

ETeC24: Prevention first, Succes second: Een verhaal over ESET MDR

Tijdens de jaarlijkse interne ESET Technology Conference 2024 (ETeC) werden workshops, seminars en presentaties gehouden die een diepgaande kijk boden op ESET MDR. Experts zoals Gabriel Balla, James Rodewald en Michal Hajovsky deelden inzichten over de evolutie van ESET MDR, hoe het wordt geleverd en de succesverhalen die de waarde ervan aantonen.

De weg naar succes met ESET MDR

Gabriel Balla, productmanager voor Enterprise Solutions, schetste een herkenbaar probleem: IT-beheerders kampen vaak met te veel taken, zoals gebruikersondersteuning, apparaatbeheer en monitoring. Vooral kleine en middelgrote bedrijven (mkb's) hebben het zwaar door:

- **Budgetbeperkingen:** Specialisten zijn duur en schaars.
- **Tijdsgebrek:** Een EDR/XDR-oplossing kan 160.000 meldingen genereren voor een bedrijf met 250 werkplekken, wat leidt tot [waarschuwingsmoeheid](#).
- **Kennisgebrek:** Het herkennen van bedreigingen vraagt expertise en actuele kennis van cyberdreigingen.



Gabriel Balla, Product Manager for Enterprise Solutions and Services, ESET

Ook grote ondernemingen hebben uitdagingen, zoals complexe compliance-eisen en een grotere kans op beveiligingslekken door hun omvang. Rodewald illustreerde dit met een voorbeeld waarin een bedrijf een beveiligingsdienst aanschafte maar vergat deze te implementeren – een kostbare fout.

Waarom kiezen voor MDR?

Michal Hajovsky, global sales lead bij ESET, benadrukte dat 82% van de ransomware-aanvallen gericht is op het mkb. Dreigingen zoals [misbruik van RDP](#) of [MS SQL](#) kunnen zonder malware toegang krijgen tot systemen. Hier is snelle detectie cruciaal:

- Zonder EDR/XDR duurt detectie gemiddeld [277 dagen](#).
- Een intern Security Operations Center (SOC) kan dit verkorten tot 16 uur.
- Met MDR kan detectie en reactie al binnen 30 minuten plaatsvinden.

ESET MDR combineert [topdeskundigen](#), geavanceerde [SOAR/SIEM-tools](#), AI, en actuele dreigingsinformatie. Dit biedt niet alleen snelle bescherming, maar helpt ook bij compliance en verzekeringsvereisten.

ESET MDR in actie

James Rodewald, security monitoring analyst, deelde praktijkverhalen:

- **Case 1:** Verdachte gebruikersaccounts werden toegevoegd aan lokale beheerders via een legitiem ogend [RMM-tool](#). Dankzij ESET MDR werd een ransomware-aanval vroegtijdig gestopt.
- **Case 2:** Een gecompromitteerde MS SQL-server voerde verdachte PowerShell-commando's uit. De MDR-teamleden isoleerden het apparaat en voorkwamen verdere schade. Na onderzoek bleek het om een Mallox-ransomware-aanval te gaan.



James Rodewald, Security Monitoring Analyst, ESET

Preventie als prioriteit

Volgens ESET's gegevens zijn ransomware-aanvallen in de eerste helft van 2024 met 32% toegenomen. Diensten zoals ESET MDR richten zich op preventie door bedreigingen vroegtijdig op te sporen en aan te pakken zonder bedrijfsprocessen te verstoren.

Gabriel Balla vatte het samen: *“Succes in beveiliging betekent zorgeloos werken, zonder constante meldingen. Met ESET MDR blijft alles veilig en overzichtelijk – met groene vinkjes als bewijs.”*