PREGLED

INSPECT

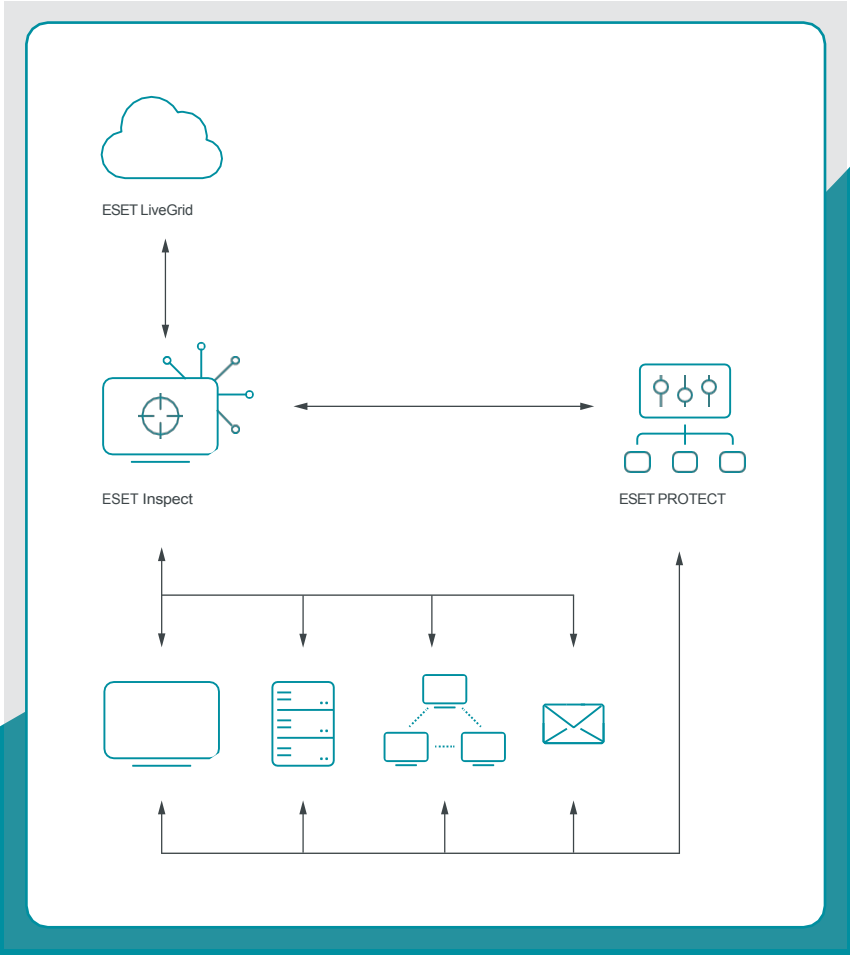
Komponenta platforme ESET PROTECT, ki omogoča XDR, zagotavlja preprečevanje kršitev, izboljšano vidljivost in sanacijo

Progress. Protected.

Kaj je **rešitev za razširjeno odkrivanje in odzivanje (XDR)?**

ESET Inspect, komponenta platforme ESET PROTECT, ki omogoča XDR, je orodje za prepoznavanje anomalnega vedenja in kršitev, oceno tveganja, odzivanje na incidente, preiskave in sanacijo.

Omogoča odzivnikom na incidente, da spremljajo in ocenjujejo vse dejavnosti v omrežju in povezanih napravah. Pomaga tudi avtomatizirati takojšnje popravne ukrepe, če je to potrebno. ESET-ovih več kot 800 (in še več) pravil za odkrivanje omogoča celovit lov na grožnje.



Razlike družbe ESET

CELOVITO PREPREČEVANJE, ODKRIVANJE IN ODZIVANJE

Omogoča hitro analizo in odpravo vseh varnostnih težav v omrežju. ESET-ova osnovna večplastna varnost, v kateri je vsak posamezen
plast pošilja podatke programu ESET Inspect, analizira velike količine podatkov v realnem času, tako da nobena grožnja ne ostane neodkrita.

REŠITEV OD PONUDNIKA, KI JE NA PRVEM MESTU NA PODROČJU VARNOSTI

ESET se proti kibernetskim grožnjam bori že več kot 30 let. Kot podjetje, ki temelji na znanosti, je že dolgo v ospredju razvoja, kot so strojno učenje, tehnologija v oblaku in zdaj XDR.

PREPREČEVANJE JE BOLJŠE OD ZDRAVLJENJA

ESET-ov pristop k XDR je tesno povezan z njegovimi večkrat nagrajenimi izdelki za preprečevanje. Zaradi zavezanosti k razvoju visokokakovostne tehnologije odkrivanja je tehnologija preprečevanja družbe ESET vodilna na svetu.

PODROBNA VIDLJIVOST OMREŽJA

S preglednimi pravili za zaznavanje (ESET jih ima več kot 800 in jih še šteje), naprednimi kazalniki kompromitacije (IoC) in možnostjo iskanja boste s poglobljenim pregledom vašega omrežja v izvedljivem programu lahko prepoznali vse, kar je sumljivo.

PRILAGODLJIVOST UVAJANJA

Omogočamo vam, da se sami odločite, kako boste namestili svojo varnostno rešitev: ESET Inspect se lahko izvaja prek lastnih strežnikov na lokaciji ali prek namestitve v oblaku, kar vam omogoča, da nastavitev prilagodite glede na svoje cilje glede stroškov lastništva in zmogljivosti strojne opreme.

PRIPRAVLJEN ZA ZAČETEK DELA

ESET-ova rešitev deluje že v izhodišču, vendar je dovolj zmogljiva, da izkušenim lovcem na grožnje omogoča granularno spreminjanje.

MITRE ATT&CK

ESET Inspect se pri svojih zaznavah sklicuje na okvir MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), ki vam - s samo enim klikom - zagotavlja izčrpne informacije tudi o najbolj zapletenih grožnjah.

SISTEM UGLEDA

Obsežno filtriranje omogoča varnostnim inženirjem, da s pomočjo ESET-ovega robustnega sistema ugleda prepoznajo vsako znano dobro aplikacijo. ESET-ov sistem vsebuje podatkovno zbirko več sto milijonov neškodljivih datotek, kar zagotavlja, da varnostne ekipe porabijo svoj čas za neznane in potencialno škodljive datoteke, ne pa za lažno pozitivne rezultate.

AVTOMATIZACIJA IN PRILAGAJANJE

Program ESET Inspect enostavno prilagodite stopnji podrobnosti in avtomatizacije, ki jo potrebujete. Izberite raven želene interakcije - ter vrsto in količino podatkov, ki jih želite shraniti - med začetno nastavitvijo in s pomočjo prednastavljenih uporabniških profilov, nato pa omogočite, da način učenja kartira okolje vaše organizacije in po potrebi predlaga izključitve lažno pozitivnih rezultatov.

Zmogljivosti rešitve

SISTEM ZA UPRAVLJANJE INCIDENTOV

Združite predmete, kot so odkritja, računalniki, izvršilni programi ali procesi, v logične enote za prikaz potencialno zlonamernih dogodkov na časovni osi s povezanimi dejanji uporabnikov. ESET Inspect odzivniku za incidente samodejno predlaga vse povezane dogodke in predmete, ki so lahko v veliko pomoč pri triaži, preiskavi in reševanju incidenta.

MOŽNOSTI ODZIVANJA V ŽIVO

Program ESET Inspect je opremljen z enostavno dostopnimi odzivnimi ukrepi z enim klikom, kot so ponovni zagon in izklop končne točke, izolacija končnih točk od preostalega omrežja, zagon pregleda na zahtevo, ubijanje vseh zagnanih procesov in blokiranje katere koli aplikacije na podlagi njene vrednosti hash. Poleg tega lahko varnostni strokovnjaki zaradi možnosti odzivanja v živo v programu ESET Inspect, imenovane Terminal, izkoristijo celoten nabor možnosti preiskovanja in sanacije v okolju PowerShell.

ANALIZA TEMELJNIH VZROKOV

Enostavno si oglejte analizo osnovnega vzroka in celotno procesno drevo katere koli potencialno zlonamerne verige dogodkov, se poglobite do želene ravni podrobnosti in sprejemajte utemeljene odločitve na podlagi bogatega zagotovljenega konteksta in razlag tako benignih kot zlonamernih vzrokov, ki so jih napisali naši strokovnjaki za zlonamerno programsko opremo.

PUBLIČNI API

ESET Inspect ima javni vmesnik API REST, ki omogoča dostop in izvoz zaznav ter njihovo sanacijo, kar omogoča učinkovito integracijo z orodji, kot so SIEM, SOAR, orodja za izdajo vozovnic in številna druga.

VEČ KAZALNIKOV KOMPROMITACIJE

Oglejte in blokirajte module na podlagi več kot 30 različnih kazalnikov, vključno s hashi, spremembami registra, spremembami datotek in omrežnimi povezavami.

LOVIŠČE OGROŽITEV

Uporabite zmogljivo iskanje IoC na podlagi poizvedb in uporabite filtre za surove podatke za razvrščanje na podlagi priljubljenosti datotek, ugleda, digitalnega podpisa, vedenja, ali drugih kontekstualnih informacij. Nastavitev več filtrov omogoča avtomatizirano, enostavno iskanje groženj in odzivanje na incidente, vključno z možnostjo odkrivanja in ustavljanja APT in ciljno usmerjenih napadov.

VAREN IN NEMOTEN DOSTOP NA DALJAVO

Odzivanje na incidente in varnostne storitve so le tako nemoteni, kot je enostaven dostop do njih - tako v smislu povezave odzivnika na incidente s konzolo kot povezave s končnimi točkami. Povezava deluje skoraj v realnem času z uporabo največjih varnostnih ukrepov, vse to brez potrebe po orodjih tretjih oseb.

IZOLACIJA Z ENIM KLIKOM

Določite politike dostopa do omrežja in hitro zaustavite bočno gibanje zlonamerne programske opreme. Izolirajte z enim klikom v vmesniku ESET Inspect izločite ogroženo napravo iz omrežja. Prav tako lahko preprosto odstranite naprave iz stanja izolacije.

ZAZNAVANJE ANOMALIJ IN VEDENJA

Preverite dejanja, ki jih izvede izvršilni program, in uporabite sistem ugleda ESET LiveGrid®, da hitro ocenite, ali so izvedeni procesi varni ali sumljivi. Spremljanje nepravilnih dogodkov, povezanih z uporabniki, je mogoče zaradi posebnih pravil, ki so napisana tako, da se sprožijo na podlagi vedenja in ne preprostih zaznav malwara ali podpisov. Združevanje računalnikov po uporabnikih ali oddelkih omogoča varnostnim ekipam, da ugotovijo, ali je uporabnik upravičen do izvedbe določenega dejanja ali ne.

OZNAČEVANJE

Dodeljevanje in odvzemanje oznak za hitro filtriranje predmetov, kot so računalniki, alarmi, izključitve, opravila, izvedljivi programi, procesi in skripte. Oznake so v skupni rabi med uporabniki in jih lahko po ustvarjanju dodelite v nekaj sekundah.

ZAZNAVANJE KRŠITEV POLITIKE PODJETJA

Blokirajte izvajanje zlonamernih modulov v katerem koli računalniku v omrežju vaše organizacije. Odprta arhitektura programa ESET Inspect omogoča prilagodljivost pri odkrivanju kršitev pravilnikov, ki veljajo za uporabo
določene programske opreme, kot so aplikacije torrent, shranjevanje v oblaku, brskanje po brskalniku Tor ali druga neželena programska oprema.

ODPRTA ARHITEKTURA IN INTEGRACIJE

ESET Inspect zagotavlja edinstveno odkrivanje na podlagi vedenja in ugleda, ki je popolnoma pregledno za varnostne ekipe. Vsa pravila je mogoče enostavno urejati prek XML, kar omogoča natančno prilagajanje, ali pa jih je mogoče enostavno ustvariti tako, da ustrezajo potrebam specifičnih podjetniških okolij, vključno z integracijami SIEM.

IZPOPOLNJENO OCENJEVANJE

Določite prednostno razvrstitev resnosti alarmov s funkcijo točkovanja, ki incidentom pripiše vrednost resnosti in administratorjem omogoča hitro
prepoznajo računalnike z večjo verjetnostjo potencialnih incidentov.

ZBIRANJE LOKALNIH PODATKOV

Oglejte si izčrpne podatke o novo izvedenem modulu, vključno s časom izvedbe, uporabnikom, ki ga je izvedel, časom zadrževanja in napadenimi napravami. Vsi podatki so shranjeni lokalno, da se prepreči uhajanje občutljivih podatkov.

Primeri uporabe

Zaznavanje vedenja in ponavljajočih se kršiteljev

PROBLEM

V omrežju imate uporabnike, ki se ponavljajo pri zlonamerni programski opremi. Isti uporabniki se vedno znova okužijo. Je to posledica tveganega vedenja? Ali pa so pogosteje tarča napadov kot drugi uporabniki?

REŠITEV

- ✓ Enostavno preglejte problematične uporabnike in naprave.
- ✓ Hitro opravite analizo temeljnih vzrokov in poiščite vir okužb.
- ✓ Odpravite najdene prenašalce okužb, kot so e-pošta, splet ali naprave USB.

Lovljenje in blokiranje groženj

PROBLEM

Vaš sistem zgodnjega opozarjanja ali varnostni operativni center (SOC) izda novo opozorilo o grožnji. Kakšni so vaši naslednji koraki?

REŠITEV

- ✓ Uporabite sistem zgodnjega opozarjanja za pridobivanje podatkov o prihajajočih ali novih grožnjah.
- ✓ Poiščite v vseh računalnikih, ali obstaja nova grožnja.
- ✓ V vseh računalnikih poiščite kazalnike kompromitacije, ki kažejo, da je grožnja obstajala že pred opozorilom.
- ✓ preprečite, da bi grožnja lahko prodrla v omrežje ali se izvajala v organizaciji.

Enostavna namestitev in enostavno odzivanje - varnostna ekipa ni potrebna

PROBLEM

Vsa podjetja nimajo namenskih varnostnih ekip, vnos in izvajanje naprednih pravil za odkrivanje pa sta lahko težavna.

REŠITEV

- ✓ Več kot 300+ vgrajenih vnaprej konfiguriranih pravil.
- ✓ Enostavno se odzovite tako, da preprosto kliknete en sam gumb za blokiranje, uničenje ali postavitev naprav v karanteno.
- ✓ Predlagana sanacija in naslednji koraki so vgrajeni v alarme.
- ✓ Pravila je mogoče urejati prek jezika XML, kar omogoča enostavno prilagajanje ali ustvarjanje novih pravil.

Preglednost omrežja

PROBLEM

Nekatera podjetja so zaskrbljena zaradi aplikacij, ki jih uporabniki uporabljajo v sistemih. Skrbeti vas morajo ne le tradicionalno nameščene aplikacije, temveč tudi prenosne aplikacije, ki se dejansko ne namestijo. Kako jih lahko nadzorujete?

REŠITEV

- ✓ Enostavno preglejte in filtrirajte vse nameščene aplikacije v napravah.
- ✓ Oglejte si in filtrirajte vse skripte v napravah.
- ✓ Enostavno blokirajte izvajanje nepooblaščenih skript ali aplikacij.
- ✓ Odpravite nepravilnosti z obveščanjem uporabnikov o nepooblaščenih aplikacijah in jih samodejno odstranite.

Poglobljeno zaznavanje groženj - izsiljevalska programska oprema

PROBLEM

Podjetje želi dodatna orodja za proaktivno odkrivanje izsiljevalske programske opreme poleg takojšnjega obveščanja, če se v omrežju pojavi vedenje, podobno izsiljevalski programski opremi.

REŠITEV

- ✓ Vnesite pravila za odkrivanje aplikacij pri izvajanju iz začasnih map.
- ✓ Vnosna pravila za zaznavanje pisarniških datotek (Word, Excel, PowerPoint), ko se izvajajo dodatno skripte ali izvršilne datoteke.
- ✓ Opozorilo, če je v napravi opažena katera od najpogostejših razširitev izsiljevalske programske opreme.
- ✓ V isti konzoli si oglejte opozorila Ransomware Shield iz rešitev ESET Endpoint Security Solutions.

Preiskava z upoštevanjem konteksta in sanacija

PROBLEM

Podatki so le tako dobri, kot je dober kontekst v ozadju. Za pravilne odločitve morate vedeti, kakšna so opozorila, v katerih napravah se pojavljajo in kateri uporabniki jih sprožajo.

REŠITEV

- ✓ Prepoznajte in razvrstite vse računalnike glede na imenik Active Directory, samodejne skupine ali ročnega razvrščanja.
- ✓ Dovolite ali blokirajte aplikacije ali skripte na podlagi razvrščanja računalnikov v skupine.
- ✓ Dovolite ali blokirajte aplikacije ali skripte na podlagi uporabnika.
- ✓ Prejemanje obvestil samo za določene skupine.

ESET Digital Security
Progress. Protected.

O družbi ESET

KO TEHNOLOGIJA OMOGOČA NAPREDEK, JE DRUŽBA ESET® TU, DA GA ZAŠČITI.

Družba ESET že več kot 30 let ustvarja tehnološke inovacije in ponuja najnaprednejše rešitve za kibernetsko varnost na trgu. Naša sodobna zaščita končnih točk temelji na edinstvenih večplastnih varnostnih tehnologijah ESET LiveSense® v kombinaciji s stalno uporabo strojnega učenja in računalništva v oblaku.
Izdelki družbe ESET, ki jih podpirajo najboljši svetovni podatki o grožnjah in raziskave, ponujajo popolno ravnovesje med zmogljivostmi preprečevanja, odkrivanja in odzivanja. Z visoko uporabnostjo in neprimerljivo hitrostjo smo predani zaščiti napredka naših strank, s čimer zagotavljamo največjo možno zaščito.

ESET V ŠTEVILKAH

Več kot 1 milijarda evrov
zaščitenih uporabnikov interneta

400k+
poslovnih strank

195
držav in ozemelj

13
globalni centri za raziskave in razvoj

NEKATERE NAŠE STRANKE

MITSUBISHI MOTORS
Drive your Ambition

ki jih ESET ščiti od leta 2017 več kot 9.000 končnih točk

Allianz Suisse

zaščiteni s programom ESET od leta 2016 več kot 4.000 poštnih predalov

Canon
Canon Marketing Japan Group

zaščiteni s programom ESET od leta 2016 več kot 32.000 končnih točk

varnostni partner ponudnikov internetnih storitev od leta 2008
2 milijona strank

PRIZNANJE

MITRE ATT&CK™

ESET je eden od najbolj referenčnih in angažiranih ponudnikov, ki neposredno sodelujejo pri izpopolnjevanju in populaciji baze znanja MITRE ATT&CK.

G2 Leader SPRING 2023

ESET na globalni platformi za pregledovanje uporabnikov G2 dosledno dosega najvišje uvrstitve, njegove rešitve pa cenijo stranke po vsem svetu.

The Radicati Group, Inc.
A TECHNOLOGY MARKET RESEARCH FIRM

Družba ESET je bila že četrto leto zapored priznana kot "najboljši igralec" v Radicatijevem tržnem kvadrantu za napredne trajne grožnje za leto 2023.