VAN DETECTIE TOT HERSTEL IN 7 STAPPEN

Weet jouw organisatie hoe te reageren wanneer het misgaat?

1. DETECTIE
Het incident wordt gesignaleerd

Een aanval begint vaak stil. Pas als je het weet, kun je handelen — en elke minuut telt. Geautomatiseerde detectie verkort de gemiddelde detectietijd (MTTD) van dagen naar minuten, en beperkt daarmee de impact direct.

Hoe: Microsoft Sentinel verzamelt en correleert logdata uit je hele omgeving. Defender XDR detecteert bedreigingen op endpoints, identiteiten, e-mail en cloud-apps.

2. TRIAGE
De ernst wordt bepaald

Niet elke alert is een crisis. Maar je hebt geen tijd om dat handmatig uit te zoeken. Effectieve triage scheidt ruis van echte dreiging — zodat je team reageert op wat er écht toe doet.

Hoe: Security Copilot analyseert alerts met AI en geeft directe context. Sentinel groepeert gerelateerde alerts automatisch in één incidentweergave.

3. INPERKING
De schade wordt beperkt

Een getroffen systeem is gevaarlijk zolang het verbonden is. Binnen minuten isoleren voorkomt dat de aanvaller zich door je netwerk beweegt — elke seconde dat je wacht, vergroot de schade.

Hoe: Defender for Endpoint isoleert apparaten met één klik. Entra ID blokkeert verdachte accounts of forceert direct een wachtwoordreset.

4. ONDERZOEK
De aanvalsketen wordt blootgelegd

Waar is de aanvaller binnengekomen? Wat heeft hij geraakt? Hoe groot is de scope? Pas als je de volledige kill chain begrijpt — initiële toegang, laterale beweging, data-exfiltratie — kun je het incident echt afsluiten.

Hoe: Sentinel's hunting queries en workbooks ondersteunen deep-dive analyse. Security Copilot genereert incidentsamenvattingen en stelt gerichte onderzoeksvragen voor.

5. HERSTEL

Systemen worden hersteld naar een veilige staat

Herstarten is niet genoeg. Herstel betekent: schone images deployen, getroffen credentials roteren en firewall-regels aanscherpen — én verifieren dat de aanvaller geen persistence heeft achtergelaten. Anders los je het symptoom op, niet het probleem.

Hoe: Defender Vulnerability Management identificeert openstaande kwetsbaarheden. Intune pusht configuratie-updates naar herstelde apparaten.

6. RAPPORTAGE

Het incident wordt gedocumenteerd

Onder NIS2 ben je verplicht significante incidenten binnen 24 uur te melden. Zonder voorbereiding is dat een stressvolle race tegen de klok. Met een gestructureerd rapportageproces lever je tijdig en volledig — en sta je sterk tegenover de toezichthouder.

Hoe: Sentinel genereert geautomatiseerde incidentrapporten met tijdlijn, betrokken entiteiten en ondernomen acties — direct bruikbaar als basis voor je NIS2-melding.

7. EVALUATIE

Het incident wordt geëvalueerd

Een incident dat je niets leert, is dubbel verlies. Een blameless post-mortem, bijgewerkte playbooks en gerichte training maken van elke aanval een investering in weerbaarheid. Zo kom je sterker uit elke crisis.

Hoe: Security Copilot genereert post-incident samenvattingen. Sentinel's analytics rules worden bijgewerkt op basis van nieuwe indicators of compromise (IoC's).

Weet jij hoe jouw organisatie reageert als het er écht op aankomt?

Veel organisaties beschikken al over de juiste Microsoft-tools — maar halen er lang niet alles uit. Tijdens een gratis live SOC demo laat Interstellar je zien hoe detectie en respons er in de praktijk uitzien, en hoe je met je bestaande tooling meer grip krijgt op incidenten.

Ja, ik wil een live SOC demo