

# Attic MDR

24/7 beveiliging en response op verdachte activiteiten in je Microsoft 365

**Microsoft 365 beveiliging is pas effectief als je verdacht gedrag opmerkt en onderzoekt.**

Cybersecurity draait niet alleen om het hebben van de juiste tools, maar ook om effectieve incidentafhandeling als er een alarmsignaal afgaat.

Regelgeving zoals NIS2 vereist dat bedrijven aantonen dat ze cyberaanvallen detecteren en er snel op reageren. Attic regelt dit. Wij monitoren je Microsoft 365 omgeving 24/7 en volgen alarmen voor je op.

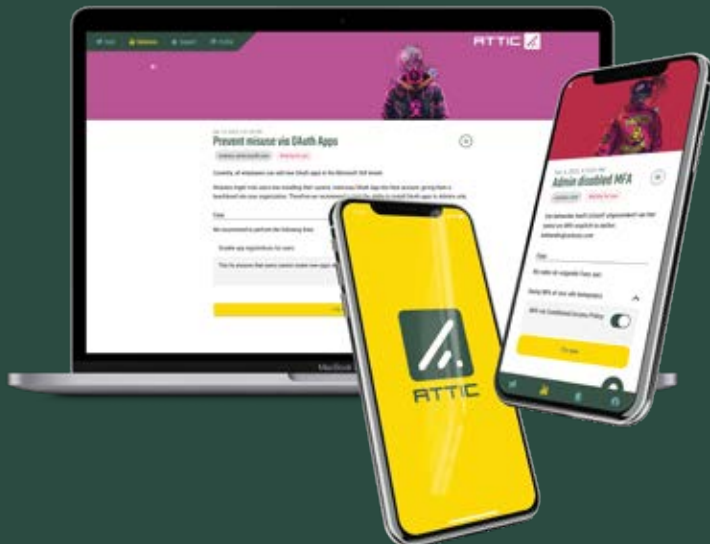


**Microsoft 365**

**Met Managed Detection & Response (MDR) reageren wij direct op verdachte activiteiten.**

Je hebt dan een team dat 24/7 je digitale werkplek bewaakt op cyberdreigingen. Zo voorkomen we proactief schade door hackers, zoals:

- 🚨 Aanmaken van geheime admin-accounts voor blijvende toegang
- 🚨 Uitschakelen van logbestanden om hun sporen uit te wissen
- 🚨 Versturen van nep-facturen naar jouw klanten
- 🚨 Kopiëren van jouw bedrijfsdata naar hun eigen servers
- 🚨 Ransomware aanvallen opzetten vanuit jouw systeem



**Attic MDR bewaakt je digitale werkplek 24/7 en grijpt direct in.**

Attic MDR houdt realtime en grotendeels geautomatiseerd in de gaten of er verdachte activiteiten plaatsvinden in je Microsoft 365 omgeving, de cloud en op apparaten zoals je laptop, desktop en smartphone.

Zien we iets verdachts? Dan grijpen we direct en automatisch in om de hackers te stoppen. Hiermee voorkomen we dat criminelen zorgen voor financiële schade en blijvende reputatieschade.

## Welke beveiliging zit in Attic MDR?

### Bescherming tegen phishing

- ✓ Realtime detectie van fake Microsoft 365 inlogpagina's
- ✓ Waarschuwing met rood alarmscherm bij nep-pagina's
- ✓ Echtheidszegel op échte Microsoft 365 inlogpagina's
- ✓ Push-bericht in de app wanneer een collega een valse pagina bezoekt

### Bescherming tegen inlogpogingen van hackers

- ✓ Monitoring van alle Microsoft 365 inlogactiviteiten
- ✓ Detectie van verdachte inlogpogingen (wie, waar, hoe vaak)
- ✓ Push-bericht bij verdachte inlogactiviteiten

### Online security awareness training

- ✓ Gericht op het herkennen van risico's

### Automatische updates beveiligingscontrole

- ✓ Dagelijkse controle op Microsoft 365 beveiligingsinstellingen
- ✓ Automatische fixes voor beveiligingsproblemen
- ✓ Controle op basis van internationale beveiligingsstandaarden (CIS)
- ✓ Monitoring dat beveiligingsinstellingen correct blijven

### 24/7 bewaking & incidentafhandeling

- ✓ Realtime monitoring van je cloud, apparaten, e-mails, bestanden, Teams, admin-activiteiten en verdachte netwerkverbindingen
- ✓ Directe geautomatiseerde actie zodra iets verdachts gebeurt
- ✓ Langdurige opslag van logs voor forensisch onderzoek
- ✓ Ondersteuning bij de verplichte NIS2 compliance

### Attic app

- ✓ Ontvang meldingen en geef toestemming voor fixes waar je ook bent

## WIJ ZIJN ATTIC SECURITY

Een productgedreven beveiligingsbedrijf voor de praktijk van het mkb. Opgericht door hackers en engineers.

Geen jargon, geen ballast, alleen slimme en schaalbare bescherming waar dat het hardst nodig is.

**€ 300** /maand  
Incl. 100 gebruikers, +€1 per extra



### Cybersecurity made in Europe

Dataproductie, naleving van regelgeving en culturele aansluiting.



### Betaalbare beveiliging door automatisering

Efficiëntie en schaal zonder hoge kosten.



### Attic LAB

Ontwikkeld door hackers en engineers, gericht op automatisering en onderzoek.



### Gericht op Microsoft 365

Maximale bescherming van het platform tegen BEC, datalekken en afpersing.

### Voor wie is Attic MDR geschikt?

- Mkb'ers met een Microsoft 365 omgeving
- Mkb'ers zonder eigen IT-afdeling
- Mkb'ers die zich zorgen maken over hackers, phishing, betaalfraude en ransomware
- Mkb'ers die inzicht willen in wie wanneer inlogt
- Mkb'ers die verdachte inlogpogingen willen detecteren



[atticsecurity.com/mdr](https://atticsecurity.com/mdr)



[support@atticsecurity.com](mailto:support@atticsecurity.com)