ATT&CK® Evaluations Enterprise 2024 benadrukt ESET's AI-native benadering van detectie en respons

***Let op:** De meningen en standpunten in deze blogpost zijn van ESET en vertegenwoordigen niet noodzakelijk de zienswijze van MITRE Engenuity.*

De nieuwste editie van de ATT&CK® Evaluations voor Enterprise richtte zich op drie aanvalsscenario's:

- **DPRK-scenario**: cyberespionage op een macOS-systeem.
- **Cl0p-scenario:** ransomware-aanval op een Windows-systeem.
- **LockBit-scenario:** ransomware-aanval in een bedrijfsomgeving met zowel Linux- als Windows-systemen.

ESET Inspect toonde uitstekende zichtbaarheid in alle scenario's en detecteerde elke stap, met een lage totale hoeveelheid meldingen. Dankzij de Incident Creator werden deze meldingen automatisch gebundeld in overzichtelijke incidenten, waardoor security-analisten een helder beeld kregen van de aanvalsstappen.

Methodologie: verbeteringen in realiteitsgetrouwheid

De evaluatie van 2024 introduceerde diverse wijzigingen om beter aan te sluiten bij het werk van security-analisten:

1. **Telemetrie niet meer als detectiecategorie:** Detecties moeten nu aantonen dat een gebeurtenis verdacht of schadelijk is, met concrete details over wat, waar, wanneer en wie.
2. **Testen op false positives:** Benigne substappen worden gebruikt om false positives te identificeren, wat ruis vermindert en precisie bevordert.
3. **Realistische aanvalssimulaties:** Substappen zonder evaluatie werden toegevoegd om een logisch verloop van de aanval te simuleren.
4. **Volume als meetcriterium:** Het aantal meldingen op het dashboard wordt bijgehouden, inclusief hun ernst. Dit ontmoedigt een "detecteer alles"-benadering die leidt tot onnodige meldingen.

Tabel 1. Mapping tussen ATT&CK-evaluatie en ESET Inspect ernstniveaus

ATT&CK-evaluatie	ESET Inspect
Kritiek	Hoog-ernst incident
Hoog	Dreigingsdetectie, gekoppeld aan incident
Medium	Waarschuwing, gekoppeld aan incident
Laag	Info-detectie met score > 22, gekoppeld
Info	Info-detectie met score ≤ 22, gekoppeld

Incidenten die niet aan meldingen gekoppeld zijn, vielen buiten de evaluatie. ESET Inspect richt zich primair op incidenten, met aanvullende informatie als secundair hulpmiddel.

Incidenten en workflow

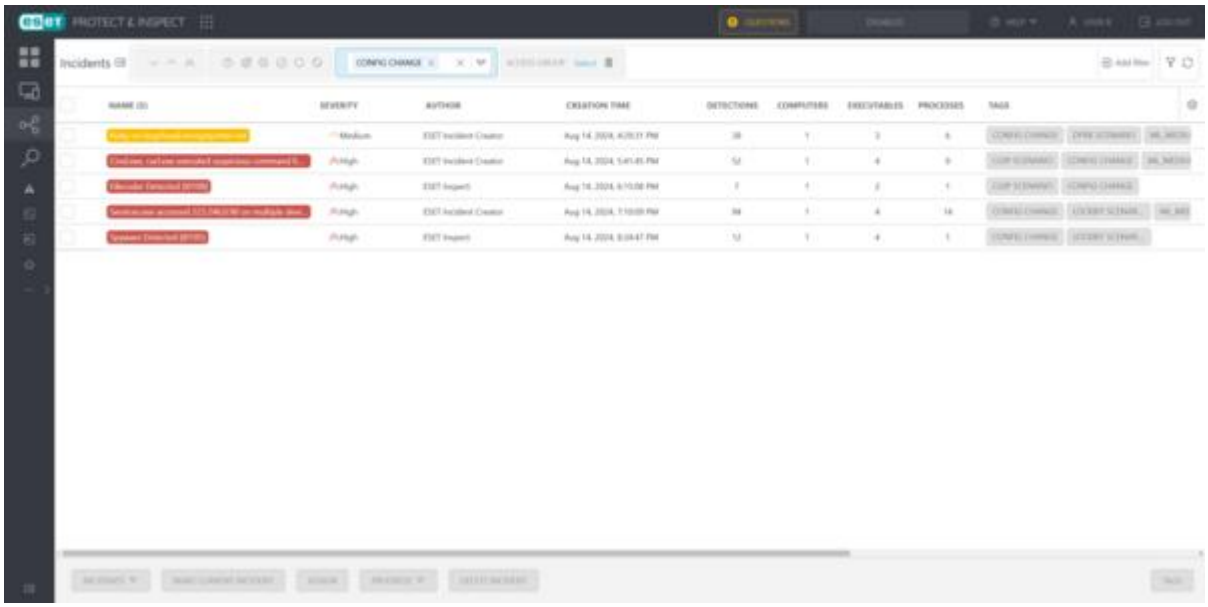
De incidentenweergave is de kern van ESET Inspect. Incidenten worden automatisch gegenereerd via:

1. ESET Incident Creator: Gebruikt AI om detecties te groeperen.
2. Inspect-regels: Meer dan 100 regels die incidenten creëren op basis van getroffen systemen en tijdsperiodes.

Security-analisten werken volgens dit proces:

- Onderzoek elk incident.
- Analyseer, indien mogelijk, niet-gecorreleerde detecties van hoge ernst.

Tijdens de evaluatie konden leveranciers configuraties aanpassen om zichtbaarheid te vergroten en ruis te verminderen. Na deze aanpassingen creëerde Incident Creator slechts één of twee incidenten per scenario, zonder false positives.



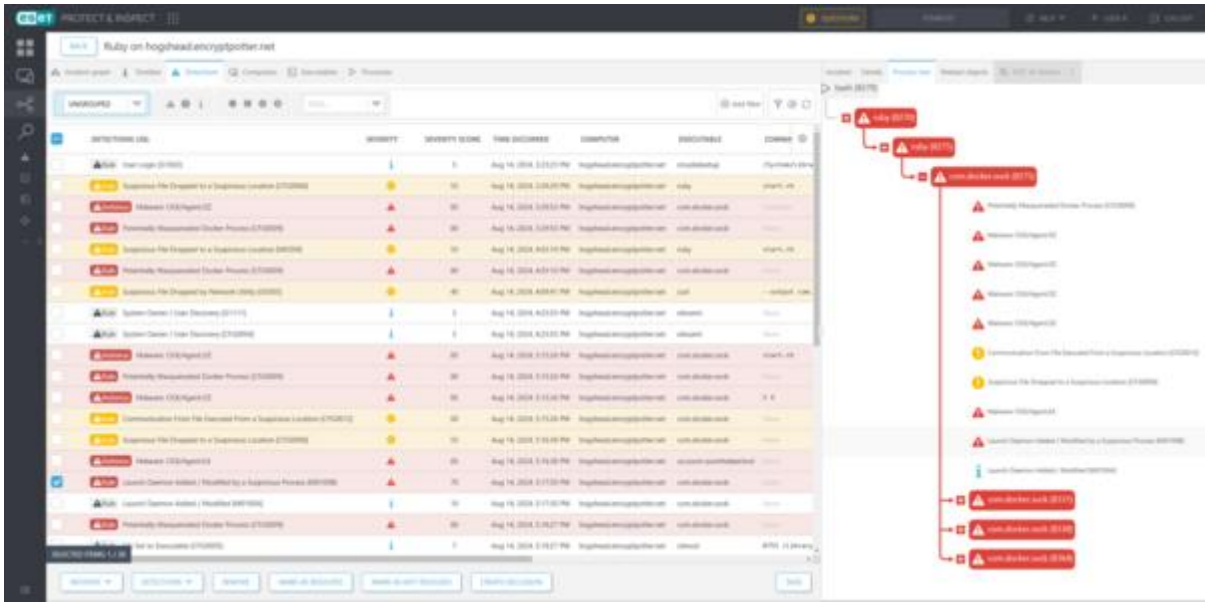
Afbeelding 1. De incidentenweergave in ESET Inspect voor de config change run

Scenarioresultaten

In de volgende secties bespreken we de hoogtepunten van ESET's resultaten in elk scenario.

DPRK

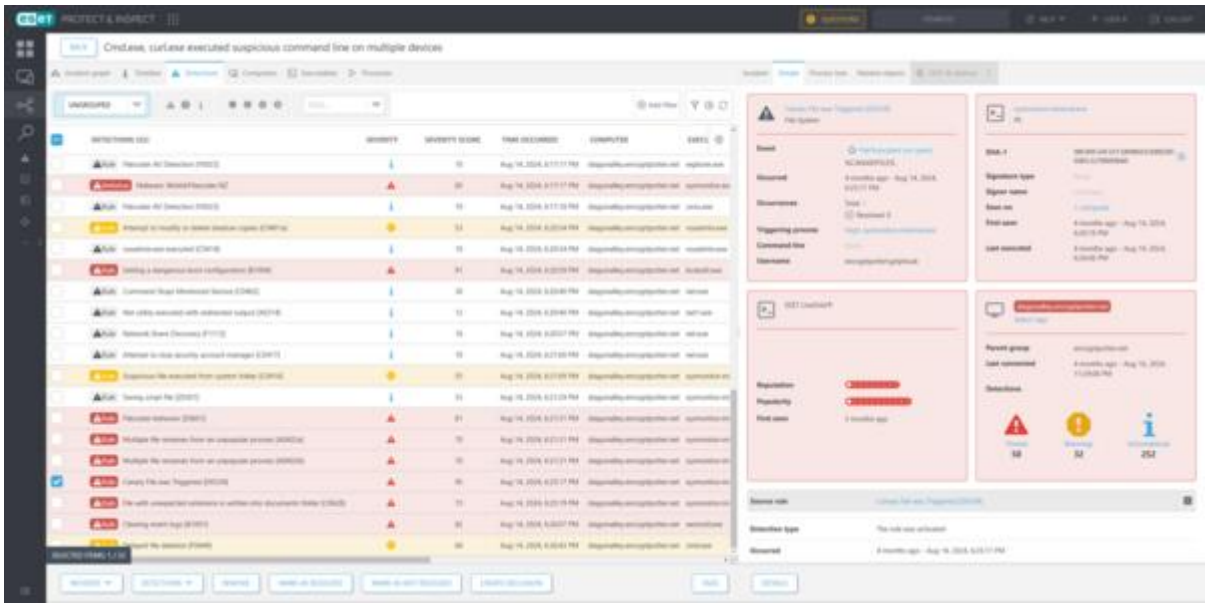
- ESET Inspect behandelde dit als een incident van gemiddelde ernst.
- Hoogtepunten: detectie van backdoors (verkleed als Docker en Zoom), keychain-diefstal, en installatie van tweede backdoor zonder false positives.



Afbeelding 2 toont een deel van het incident voor de detecties die gecorreleerd zijn aan deze aanval, met de nadruk op een detectie voor de FULLHOUSE.DOORED backdoor die persistentie installeert voor een tweede fase backdoor, STRATOFEAR, als een launch daemon.

Cl0p

- Twee incidenten met hoge ernst werden gegenereerd.
- Hoogtepunten: detectie van SDBbot-installaties, verwijdering van schaduwkopieën, uitschakeling van Windows-herstel en uitvoering van Cl0p-ransomware.

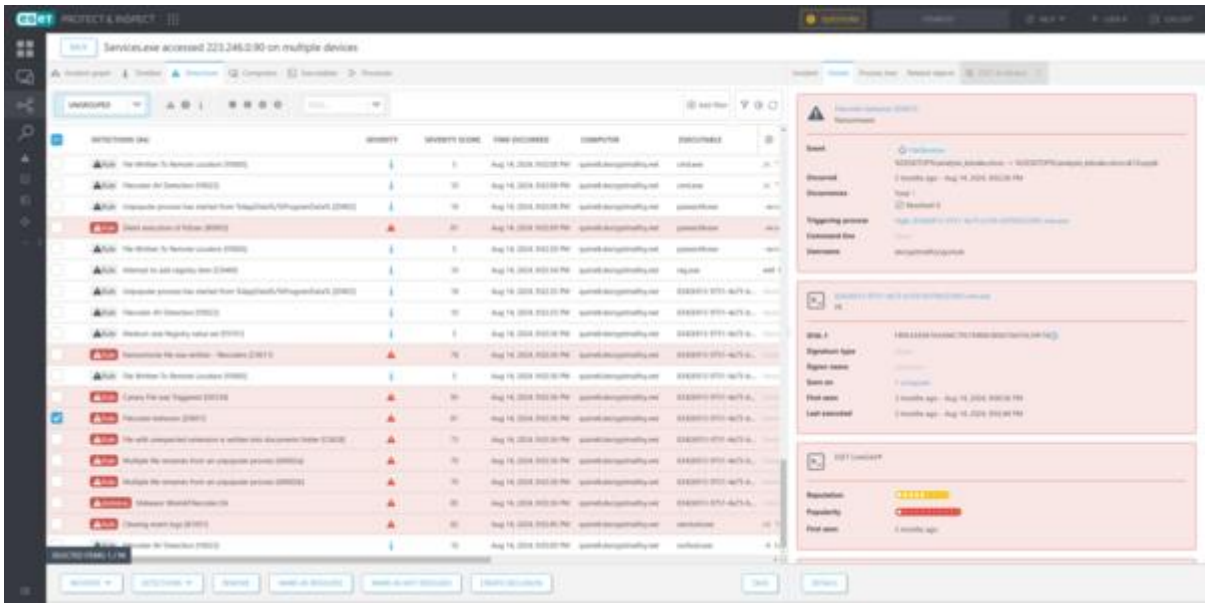


Afbeelding 3 toont een deel van het incident voor de detecties die zijn gerelateerd aan deze aanval, met de nadruk op een detectie voor het schrijven van bestanden of het hernoemen van canary

bestanden voor vroege detectie van de uitvoering van ransomware. De getriggerde regel doodt niet alleen het overtredende proces, maar creëert ook een incident in de weergave Incidenten.

LockBit

- Twee incidenten met hoge ernst werden gegenereerd.
- Hoogtepunten: detectie van aanvaller-login via VNC, SSH-verbindingen, verspreiding van ransomware via PsExec en verwijdering van Windows-logboeken.



Afbeelding 4 toont een deel van het incident voor de detecties die zijn gerelateerd aan deze aanval, met de nadruk op een detectie voor een verdacht proces dat bestanden schrijft of hernoemt met specifieke, zogenaamde dubbele extensies - typisch gedrag van filecoders.

"Bedrijven die het MITRE ATT&CK raamwerk gebruiken, stelt hen instaat om slimmer, sneller en efficiënter om te gaan met cyberdreigingen. Ze zijn beter voorbereid, hebben een verbeterde detectiecapaciteit en versterken hun positie in de steeds complexere cybersecurityomgeving. Bedrijven die het niet gebruiken, missen deze gestandaardiseerde aanpak en lopen een groter risico op succesvolle cyberaanvallen en reputatieschade", volgens Patrick Jonker, Head of Corporate Cybersecurity Solutions van ESET.

De resultaten van ESET Inspect in deze evaluatie onderstrepen de betrouwbaarheid van onze aanpak. Security-analisten kunnen erop vertrouwen dat ze echte bedreigingen effectief aanpakken dankzij helder samengestelde incidenten.