Cybersecurity
Progress. Protected.

Prijímajte isté a rýchle rozhodnutia vďaka vyhľadávaniu indikátorov IoC a analýze vzoriek

Problém

Bezpečnostné tímy sa pravidelne stretávajú s podozrivými súbormi a indikátormi, ale rozhodnúť sa, čo s nimi ďalej, nie je vždy jednoduché. Nástroje môžu ponúkať protichodné verdikty alebo im môže chýbať kontext potrebný na vysvetlenie dôvodu označenia určitých vzoriek. **Analytici potrebujú jasnejšie a spoľahlivejšie dôkazy na zníženie miery neistoty** bez toho, aby odhalili citlivé vzorky alebo sa spoliehali na drahé súkromné služby. Tímy SOC musia zároveň efektívne triediť veľké množstvo súborov a do hĺbky analyzovať najdôležitejšie vzorky bez zbytočného množstva upozornení a dodatočnej záťaže na infraštruktúru.

5 minút

overenie na základe najnovších dát ESET

20 kanálov

jedinečné IoC z 20 špecializovaných informačných kanálov

900+ interných expertov

dáta založené na poznatkoch analytikov hrozieb, výskumníkov malvéru a odborníkov na AI

Riešenie

ESET THREAT INTELLIGENCE INVESTIGATION LAB

Služba ESET Threat Intelligence Investigation Lab pomáha analytikom vyhodnocovať podozrivé súbory a indikátory s istotou. **Získajte spoľahlivý druhý názor** podložený telemetriou spoločnosti ESET, informáciami o reputácii a desaťročiami skúseností s analýzou hrozieb bez toho, aby došlo k odhaleniu citlivých dát z vyšetrovania. Pomocou **vyhľadávania indikátorov IoC** získate rýchle odpovede s minimom informačného šumu. Ak potrebujete podrobnejšie dôkazy o aktivite a lepší kontext, môžete využiť komplexnú funkciu **odosielania vzoriek**.

AKO TO FUNGUJE?

Investigation Lab: dospejte k rozhodnutiu rýchlejšie

Služba Investigation Lab je prostredníctvom rozhraní API integrovaná do bezpečnostných nástrojov, ktoré už váš tím používa. Získajte dodatočný kontext k upozorneniam, rozhodnite o ďalšom kroku a odošlite vzorku do sandboxu, ak je potrebná podrobnejšia analýza aktivity.

Váš ekosystém zabezpečenia

- SIEM
- SOAR
- TIP
- Firewall
- XDR

→ API alebo manuálna požiadavka

Investigation Lab

Získajte rýchlu odpoveď

V prípade potreby odošlite vzorku na hĺbkovú analýzu aktivity v sandboxe

→

Konajte s istotou

- Dodatočný kontext
- Zablokovanie
- Izolácia
- Vyšetrovanie
- Uzavretie

HLAVNÉ VÝHODY

Regionálny prehľad

Globálna telemetria spoločnosti ESET poskytuje jedinečný prehľad o regiónoch, ktoré sú často zmieňované len okrajovo, a ponúka dôveryhodné odpovede, ktoré v zdrojoch zameraných predovšetkým na USA nemusia byť dostupné.

Rýchlejšie vyšetrovanie

Desaťročia budovaná infraštruktúra spoločnosti ESET, ktorá spája globálnu telemetriu, spracúvanie dát poháňané umelou inteligenciou a komplexný analytický proces, urýchľuje vyšetrovanie a pomáha rýchlejšie dospieť k praktickým odpovediam.

Dohľad odborníkov

Zatiaľ čo umelá inteligencia urýchľuje analýzu, odborníci spoločnosti ESET priebežne vyhodnocujú a overujú zistenia, aby boli potvrdené indikátory presné, relevantné a pripravené na použitie.

Čo zahŕňa ESET Threat Intelligence Investigation Lab

	Investigation Lab	Investigation Lab Advanced
Cieľová skupina	Tímy, ktoré potrebujú spoľahlivý kontext k indikátorom IoC a príležitostnú hĺbkovú analýzu súborov	Tímy s väčším objemom prípadov a pokročilými požiadavkami na analýzu
Plný prístup k API	Áno	Áno
Vyhľadávanie indikátorov IoC (botnety, C&C servery, domény, IP adresy, URL adresy)	1 000 za deň; 5 000 za týždeň	10 000 za deň; 50 000 za týždeň
Pokročilé vyhľadávanie v databáze spoločnosti ESET	Áno	Áno
Odosielanie vzoriek	50 za deň; 250 za týždeň	500 za deň; 2 500 za týždeň
Hĺbková analýza aktivity	Áno	Áno
Prispôsobenie sandboxu	Nie	Áno
Priorita spracovania v sandboxe	Štandardná	Vysoká
Ochrana vzoriek	Štandardná – vzorka je odstránená; výsledok analýzy a hash zostávajú zachované	Vysoká – vzorka, výsledok analýzy a hash sú odstránené