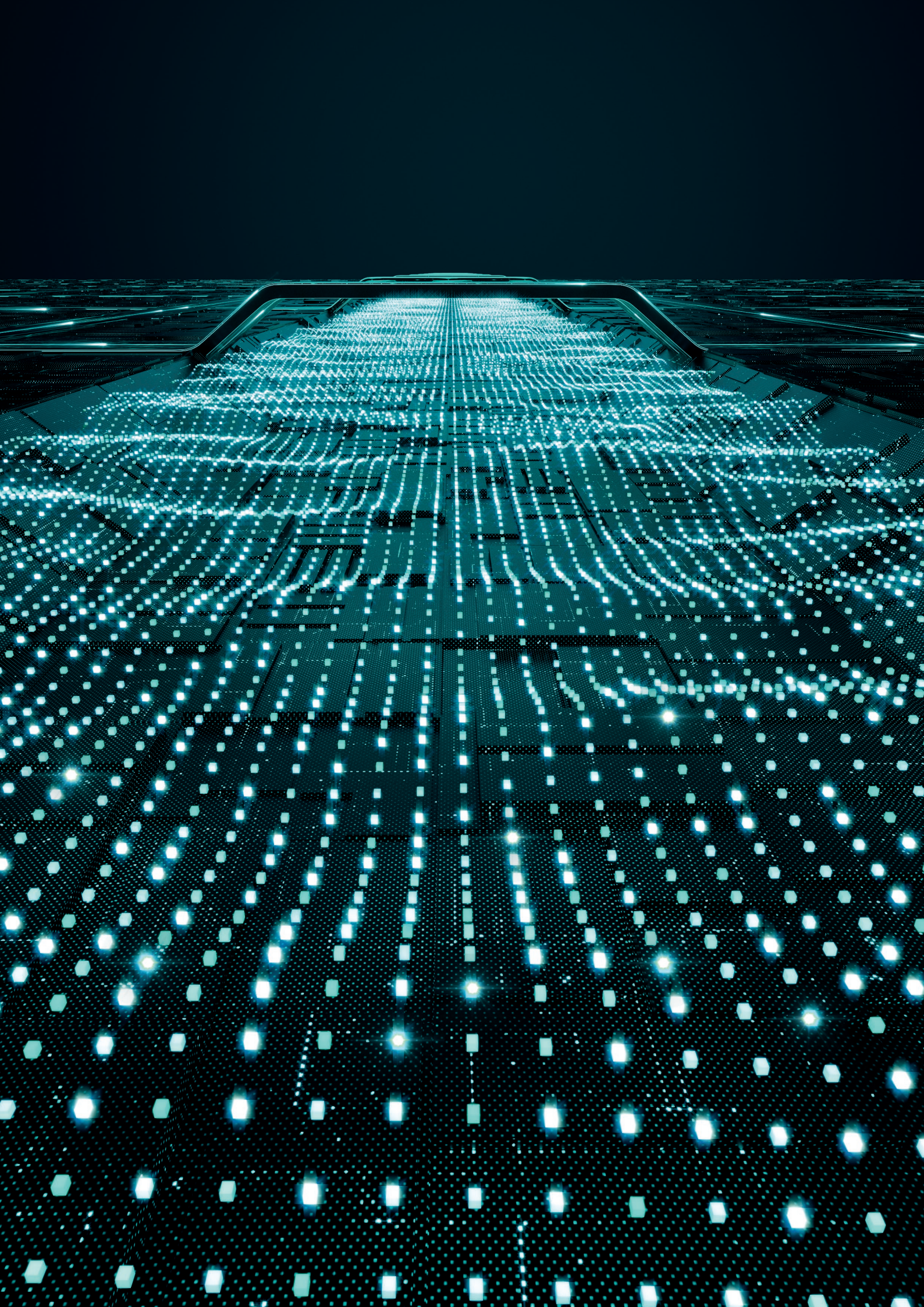
SOLUTION OVERVIEW

INSPECT

Componenta XDR a platformei ESET PROTECT care oferă prevenție pentru brețele de securitate și îmbunătățește vizibilitatea și remedierea amenințărilor

Progress. Protected.



Ce este **soluția Extended Detection & Response (XDR)?**

ESET Inspect, componenta XDR a platformei ESET PROTECT, este un instrument pentru identificarea comportamentelor suspecte și a breșelor de securitate, evaluarea riscurilor, răspuns la incidente, investigare și remediere în caz de amenințări.

Le permite celor responsabili să răspundă în caz de incidente să monitorizeze și să evalueze toate activitățile din rețea și de pe dispozitivele conectatea la aceasta. Ajută, de asemenea, la automatizarea imediată a acțiunilor de remediere, atunci când este cazul. Cele peste 800 de reguli de detecție ESET (număr ce continuă să crească) facilitează înțelegerea mecanismului de threat hunting.

De ce să folosiți **Extended Detection & Response?**

BREȘE DE DATE

Companiile nu trebuie doar să identifice că a avut loc o breșă de încălcare a datelor, acestea trebuie să le controleze și să le remedieze. Toate acestea trebuie făcute cu cea mai mare precizie și fără nicio întrerupere a continuității afacerii. Majoritatea afacerilor nu sunt pregătite pentru a efectua acest tip de investigație cu drepturi depline și angajează un furnizor extern pentru acest serviciu. Azi, organizațiile au nevoie de o vizibilitate sporită asupra computerelor lor pentru a se asigura că amenințările emergente, comportamentul riscant al angajaților și aplicațiile nedorite nu pun în pericol profiturile și reputația companiei.

Industriile de top care sunt țintele preferate pentru breșe de încălcare a datelor sunt în mod tradițional cele care dețin date valoroase, cum ar fi cele financiare, de retail, asistență medicală și sectorul public. Cu toate acestea, nu înseamnă că alte industrii sunt în siguranță – pentru hackeri primează ponderea efortului depus față de potențialul câștig.

AMENINȚĂRI PERSISTENTE AVANSATE (APT) ȘI ATACURI DIRECȚIONATE

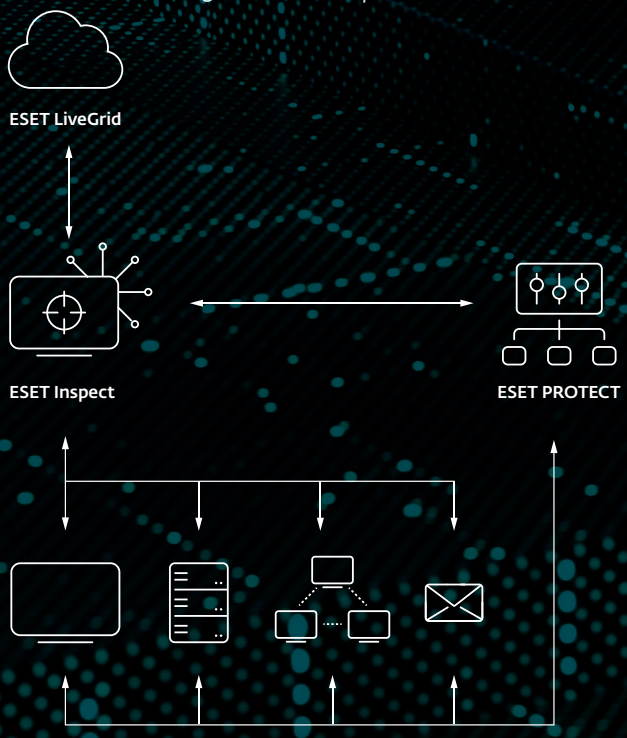
Sistemele XDR sunt utilizate în mod obișnuit pentru a identifica APT-uri sau atacuri direcționate prin Threat Hunting, pentru a reduce timpul de răspuns la incident și pentru a preveni în mod proactiv viitoarele atacuri.

Detecție unică bazată pe comportament și reputație, cu un grad ridicat de transparență pentru echipele de securitate, care le oferă acestora feedback în timp real adunat de la peste 100 de milioane de endpoint-uri din LiveGrid-ul ESET.

Descoperirea APT-urilor ,în special, este importantă pentru companii, întrucât majoritatea afacerilor de astăzi nu se simte pregătită pentru cele mai noi amenințări care pot rămâne nedetectate în rețea timp de zile sau chiar luni.

VIZIBILITATE CRESCUTĂ A ORGANIZAȚIEI

Amenințările din interior și atacurile de phishing reprezintă probleme majore pentru organizațiile comerciale. Atacurile de phishing sunt utilizate în mod obișnuit împotriva companiilor medii și mari din cauza numărului mare de angajați de vizat. Șansele ca un singur angajat să cadă pradă sunt foarte mari și astfel se ajunge la compromiterea întregii rețele din care face parte. Atacurile din interior sunt o altă amenințare pentru întreprinderi, din nou pentru că numărul ridicat de angajați crește probabilitatea ca unul dintre ei să acționeze împotriva intereselor companiei. Sistemele XDR oferă vizibilitatea sporită necesară pentru ca organizațiile să vadă, să înțeleagă, să blocheze și să remedieze orice problemă pe toate dispozitivele lor. ESET Inspect poate, de exemplu, identifica și opri rapid script-uri rău intenționate care se camuflează ca părți ale documentelor benigne, cum ar fi fișierele Word.



În ziua de azi, organizațiile au nevoie de o vizibilitate sporită asupra computerelor lor pentru a se asigura că **amenințările emergente, comportamentul riscant al angajaților și aplicațiile nedorite** nu pun în pericol profiturile și reputația companiei.

Cu ce diferă ESET

PREVENȚIE, DETECȚIE ȘI RĂSPUNS COMPLETE

Permite o analiză rapidă și remedierea oricărei probleme de securitate în rețeaua dvs. Securitatea ESET multistratificată de fond, în care fiecare nivel trimite date către ESET Inspect, analizează cantități vaste de date în timp real astfel încât nicio amenințare nu rămâne nedetectată.

SOLUȚII DE LA UN FURNIZOR CARE PUNE SECURITATEA PE PRIMUL LOC

ESET s-a luptat cu amenințările cibernetice de mai bine de 30 de ani. Fiind o companie bazată pe știință, aceasta a fost încă de la început pionier în dezvoltarea de tehnologii precum machine learning, sisteme cloud și acum XDR.

MAI BINE PREVENIȚI DECÂT SĂ TRATAȚI

Abordarea ESET față de XDR este strict conectată cu produsele sale de securitate multiplu premiate. Datorită angajamentului său față de dezvoltarea tehnologiei de detecție de înaltă calitate, soluțiile ESET de prevenție sunt mereu în top.

VIZIBILITATEA DETALIATĂ ASUPRA REȚELEI

Cu reguli de detecție transparente (ESET are o bază de date de peste 800 de reguli, număr în continuă creștere), indicatori avansați de compromis (IoC) și capabilități de căutare, realizarea unui In-Depth Executable Review pentru rețeaua dvs. vă va permite să identificați orice activitate suspectă.

GATA DE LUCRU

Soluțiille ESET funcționează imediat după instalare și sunt suficient de puternice pentru a permite modificarea granulară realizată de analiști de amenințări experimentați.

FLEXIBILITATE ÎN APLICARE

Vă lăsăm să decideți cum să implementați soluția aleasă de securitate: ESET Inspect poate rula prin propriile dvs servere on-prem sau printr-o instalare în cloud și permite o configurare personalizată, în funcție de obiectivele TCO și capacitățile echipamentelor dvs. hardware.

MITRE ATT&CK™

ESET Inspect are ca punct de referință pentru detecțiile sale cadrul MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) care, cu un singur click, vă oferă informații complete chiar și despre cele mai complexe amenințări.

REPUTAȚIE DE SISTEM

Filtrarea extinsă le permite inginerilor de sistem să identifice fiecare aplicație, folosind sistemul robust de reputație ESET. Sistemul ESET conține o bază de date de sute de milioane de fișiere benigne pentru a oferi echipelor de securitate timpul necesar să analizeze fișierele necunoscute și cele potențial malițioase, și nu pe cele identificate ca fiind fals pozitive.

AUTOMATIZARE ȘI PERSONALIZARE

Ajustați cu ușurință ESET Inspect la gradul de detaliu și automatizare de care aveți nevoie. În timpul configurării inițiale, alegeți, cu ajutorul profilurilor de utilizator prestabilite, nivelul de interacțiune dorit, plus tipul și cantitatea de date care trebuie stocate, pentru ca mai apoi să lăsați instanța Learning Mode să mapeze mediul organizației dvs. și să sugereze, acolo unde este nevoie, excluderi pentru rezultatele fals pozitive.

Studii de caz

In-Depth Threat Detection - Ransomware

În zilele noastre, ransomware-ul încearcă să treacă neobservat în rețea, răspândindu-se în cât mai multe endpoint-uri. Pătrunde în backup-urile de date ale sistemelor pentru a se asigura că revenirea la instanțele anterioare nu va împiedica executarea ransomware-ului.

Agentul ESET Inspect extinde funcționalitatea soluțiilor ESET Endpoint Security și vă permite să detectați ransomware-ul care ar putea exista deja în rețeaua dvs. Într-un scenariu tipic de atac ransomware, un utilizator primește un e-mail cu un document atașat. Utilizatorul continuă apoi să deschidă documentul Word și i se cere să ruleze in modul macros. Odată ce utilizatorul rulează macros, un executabil este inserat în sistem și începe criptarea oricăror date accesibile, inclusiv a unităților drive mapate.

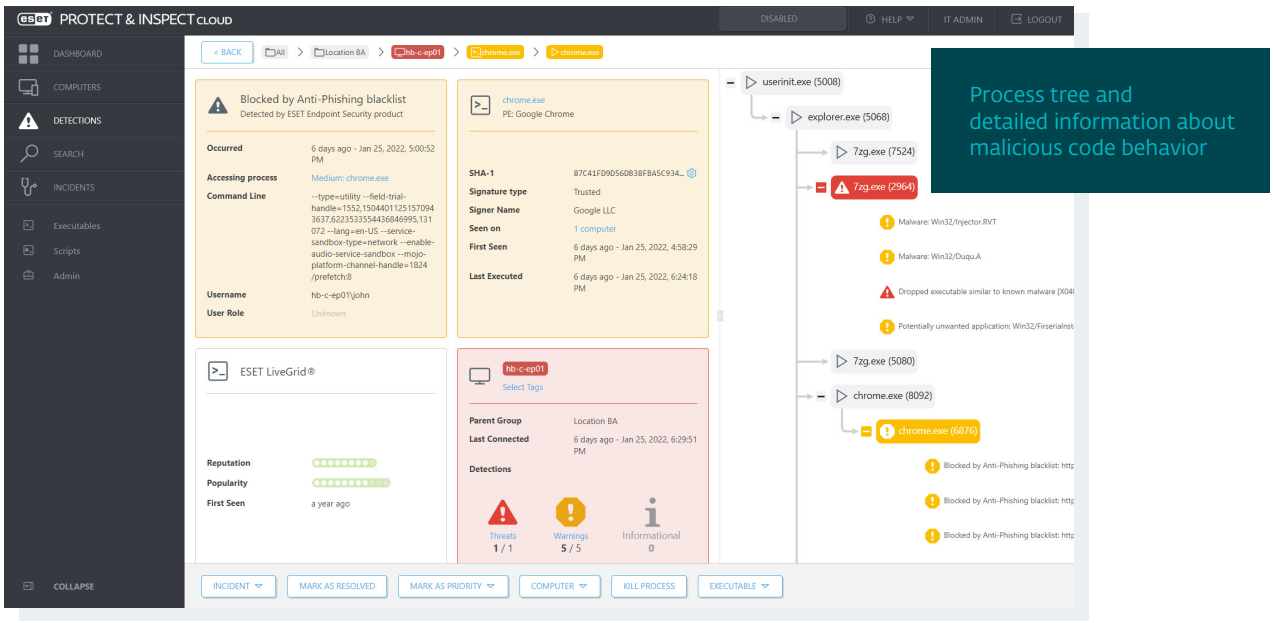
ESET Inspect permite echipei dvs. de securitate să vadă alertele legate de acest tip de comportament și prin câteva click-uri, furnizează un raport cu tot ceea ce a fost afectat, unde și când au fost efectuate un anume executabil, script sau acțiune și analizează cauza folosind tehnica „back to the root”.

STUDIU DE CAZ

O companie dorește instrumente suplimentare pentru a detecta în mod proactiv atacurile de tip ransomware, pe lângă notificările prompte în caz că în rețea a fost observat un comportament asemănător unui program ransomware.

SOLUȚIE

- ✓ Introduceți reguli pentru a detecta aplicațiile în modul execuție din folderele temporare.
- ✓ Introduceți reguli pentru a detecta fișierele Office (Word, Excel, PowerPoint) când execută scripturi suplimentare sau executabile.
- ✓ Activați, pe dispozitivele dvs., notificările de alertă în cazul detecției oricărei dintre cele mai comune extensii ale programelor ransomware în sistem.
- ✓ Vizualizați toate alertele Ransomware Shield de la toate soluțiile ESET Endpoint Security în aceeași consolă.



Detecție de comportament și agresori recidiviști

Veriga cea mai slabă la nivel de securitate este adesea o persoană obișnuită, stând lângă tastatură, fără niciun fel intenții rele.

ESET Inspect identifică cu ușurință aceste elemente potențial vulnerabile prin filtrarea calculatoarelor după numărul de alarme unice declanșate. În cazul în care același utilizator declanșează alarme multiple, acesta este un indicator clar pentru o verificare suplimentară a activității acestuia.

STUDIU DE CAZ

În rețeaua dvs., aveți utilizatori care sunt recidiviști când vine vorba de malware. Aceiași utilizatori continuă să compromită dispozitivele în repetate rânduri. Se datorează acest lucru unui comportament riscant? Sau sunt vizați mai des decât alți utilizatori?

SOLUȚIE

- ✓ Identificați cu ușurință utilizatorii și dispozitivele cu probleme.
- ✓ Rulați o analiză rapidă de tip root cause pentru a găsi sursa infectărilor.
- ✓ Remediați vectorii de infectare identificați, cum ar fi mesaje de tip e-mail, link-uri web sau dispozitive USB.

Funcțiile de blocare și Threat Hunting

Puterea distinctivă a ESET Inspect constă în capacitatea sa de Threat Hunting de a „găsi un ac în carul cu fân”.

Prin aplicarea de filtre pentru datele vizate, care sortează în funcție de popularitatea fișierului sau reputație, semnătura digitală, comportament și informații contextuale, orice activitate rău intenționată poate fi ușor identificată și investigată. Setarea mai multor filtre permite activități automatizate de Threat Hunting și poate ajusta nivelul de detecție la mediul specific companiei.

Any malicious activity can be easily identified and investigated.

STUDIU DE CAZ

Sistemul dvs. de avertizare timpurie sau Centrul de Operațiuni de Securitate (SOC) emite un nou avertisment de amenințare. Care sunt următorii pași de urmat?

SOLUȚIE

- ✓ Utilizați sistemul de avertizare timpurie pentru a prelua date despre amenințări apropiate sau noi. .
- ✓ Căutați în toate computerele existența noi amenințări.
- ✓ Căutați în toate computerele indicatori care să ateste dacă dispozitivele au fost compromise înainte de avertizare.
- ✓ Blocați amenințarea pentru a nu se putea infiltra într-o rețea sau pentru a nu efectua schimbări în sistemul informatic al unei companii.

Vizibilitatea rețelei

ESET Inspect este o soluție cu arhitectură deschisă, ceea ce înseamnă că o echipă de securitate poate ajusta regulile de detecție care descriu tehnicile de atac la mediul specific al organizației.

Arhitectura deschisă oferă, de asemenea, flexibilitate pentru configurarea ESET Inspect să detecteze încălcările politicilor organizației cu privire la utilizarea unui software specific, cum ar fi aplicații torrent, stocări în cloud, navigarea Tor, pornirea propriilor servere și alte programe nedorite.

STUDIU DE CAZ

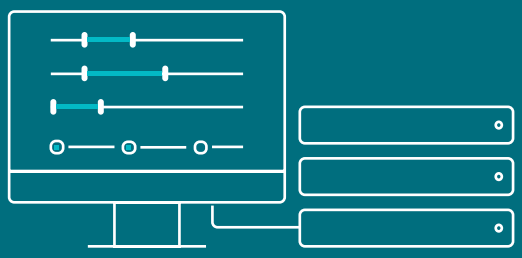
Unele companii sunt îngrijorate de aplicațiile pe care utilizatorii le rulează pe sistemele corporative. Nu doar aplicațiile cu instalare tradițională sunt un motiv de îngrijorare, cât și aplicațiile portabile care nu se instalează efectiv. Cum puteți să le țineți sub control?

SOLUȚIE

- ✓ Vizualizați și filtrați cu ușurință toate aplicațiile instalate pe dispozitive.
- ✓ Vizualizați și filtrați toate scripturile pe dispozitive.
- ✓ Blocați cu ușurință rularea scripturilor sau aplicațiilor neautorizate.
- ✓ Remediați prin notificarea utilizatorilor despre aplicațiile neautorizate și dezinstalarea lor automată.

Nu doar aplicațiile cu instalare tradițională sunt un motiv de îngrijorare, cât și aplicațiile portabile care nu se instalează efectiv. Cum puteți să le țineți sub control?

O echipă de securitate poate **ajusta regulile de detecție** care descriu tehnicile de atac la mediul specific al organizației.



Investigație Conștientă de Context și Remediere

„Caracterul malițios” unei activități depinde de context.

Activitățile desfășurate pe computere de către administratorii de rețea sunt foarte diferite de cele derulate în departamentul financiar. Gruparea adecvată a dispozitivelor ajută echipele de securitate să identifice cu ușurință dacă un anumit utilizator are dreptul de a efectua o activitate specifică pe un anumit dispozitiv. Sincronizarea dintre grupurile de endpoint-uri cu soluții ESET PROTECT instalate și seturile de reguli ESET Inspect oferă rezultate remarcabile ale informațiilor contextuale.

STUDIU DE CAZ

Datele sunt folositoare doar dacă sunt analizate împreună cu contextul din spatele lor. Pentru a lua decizii corecte, trebuie să știți care sunt alertele, pe ce dispozitive au avut loc incidente și ce utilizatori le declanșează.

SOLUȚIE

- ✓ Identificați și sortați toate computerele în funcție de Active Directory, grupări automate sau grupări manuale.
- ✓ Permiteți sau blocați aplicații sau scripturi pe baza grupării computerelor.
- ✓ Permiteți sau blocați aplicații sau scripturi în funcție de utilizator.
- ✓ Primiți notificări numai pentru anumite grupuri.

Configurare ușoară și răspuns rapid - Nu este necesară nicio echipă de securitate.

Chiar dacă o companie are echipe de securitate dedicate, este adesea dificil să prioritizezi rapid și să decizi următorii pași printre toate alarmele declanșate.

Prin urmare, pentru fiecare alarmă declanșată se propun anumiți pași de urmat, prestabiliți pentru remediere. Când ESET Inspect identifică o amenințare, oferă o funcționalitate de răspuns rapid. Anumite fișiere pot fi blocate după hash-ul acestora, anumite procese pot fi oprite și puse în carantină și dispozitivele selectate pot fi izolate sau oprite de la distanță.

USE CASE

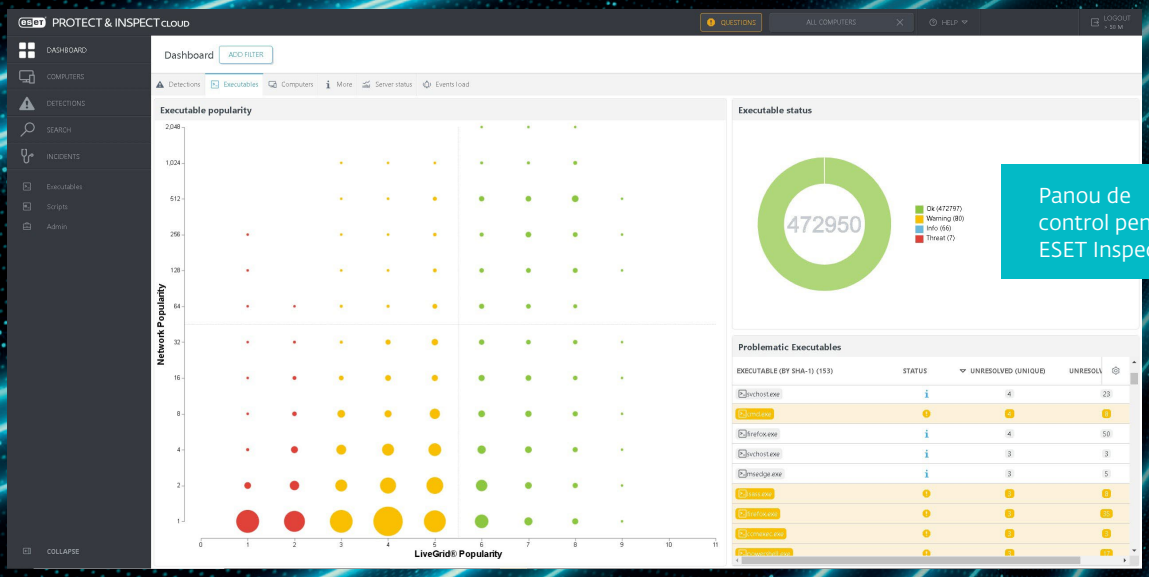
Nu toate companiile au echipe de securitate dedicate, iar introducerea și implementarea regulilor avansate de detecție poate fi anevoioasă.

SOLUȚIE

- ✓ Bază de proceduri generoasă, cu peste 300 de reguli preconfigurat încorporate.
- ✓ Răspundeți cu ușurință făcând click pe un singur buton pentru a bloca, opri sau a carantina dispozitivele compromise.
- ✓ Remedierea propusă și pașii de urmat sunt încorporate în alarmele prestabilite.
- ✓ Regulile sunt editabile prin limbaj XML pentru a permite reglajul fin sau crearea unora noi.

„Malițiozitatea” unei activități depinde de context. Sincronizarea dintre grupurile de endpoint-uri cu soluții ESET PROTECT instalate și seturile de reguli ESET Inspect oferă rezultate remarcabile ale informațiilor contextuale.

Pentru fiecare alarmă declanșată se propun anumiți pași de urmat prestabiliți pentru remediere.



Panou de control pentru ESET Inspect

Caracteristicile soluției

SISTEM DE GESTIONARE A INCIDENTELOR

Grupați obiecte precum detectii, computere, executabile sau procese în unități logice pentru a putea vizualiza evenimentele potențial rău intenționate pe o cronologie, corelate cu acțiunile utilizatorului. ESET Inspect îi furnizează automat responsabilului în caz de incidente detalii despre toate evenimentele și obiectele conexe care pot ajuta la triajul unui incident, investigarea acestuia și în etapele de rezoluție.

OPȚIUNI DE LIVE RESPONSE

ESET Inspect vine cu acțiuni de răspuns ușor accesibil printr-un singur click, cum ar fi repornirea și închiderea unui endpoint, izolarea endpoint-urilor compromise de restul rețelei, scanarea la cerere, oprirea oricărui proces suspect care rulează activ și blocarea oricărei aplicații bazându-se pe valoarea sa hash. În plus, datorită opțiunii ESET Inspect de Live Response, numită Terminal, profesioniștii în securitate pot beneficia de întreaga suită de investigații și opțiuni de remediere în PowerShell.

ANALIZA ROOT CAUSE

Vizualizați cu ușurință analiza de tip root cause și schema completă de procese în derulare, pentru oricare lanț de evenimente potențial malițios, personalizați nivelul dorit de detaliu și luați decizii bine documentate, bazate pe contextul complet și explicațiile oferite de către experții noștri în malware, atât pentru cauzele benigne, cât și pentru cele rău intenționate.

API PUBLIC

ESET Inspect dispune de un API REST Public care permite accesarea și exportarea detecțiilor și a procedurilor de remediere a acestora pentru a permite integrarea eficientă cu instrumente precum SIEM, SOAR, instrumente de ticketing și multe altele.

THREAT HUNTING

Utilizați puternica căutare IOC bazată pe interogări și aplicați filtre datelor brute pentru sortare în funcție de popularitatea fișierului, reputație, semnătura digitală, comportament sau alte informații contextuale. Configurarea mai multor filtre permite threat hunting automatizat și răspuns rapid la incidente, inclusiv capacitatea de a detecta și opri atacuri APT și atacuri cu țintă precisă.

ACCES DE LA DISTANȚĂ. SIGUR ȘI LIN

Serviciile de răspuns la incident și de securitate sunt considerate accesibile în măsura în care procedura de accesare este ușoară și lină - atât în ceea ce privește conexiunea responsabilului în caz de incident cu consola de management cât și legătura consolei cu endpoint-urile conectate. Viteza conexiunilor este aproape în timp real, iar măsurile de maximă securitate sunt aplicate concomitent, fără a fi nevoie de instrumente terțe.

IZOLARE PRINTR-UN SINGUR CLICK

Definiți politicile de acces la rețea pentru a opri rapid mișcarea laterală a programelor malware. Izolați un dispozitiv compromis din rețea cu un singur click în interfața ESET Inspect. De asemenea, eliminați cu ușurință dispozitivele aflate în stare de izolare.

DETECȚIA DE COMPORTAMENT ȘI DE ANOMALII

Verificați acțiunile efectuate de un executabil și utilizați Sistemul ESET LiveGrid® Reputation pentru a evalua rapid dacă procesele executate sunt sigure sau suspecte. Monitorizarea incidentelor anormale legate de utilizator sunt posibile din cauza regulilor specifice proiectate pentru a fi declanșate de comportament, nu doar de programele simple de malware sau prin detecția de semnături malițioase. Gruparea de calculatoare după utilizator sau departament le permite echipelor de securitate să identifice dacă un anumit utilizator are dreptul să efectueze o anumită acțiune sau nu.

TAGGING

Atribuiți și anulați atribuirea de etichete pentru filtrarea rapidă a obiectelor cum ar fi computere, alarme, excluderi, sarcini, executabile, procese și scripturi. Etichetele sunt partajate între utilizatori și, odată create, pot fi atribuite în câteva secunde.

INDICATORI MULTIPLI ÎN CAZ DE COMPROMITERE

Vizualizați și blocați module, folosind peste 30 de indicatori diferiți, inclusiv valoarea hash, modificări de registry, modificări de fișier și conexiuni la rețea.

ARHITECTURA DESCHISĂ ȘI INTEGRARE

ESET Inspect oferă detecție unică bazată pe comportament și reputație, cu un grad ridicat de transparență pentru echipele de securitate. Toate regulile sunt ușor de editat prin limbaj XML pentru a permite reglarea fină și sunt ușor de creat pentru a se potrivi nevoilor specifice mediilor companiilor, inclusiv integrări SIEM.

DETECȚIA ÎNCĂLCĂRII POLITICII COMPANIEI

Blocați executarea modulelor rău intenționate pe oricare computer din rețeaua companiei dvs.. Arhitectura deschisă a ESET Inspect oferă flexibilitate pentru detecția încălcărilor politicilor companiei care se referă la utilizarea de software specific, precum aplicații torrent, stocare în cloud, navigare Tor sau alte tipuri de software nedorit.

CLASIFICARE SOFISTICATĂ

Prioritizați gravitatea alarmelor și efectuați o clasificare a funcționalității acestora prin care se atribuie anumite valori de severitate în funcție de incident și care le permite administratorilor de rețea să identifice rapid calculatoarele cu o probabilitate mai mare de a fi compromise.

COLECTARE LOCALĂ DE DATE

Vizualizați date complete despre un nou modul executat, inclusiv timpul de execuție, utilizatorul care l-a executat, perioada petrecută în interiorul rețelei și dispozitivele atacate. Toate informațiile sunt stocate local pentru a preveni scurgerea datelor sensibile.

Despre ESET

De mai bine de 30 de ani, ESET® dezvoltă software și servicii de securitate IT de top în industrie, oferind protecție instantanee și completă împotriva amenințărilor cibernetice care afectează companiile și consumatorii din întreaga lume.

ESET este unul dintre pionierii implementării machine learning și de tehnologii cloud care previn, detectează și răspund în fața atacurilor malware. ESET este o companie privată care promovează la nivel mondial cercetarea științifică și dezvoltarea de software.

ESET ÎN CIFRE

1bn+
utilizatori, la nivel global

400k+
clienți business

200+
țări și teritorii

13
centre globale R&D

CÂȚIVA DINTRE CLIENȚII NOȘTRI

MITSUBISHI MOTORS
Drive your Ambition

protejat de ESET încă din 2017, peste 9.000 stații

Allianz Suisse

protejat de ESET încă din 2016, peste 4.000 căsuțe e-mail

Canon
Canon Marketing Japan Group

protejat de ESET încă din 2016, peste 32.000 stații

partener de securitate ISP încă din 2008 - bază de 2 milioane clienți

PREMIILE ESET

AV comparatives APPROVED Business Security DEC 2021

ESET a primit statutul APPROVED pentru soluțiile sale de protecție endpoint în testul AV-Comparative Business Security Test Decembrie 2021.

Leader WINTER 2022

ESET este prezent constant în poziții de top pe platforma globală G2 de recenzii ale utilizatorilor iar soluțiile sale sunt apreciate de consumatori la nivel internațional.

FORRESTER®

Soluțiile ESET sunt recunoscute în mod regulat de firme de analiști de renume, fiind numit Sample Vendor în „The Forrester Tech Tide(TM): Zero Trust Threat Detection and Response, Q2 2021".

Digital Security
Progress. Protected.