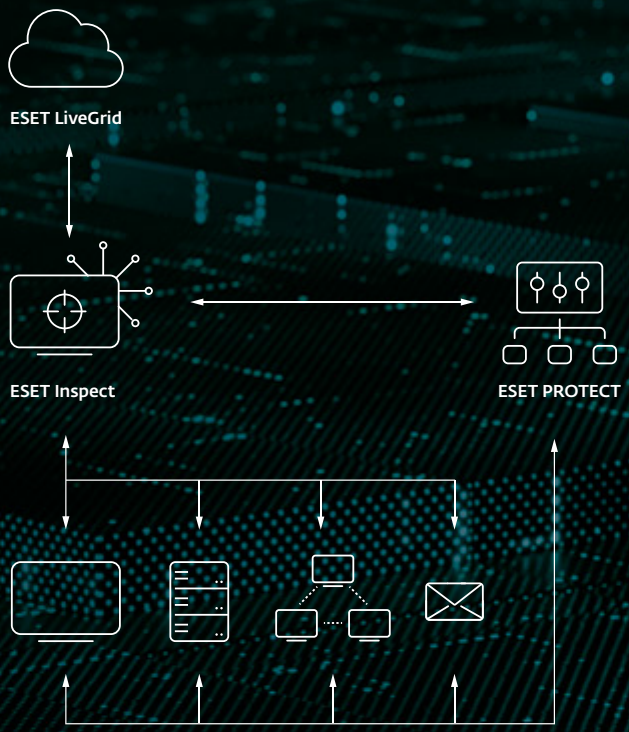
ZAAWANSOWANE ZAGROŻENIA APT I ATAKI UKIERUNKOWANE

Systemy XDR wykorzystywane są do identyfikacji zagrożeń APT i ataków ukierunkowanych dzięki usłudze Threat Hunting, skracania czasu reakcji na incydenty oraz proaktywnego zapobiegania przyszłym atakom. Wykrywanie ataków APT jest szczególnie ważne dla przedsiębiorstw, ponieważ większość firm nie jest przygotowana na nowatorskie metody ataków, które mogą pozwolić hakerom pozostawać w sieci bez wykrycia przez wiele dni lub nawet miesięcy.

LEPSZY WGLĄD W ORGANIZACJĘ

Zagrożenia wewnętrzne i ataki typu phishing stanowią znaczące zagrożenia dla przedsiębiorstw. Przestępcy wykorzystują powszechnie phishing przeciwko przedsiębiorcom ze względu na dużą liczbę pracowników, którzy mogą paść ofiarą ataków – istnieje duże prawdopodobieństwo, że jeden z pracowników złapie przynętę i narazi całą firmę na zagrożenie. Ataki z wykorzystaniem informacji wewnętrznych stanowią kolejne zagrożenie dla przedsiębiorstw, między innymi dlatego, że duża liczba pracowników przedsiębiorstwa zwiększa prawdopodobieństwo, że jeden z nich może działać wbrew jego interesom.

Systemy XDR zapewniają lepszy wgląd w strukturę IT organizacji, dzięki czemu możliwe jest rozpoznanie i zablokowanie nawet najbardziej wyszukanych ataków. Rozwiązanie ESET Inspect pozwala na szybką identyfikację i zatrzymywanie złośliwych skryptów, zamaskowanych w postaci nieszkodliwych dokumentów, takich jak pliki programu Word.



Wyjątkowa technologia wykrywania zagrożeń w oparciu o zachowanie i reputację jest całkowicie przejrzysta dla zespołów bezpieczeństwa i zapewnia im dostęp do informacji gromadzonych z przeszło 100 milionów urządzeń w naszej sieci LiveGrid® w czasie rzeczywistym.

Współczesne organizacje wymagają szerszego wglądu w posiadane komputery, by zagwarantować, że **nowe zagrożenia, ryzykowne zachowania pracowników i niechciane aplikacje** nie zagrażają zyskom i reputacji firmy.

Poczuj różnicę z ESET

KOMPLEKSOWE ZAPOBIEGANIE, WYKRYWANIE I REAGOWANIE NA ZAGROŻENIA

Umożliwia szybką analizę i rozwiązanie wszelkich problemów związanych z bezpieczeństwem w sieci. Wielowarstwowe zabezpieczenia firmy ESET, z których każda przesyła dane do usługi ESET Inspect, analizują ogromne ilości danych w czasie rzeczywistym, aby żadne zagrożenie nie pozostało niewykryte.

ROZWIĄZANIE EKSPERTÓW W DZIEDZINIE BEZPIECZEŃSTWA

ESET już od ponad 30 lat walczy z cyberzagrożeniami. Jako dostawca rozwiązań opartych na zdobyczach nauki, od wielu lat znajdujemy się w czołówce firm zajmujących się takimi dziedzinami, jak uczenie maszynowe, chmury obliczeniowe oraz XDR.

LEPIEJ ZAPOBIEGAĆ NIŻ LECZYĆ

Podejście firmy ESET do rozwiązań XDR jest ściśle związane z jej wielokrotnie nagradzanymi produktami zabezpieczającymi. Dzięki zaangażowaniu w rozwój wyjątkowej technologii wykrywania zagrożeń, zabezpieczenia firmy ESET są powszechnie uznawane za wiodące rozwiązania na całym świecie.

KOMPLEKSOWE BEZPIECZEŃSTWO SIECI

Dzięki przejrzystym regułom (w produkcie wbudowanych jest 800 i liczba ta stale rośnie), zaawansowanym wskaźnikom włamania (IoC) oraz możliwości wyszukiwania, dogłębny audyt sieci pozwala użytkownikom zidentyfikować wszystkie podejrzane elementy.

ROZWIĄZANIE GOTOWE DO DZIAŁANIA

Rozwiązanie firmy ESET zaczyna działać natychmiast po zainstalowaniu, ale jego możliwości pozwalają na dokładne dostosowanie go do potrzeb nawet najbardziej doświadczonych łowców zagrożeń.

ELASTYCZNE WDROŻENIE

Zostawiamy naszym klientom decyzję dotyczącą tego, w jaki sposób chcą wdrożyć rozwiązania zabezpieczające. ESET Inspect może zostać wdrożony na serwerach lokalnych lub w chmurze Dzięki temu możliwe jest idealne dopasowanie rozwiązania do potrzeb i wymogów bezpieczeństwa, a także wymogów sprzętowych i kosztowych.

MITRE ATT&CK™

Rozwiązanie ESET Inspect porównuje wykrywane przez siebie próbki do wyników z bazy MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), dzięki której jedno kliknięcie pozwala na dostęp do kompleksowych informacji o wszystkich zagrożeniach – nawet tych najbardziej złożonych.

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.

AUTOMATYZACJA I DOSTOSOWANIE

Z łatwością dostosujesz rozwiązanie ESET Inspect do swoich wymagań w zakresie automatyzacji oraz szczegółowości wykrywania. Podczas wstępnej konfiguracji i za pomocą wstępnie ustawionych profili użytkowników można wybrać pożądany poziom interaktywności oraz rodzaj i ilość danych, które mają być przechowywane, a następnie pozwolić, aby tryb uczenia się zbadał środowisko organizacji i zasugerował wykluczenia w przypadku fałszywych alarmów.

Przykłady

Dogłębne wykrywanie zagrożeń – Ransomware

Oprogramowanie ransomware stara się przedostać do firmowej sieci i pozostać w niej niezauważonym. Po cichu rozprzestrzenia się na możliwie jak najwięcej urządzeń, przedostaje się także do kopii zapasowych, przez co nawet przywrócenie poprzednich obrazów systemów nie pozwoli na odwrócenie skutków infekcji.

Agent ESET Inspect rozszerza funkcjonalność rozwiązań ESET Endpoint i umożliwia aktywne wykrywanie złośliwego oprogramowania ransomware występującego w sieci. 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.

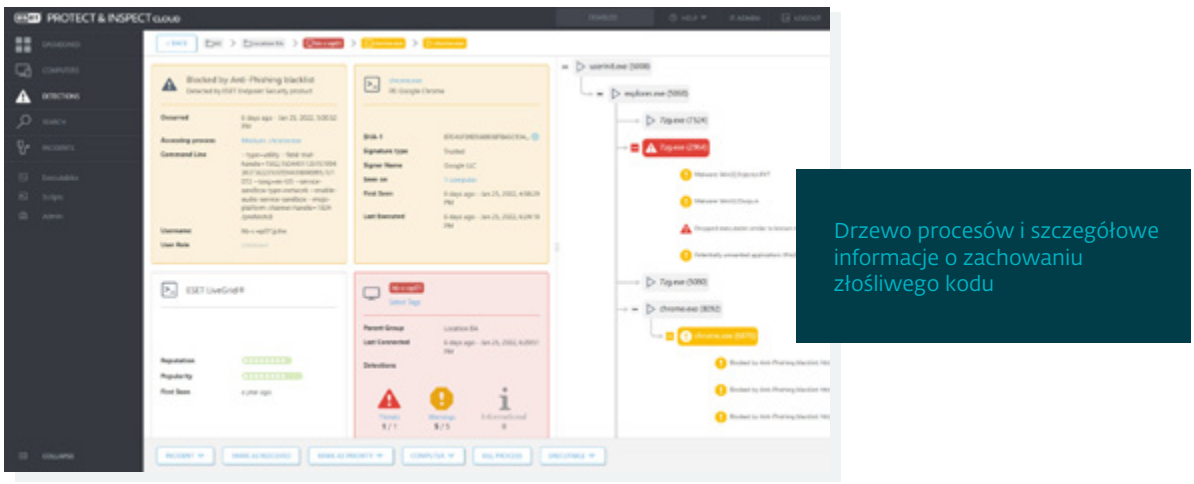
Rozwiązanie ESET Inspect ostrzega zespół odpowiedzialny za bezpieczeństwo o takich sytuacjach. Wystarczy kilka kliknięć, by administrator dowiedział się, jakie zasoby zostały zainfekowane, gdzie i kiedy uruchomiono określony plik wykonywalny lub skrypt oraz zainicjowano konkretne działanie. Dzięki temu identyfikacja źródła infekcji nie stanowi problemu.

PRZYKŁAD

Przedsiębiorstwo chce wdrożyć dodatkowe narzędzia do proaktywnego wykrywania złośliwego oprogramowania typu ransomware, a także otrzymywać natychmiastowe powiadomienia, jeśli w sieci wystąpią zachowania przypominające działanie tego rodzaju zagrożenia.

ROZWIĄZANIE

- ✓ Wprowadzenie zasad pozwalających na wykrywanie aplikacji uruchamianych z folderów tymczasowych.
- ✓ Wprowadzenie zasad pozwalających na wykrywanie plików pakietu Office (Word, Excel, PowerPoint), gdy wykonują one dodatkowe skrypty lub pliki wykonywalne.
- ✓ Ogłoszenie alarmu w przypadku wykrycia rozszerzeń plików wykorzystywanych przez popularne oprogramowanie ransomware.
- ✓ Dostęp do alertów Ransomware Shield rozwiązania ESET Endpoint Security Solutions w ramach jednej konsoli.



Drzewo procesów i szczegółowe informacje o zachowaniu złośliwego kodu

Analiza behawioralna i wykrywanie zagrożeń powtarzalnych

Najsłabszym ogniwem w bezpieczeństwie firmy jest najczęściej pracownik, nawet jeśli nie ma złych zamiarów.

Rozwiązanie ESET Inspect z łatwością rozpoznaje pracowników, którzy mogą stanowić zagrożenie dla bezpieczeństwa sieci firmowej, porządkując komputery według liczby niepowtarzalnych alarmów wywołanych przez konkretnych pracowników. Jeśli użytkownik uruchamia wiele alarmów, jest to wyraźny sygnał, że jego aktywności powinien przyjrzeć się administrator.

PRZYKŁAD

W Twojej sieci firmowej są użytkownicy, którzy wielokrotnie ulegają działaniu złośliwego oprogramowania i raz za razem są infekowani. Czy wynika to z ryzykownych zachowań? Czy może padają celem ataków częściej niż pozostali pracownicy?

ROZWIĄZANIE

- ✓ Łatwy dostęp do informacji o problematycznych użytkownikach i urządzeniach.
- ✓ Szybkie przeprowadzanie analizy przyczyn w celu znalezienia źródła infekcji.
- ✓ Usuwanie znalezionych wektorów infekcji, takich jak poczta elektroniczna, strony internetowe czy pendrive'y.

Wykrywanie i blokowanie zagrożeń

Charakterystyczną przewagą rozwiązania ESET Inspect jest wykrywanie trudnych do identyfikacji zagrożeń, ukrytych niczym „igła w stogu siana".

Filtry danych, dostępne w rozwiązaniu ESET Inspect, 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 środowiska danej firmy.

Każdą szkodliwą aktywność można łatwo rozpoznać i zbadać.

PRZYKŁAD

System wczesnego ostrzegania lub centrum operacji bezpieczeństwa (SOC) dostarcza nowe ostrzeżenie o zagrożeniu. Jakie kroki podejmiesz?

ROZWIĄZANIE

- ✓ Wykorzystanie systemu wczesnego ostrzegania do pozyskiwania danych o nadchodzących lub nowych zagrożeniach.
- ✓ Skanowanie wszystkich urządzeń pod kątem występowania nowego zagrożenia.
- ✓ Skanowanie wszystkich urządzeń pod kątem poszlak świadczących o istnieniu zagrożenia przed ostrzeżeniem.
- ✓ Zablokowanie możliwości przeniknięcia zagrożenia do sieci lub ataku na organizację.

Przejrzystość sieci

ESET Inspect jest rozwiązaniem bazującym na otwartej architekturze, co oznacza, że zespół ds. bezpieczeństwa może dostosować reguły wykrywania opisujące techniki ataków do wymogów środowiska danej organizacji.

Otwarta architektura zapewnia też elastyczność konfiguracji rozwiązania ESET Inspect. Pozwala to na wykrycie użycia aplikacji zabronionych w organizacji, m.in. klientów sieci torrent, dysków chmurowych, przeglądarki Tor, serwerów uruchamianych przez użytkowników lub innych niepożądanych programów.

PRZYKŁAD

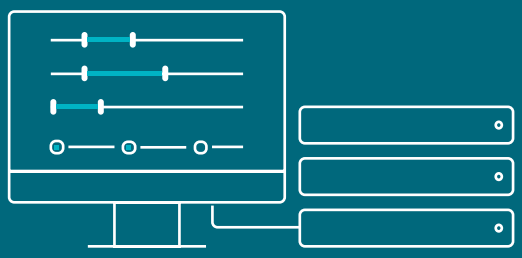
Niektóre firmy martwią się, z jakich aplikacji korzystają ich pracownicy. Dotyczy to nie tylko programów instalowanych w tradycyjny sposób, ale również aplikacji przenośnych. Jak zachować kontrolę nad wszystkimi aplikacjami, uruchamianymi w środowisku firmowym?

SOLUTION

- ✓ Łatwe przeglądanie i filtrowanie aplikacji zainstalowanych na wszystkich urządzeniach.
- ✓ Wyświetlanie i filtrowanie skryptów uruchamianych na wszystkich urządzeniach.
- ✓ Łatwe blokowanie uruchamiania nieautoryzowanych skryptów i aplikacji.
- ✓ Powiadamianie użytkowników o uruchomieniu aplikacji, która nie posiada odpowiedniej autoryzacji i automatyczne odinstalowanie.

Problemem są nie tylko aplikacje instalowane w tradycyjny sposób, ale także aplikacje przenośne, które nie wymagają instalacji. 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 przez administratorów sieci różni się znacząco od pracy wykonywanej w dziale finansowym. Dzięki odpowiedniemu grupowaniu komputerów zespoły ds. bezpieczeństwa mogą łatwo określić, czy dany użytkownik jest uprawniony do wykonywania określonej czynności na danej maszynie. Synchronizacja grup stacji roboczej w rozwiązaniu ESET PROTECT i reguł ESET Inspect umożliwia uzyskanie niezwykle dokładnych danych kontekstowych.

PRZYKŁAD

Sposób i wynik analizy informacji zależy od jej kontekstu. Aby podejmować właściwe decyzje, należy wiedzieć, jakie rodzaje alarmów występują, na jakich urządzeniach i którzy użytkownicy je wywołują.

ROZWIĄZANIE

- ✓ Grupowanie komputerów na podstawie Active Directory, grup statycznych lub dynamicznych.
- ✓ Zezwalanie na działanie lub blokowanie aplikacji i skryptów w poszczególnych grupach.
- ✓ Zezwalanie na działanie lub blokowanie aplikacji i skryptów uruchamianych przez poszczególnych użytkowników.
- ✓ Otrzymywanie powiadomień dotyczących określonych grup.

Łatwa konfiguracja i reagowanie bez angażowania inżynierów

Nawet jeśli firma posiada wyspecjalizowane zespoły zajmujące się bezpieczeństwem, często trudno jest szybko ustalić priorytety i podjąć decyzję o kolejnych krokach, gdy brzmią alarmy na temat infekcji.

Dlatego przy każdym uruchomionym alarmie ESET Inspect wyświetla propozycję kolejnych działań naprawczych. Gdy rozwiązanie rozpozna zagrożenie, udostępnia funkcję szybkiego reagowania. Określone pliki mogą być blokowane na podstawie skrótu kryptograficznego, procesy mogą być zatrzymywane i poddawane kwarantannie, a wybrane urządzenia mogą być izolowane lub wyłączane zdalnie.

PRZYKŁAD

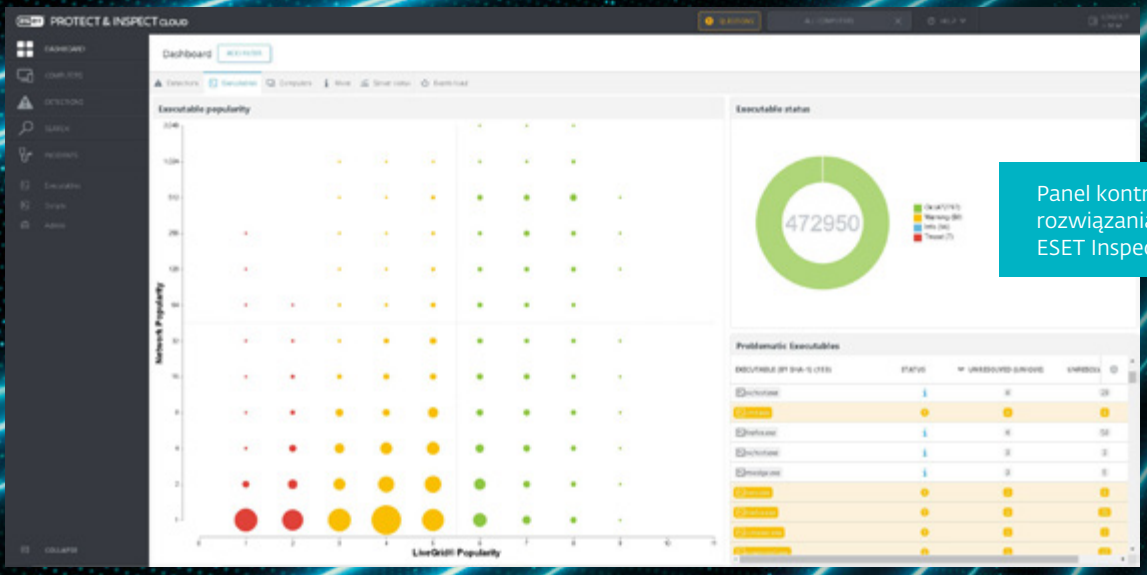
Nie wszystkie firmy mają dedykowane zespoły ds. bezpieczeństwa, a wprowadzanie i wdrażanie zaawansowanych reguł wykrywania zagrożeń może być trudnym zadaniem dla wielu organizacji.

ROZWIĄZANIE

- ✓ Ponad 300 wbudowanych, wstępnie skonfigurowanych reguł.
- ✓ Łatwa obsługa – kliknięcie jednego przycisku wystarczy, by zablokować urządzenia, wyłączyć je lub poddać kwarantannie.
- ✓ Wbudowane w alarmy możliwe kroki do wykonania.
- ✓ Możliwość edycji reguł w języku XML, co pozwala na łatwe dostosowanie lub tworzenie nowych zasad.

Charakter aktywności zależy od jej kontekstu. Synchronizacja grup stacji roboczych w rozwiązaniu ESET PROTECT i reguł ESET Inspect umożliwia uzyskanie niezwykle dokładnych danych kontekstowych.

Każdy uruchomiony alarm obejmuje propozycję kolejnych działań, które należy wykonać w celu złagodzenia skutków zdarzenia.



Panel kontrolny rozwiązania ESET Inspect

Funkcjonalności

SYSTEM ZARZĄDZANIA ZDARZENIAMI

Grupuj obiekty, takie jak wykryte zagrożenia, stacje robocze, pliki wykonywalne lub procesy w logiczne grupy, aby wyświetlać potencjalnie złośliwe zdarzenia na osi czasu wraz z powiązanymi działaniami użytkowników. Rozwiązanie ESET Inspect automatycznie podsuwa specjalistom wszystkie powiązane zdarzenia i obiekty, które mogą być bardzo pomocne na etapach diagnostyki, dochodzenia do przyczyn oraz naprawy skutków zdarzeń.

REAKCJA W CZASIE RZECZYWISTYM

Rozwiązanie ESET Inspect oferuje wachlarz łatwo dostępnych i obsługiwanych jednym kliknięciem działań, takich jak restartowanie i wyłączanie stacji roboczej użytkownika, izolacja urządzenia od reszty sieci, uruchamianie skanowania na żądanie, zamykanie wszystkich uruchomionych procesów i blokowanie aplikacji na podstawie skrótu kryptograficznego pliku wykonalnego. Dodatkowo, dzięki funkcji Terminal, zapewniającej możliwość reagowania na zagrożenia w czasie rzeczywistym, specjaliści ds. bezpieczeństwa mogą korzystać z pełnego zestawu opcji badania i usuwania skutków opartych na terminalu PowerShell.

ANALIZA PRZYCZYN

Rozwiązanie zapewnia możliwość łatwego dotarcia do podstawowych przyczyn problemu oraz pełnego drzewa procesów każdego potencjalnie złośliwego łańcucha zdarzeń. Umożliwia sprawdzenie szczegółów zdarzenia i zapewnia użytkownikom możliwość podejmowania świadomych decyzji na podstawie bogatego kontekstu i informacji dotyczących zarówno nieszkodliwych, jak i groźnych zdarzeń, opisanych przez naszych ekspertów ds. złośliwego oprogramowania.

PUBLICZNE API

Rozwiązanie ESET Inspect obejmuje publiczny interfejs REST API, pozwalający na uzyskiwanie dostępu do wykrywanych zagrożeń, ich eksportowanie oraz łagodzenie skutków ataków, co pozwala na skuteczną integrację z dostępnymi na rynku narzędziami SIEM, SOAR, systemami zgłaszania problemów i innym dostępnym oprogramowaniem.

WYKRYWANIE ZAGROŻEŃ

Rozwiązanie zapewnia dostęp do wydajnego wyszukiwania wskaźników ataku na podstawie zapytań oraz filtrów pozwalających na przeglądanie danych w celu ich sortowania na podstawie popularności plików, reputacji, podpisu cyfrowego, zachowania lub innych informacji kontekstowych. Konfiguracja wielu filtrów umożliwia zautomatyzowane, łatwe wyszukiwanie zagrożeń i reagowanie na incydenty, w tym wykrywanie i powstrzymywanie ataków APT i ataków ukierunkowanych.

BEZPIECZNY I BEZPROBLEMOWY DOSTĘP ZDALNY

Usługi reagowania na zdarzenia i zagrożenia są tak skuteczne, jak skuteczna jest możliwość uzyskania do nich dostępu w sytuacji kryzysowej. Dotyczy to zarówno możliwości połączenia się z konsolą, jak i ze stacjami roboczymi. Połączenie naszego rozwiązania działa w czasie zbliżonym do rzeczywistego, a dodatkowo zapewnia pełne bezpieczeństwo – wszystko to bez konieczności używania narzędzi zewnętrznych dostawców.

IZOLOWANIE ZAGROŻEŃ JEDNYM KLIKNIĘCIEM

Rozwiązanie pozwala na określenie zasad dostępu do sieci, aby szybko zatrzymać rozprzestrzenianie się złośliwego oprogramowania. Wystarczy jedno kliknięcie w interfejsie ESET Inspect, aby odizolować zagrożone urządzenie od sieci, a po zabezpieczeniu urządzenia równie łatwo można je usunąć z kwarantanny.

WYKRYWANIE ANOMALII I ZACHOWAŃ NIEBEZPIECZNYCH

Rozwiązanie pozwala sprawdzić, jak działa plik wykonywalny i skorzystać z możliwości systemu ESET LiveGrid® Reputation, aby szybko ocenić, czy wykonywane procesy są bezpieczne. Monitorowanie anomalii oraz zdarzeń dotyczących użytkowników jest możliwe dzięki zasadom wywoływanym na podstawie zachowań zamiast wykrycia sygnatur lub próbek złośliwego oprogramowania. Grupowanie urządzeń na podstawie użytkowników lub działów pozwala zespołom bezpieczeństwa określić, czy dany użytkownik jest uprawniony do wykonania określonej czynności.

OZNACZANIE

Przypisywanie i usuwanie znaczników pozwalają na szybkie filtrowanie obiektów takich jak: komputery, alarmy, wykluczenia, zadania, pliki wykonywalne, procesy i skrypty. Znaczniki mogą być wykorzystywane przez wielu użytkowników, a raz utworzone mogą być przypisane w ciągu kilku sekund.

ZRÓŻNICOWANE WSKAŹNIKI ATAKU

Rozwiązanie pozwala na przeglądanie i blokowanie modułów na podstawie przeszło 30 zróżnicowanych wskaźników, w tym skrótów kryptograficznych (hash), modyfikacji rejestru, modyfikacji plików i połączeń sieciowych.

OTWARTA ARCHITEKTURA I INTEGRACJE

Rozwiązanie ESET Inspect zapewnia wyjątkowe możliwości wykrywania oparte na zachowaniu i reputacji – w pełni przejrzyste dla zespołów zajmujących się bezpieczeństwem. Wszystkie reguły są oparte na języku XML, co pozwala na ich łatwą edycję i precyzyjne dostosowywanie w celu dopasowania do potrzeb konkretnych środowisk korporacyjnych, w tym integracji z systemami SIEM.

WYKRYWANIE NARUSZEŃ POLITYK FIRMOWYCH

Blokowanie wykonywania złośliwego kodu jest możliwe na dowolnym komputerze w sieci organizacji. Otwarta architektura rozwiązania ESET Inspect oferuje elastyczność w wykrywaniu naruszeń zasad dotyczących korzystania z określonego oprogramowania, takiego jak aplikacje do pobierania plików wykorzystujące protokół torrent, przechowywania danych w chmurze, przeglądania stron internetowych w sieci Tor lub innych niechcianych aplikacji.

ZAAWANSOWANA KLASYFIKACJA

Rozwiązanie pozwala na klasyfikację alarmów, która przypisuje incydentom wskaźnik dotkliwości i pozwala administratorowi szybko zidentyfikować urządzenia, które stanowią większe zagrożenie.

LOKALNE GROMADZENIE DANYCH

Administrator ma pełny dostęp do danych na temat wykonywanych modułów obejmujących czas uruchomienia, odpowiedzialnego użytkownika, czas wykonania oraz zaatakowane urządzenia. Wszystkie dane są przechowywane lokalnie, co zapobiega wyciekom wrażliwych informacji.

O firmie ESET

Od 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 pozostającą w rękach prywatnych przedsiębiorców. Dzięki temu ESET ma pełną swobodę działania i może zapewnić najlepszą ochronę wszystkim swoim klientom. Produkty ESET dostępne są w ponad 200 krajach świata. W Polsce za dystrybucję rozwiązań ESET odpowiada firma DAGMA Bezpieczeństwo IT.

ESET W LICZBACH

1mld+
chronionych użytkowników Internetu

400k+
klientów biznesowych

200+
krajów i terytoriów

13
globalnych ośrodków badań i rozwoju

NASI WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

korzysta z ochrony ESET od 2017 roku, ponad 9 000 urządzeń

Allianz Suisse

korzysta z ochrony ESET od 2016 roku, ponad 4 000 skrzynek pocztowych

Canon
Canon Marketing Japan Group

korzysta z ochrony ESET od 2016 roku, ponad 32 000 urządzeń

T

partner ISP w zakresie bezpieczeństwa od 2008 roku, 2 miliony klientów

WYBRANE NAGRODY I WYRÓŻNIENIA

AV comparatives APPROVED Business Security DEC 2021

Firma ESET otrzymała nagrodę Business Security APPROVED od AV - Comparatives w teście bezpieczeństwa biznesowego w grudniu 2021 r.

Leader WINTER 2022

Firma ESET konsekwentnie zajmuje czołowe miejsca na globalnej platformie recenzji użytkowników G2, a jej rozwiązania są doceniane przez klientów na całym świecie.

FORRESTER®

Rozwiązania ESET są regularnie doceniane przez wiodące firmy analityczne, w tym w „The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" jako przykładowy sprzedawca.

eset® Digital Security
Progress. Protected.

Digital Security
Progress. Protected.