24/7 SOC

VOLLEDIGE CYBERBEVEILIGING: DETECTIE EN RESPONS OP MAAT

Stop geavanceerde bedreigingen met Managed SOC, een beheerde detectie- en responsoplossing aangedreven door RocketCyber, het toonaangevende beveiligingsoperatiecentrum dat is afgestemd op de behoeften van moderne MSP's.

24/7 SOC DOOR CYBERSECURITY EXPERTS

24/7 SOC is een detectie- en responsdienst die gebruikmaakt van RocketCyber's Threat Monitoring Platform om kwaadaardige en verdachte activiteiten te detecteren in drie kritieke aanvalsvectoren: Endpoint, Netwerk en Cloud. Ons team van cybersecurity-veteranen jaagt op bedreigingen, beoordeelt ze en werkt samen met jouw team wanneer actie vereist is. Diensten omvatten:

- **Continue Monitoring**
  Rond-de-klok bescherming met real-time geavanceerde dreigingsdetectie.

- **Geavanceerde Beveiligingsstack**
  Speciaal ontwikkeld platform met meer dan 50 jaar beveiligingservaring, geoptimaliseerd voor managed service providers en hun klanten.

- **Inbraakdetectie**
  We vangen geavanceerde dreigingen die traditionele AV- en perimeterbeveiligingsoplossingen omzeilen.

- **Threat Hunting**
  Een elite cybersecurity-team jaagt proactief op kwaadaardige activiteiten zodat jij je kunt richten op andere dringende zaken.

- **Geen Hardware Vereist**
  Octrooiaanmeldende cloud-gebaseerde technologie elimineert de noodzaak van dure en complexe on-premise hardware.

- **Endpointbeveiliging**
  Bescherm je endpoints met Windows- en MacOS-eventlogmonitoring, geavanceerde inbraakdetectie, kwaadaardige bestanden en processen, threat hunting, inbraakdetectie, integraties met next-gen antivirussoftware van derden en meer.

- **Netwerkbeveiliging**
  Verkrijg nieuwe niveaus van netwerkbescherming met firewall- en edge-apparaatlogmonitoring, geïntegreerd met real-time dreigingsreputatie, DNS-informatie en waarschuwingen voor kwaadaardige verbindingen.

- **Cloudbeveiliging**
  Beveilig de cloud met monitoring van beveiligingseventlogs van Microsoft 365, monitoring van Azure AD, detectie van kwaadaardige logins in Microsoft 365 en een algehele Secure Score.

24/7 SOC

BELANGRIJKSTE KENMERKEN

We besparen je tijd en geld door gebruik te maken van je bestaande tools en investeringen in cybersecurity voor endpoints, netwerk en cloud. Dit stelt je in staat om je te concentreren op wat het belangrijkst is – je bedrijf.

SIEMLESS LOG MONITORING

Monitor, zoek, waarschuw en rapporteer over dreigingsvectoren voor endpoints, netwerk en cloud, inclusief belangrijke loggegevens van Windows en MacOS, firewalls, netwerkapparaten, Microsoft 365 en Azure AD – alles zonder dat een SIEM of SIEM-hardware nodig is.

THREAT INTELLIGENCE & HUNTING

Realtime monitoring van dreigingsinformatie, gekoppeld aan premium inlichtingenfeeds, biedt onze klanten de grootste wereldwijde database van dreigingsindicatoren. Dit stelt onze SOC-analisten in staat om aanvallers op te sporen en geavanceerde bedreigingen te identificeren.

BREACH DETECTION

Identificeer tegenstanders die traditionele cyberverdedigingen omzeilen. Wij identificeren aanvallerstactieken, technieken en procedures en stemmen deze af op het MITRE ATT&CK-framework. Hierdoor kunnen onze SOC-analisten indicators of compromise detecteren voordat er schade wordt aangericht.

INTRUSION MONITORING

Realtime monitoring van kwaadaardige en verdachte activiteiten, waarbij indicatoren worden geïdentificeerd zoals verbindingen met terroristische landen, ongeautoriseerde TCP/UDP-diensten, backdoorverbindingen met command-and-control-servers, laterale bewegingen en privilege-escalatie.

NEXT-GENERATION MALWARE

Gebruik je favoriete malwarepreventie of maak gebruik van onze command-and-control-applicatie voor Microsoft Defender, ondersteund door een secundaire verdedigingslinie met onze detectie van kwaadaardige bestanden, tools, processen en meer.

PSA TICKETING

Onze SOC-analisten onderzoeken elke melding, classificeren deze en maken tickets aan voor je PSA-systeem, samen met de details voor herstel, zodat je meer kunt doen zonder extra personeel aan te nemen.

NEEM DIRECT CONTACT MET ONS OP OM MEER TE WETEN TE KOMEN

info@heiper.nl