Orange
Cyberdefense

Managed threat detection: endpoint, firewall, user-identity

MicroSOC

Zichtbaarheid door de hele onderneming is essentieel als het aankomt op threat detection. De snelste manier om zichtbaarheid te krijgen is via endpoint, firewall en user-identities

100% bescherming bestaat niet. Zodra u dit heeft aanvaard, is het tijd om een strategie te implementeren om de bedreigingen te detecteren die u niet kon voorkomen. De uitdaging van detectie is dat er bij de huidige bedreigingen geen gebruik wordt gemaakt van oude malware die gemakkelijk te detecteren en te verhelpen is. Een snelle reactie is echter essentieel.

Uit onderzoek blijkt dat sinds 2018 het aantal file-less malware aanvallen gestaag toeneemt en de verwachting is dat deze trend de komende jaren doorzet. Aangezien het detecteren van file-less malware en vergelijkbare soorten geavanceerde aanvallen niet mogelijk is met statische regels of handtekeningen, hebt u detectie van gedragsafwijkingen nodig.

Dit gedrag moet geanalyseerd en gecorreleerd worden over andere endpoint, firewall en user-identity componenten om de false positives van de daadwerkelijke incidenten te kunnen onderscheiden. Dit kan veel tijd in beslag nemen als u niet over de juiste middelen en competenties beschikt. Als de onderzoeksfase eenmaal is voltooid, vereist elk kritiek incident hoogstwaarschijnlijk ook snelle maatregelen.

In de meeste gevallen is de tijdspanne tussen inbraak, detectie en herstel te lang, waardoor de kosten en schade die voorkomen hadden kunnen worden aanzienlijk toenemen.

* Ponemon 2020 State of Endpoint Security

Service Overzicht

MicroSOC is een Managed Threat Detection service op basis van Extended Detection & Response (XDR) technologie. Door low-impact sensoren op endpoints in te zetten en bestaande investeringen in firewall en user-identity opnieuw te gebruiken; worden gedragsgegevens verzameld, verrijkt en gecorreleerd met behulp van een AI zoekmachine. Door een groot aantal correlaties per seconde uit te voeren, zijn de prestaties ten opzichte van andere detectietoolsets ongeëvenaard.

Dit biedt detectiecapaciteiten die veel verder gaan dan traditionele platforms op basis van signature of regels kunnen aantonen. De uitdaging is echter, dat de detecties niet zo eenvoudig zijn als een “block or allow” proces. In sommige gevallen vereist het handmatig werk van een vakkundige analist om incidenten grondig te verifiëren en te classificeren. Dit is waar het Orange Cyberdefense MicroSOC van pas komt.

Orange Cyberdefense detecteert en reageert 24x7 op dreigingen, gebruikmakend van onze 11 internationale CyberSOC’s, jarenlange ervaring, en uitgebreide Threat Intelligence Datalake. Diepgaande analyse kan ook 8x5 worden voorzien. We werken continu samen met onze klanten om ervoor te zorgen dat we onze endpoint, gateway en identiteitscontrole begrijpen en aanpassen aan hun voortdurend veranderende omgeving.

Door low-impact sensoren op endpoints in te zetten en bestaande investeringen in firewall en user-identity opnieuw te gebruiken; worden gedragsgegevens verzameld, verrijkt en gecorreleerd met behulp van een AI-zoekmachine. Door een groot aantal correlaties per seconde uit te voeren, zijn de prestaties ten opzichte van andere detectietoolsets ongeëvenaard.

Voorkom cyberdreigingen

Detecteer en onderzoek

Reageer en verbeter continue

Uitgebreide endpoint zichtbaarheid: Endpoint, firewall en user-identity detectie op basis van cross-machine correlatie biedt een sterk fundament voor doorlopende security analyse en bedrijfsbrede dekking.

Geavanceerde analyse en opsporing: Gedetailleerde en continue afgestemde detectie verbanden voor snelle en effectieve analyse.

Vakkundige security analisten met de capaciteit om een enorme reeks telemetrie op te vragen.

Snelle time-to-value: MicroSOC biedt security analisten en platformexpertise as-a-service, waardoor u een snelle implementatie en solide, bewezen processen krijgt.

Snelle respons: 24x7 geautomatiseerde detectie en response mogelijkheden en 8x5 diepgaande analyse om bedreigingen te isoleren en de impact van inbreuken te beperken.

Business challenges

- Gebrek aan resources om uw Security Operations Center 24x7 te bemannen
- Voortdurend beheer van de EDR configuratie om voldoende context voor analisten te generen zonder “alert fatigue” te produceren
- Global intelligence toepassen op cybersecurity dreigingen
- Lage volwassenheid door beperkt budget voor cybersecurity personeel en technologie
- Dagelijkse beoordeling van uw firewall, endpoint en identity logs

Wanneer moet u dit overwegen?

- Als u experts nodig heeft voor het implementeren en uitvoeren van een op resultaat gerichte managed detectie en response service op basis van XDR
- Als u 24x7 of 8x5 managed threat response nodig heeft
- Als u op zoek bent naar een leverancier die niet alleen endpoint detectie en response biedt, maar ook log- en netwerkgebaseerde detectie en uitgebreide cyber threat intelligence
- Als u aanvullende 24x7 managed threat resposne capaciteiten wilt

Wat doen wij?

- Implementatie van het MicroSOC platform
- Doorlopende triage, analyse en prioritering van incidenten door security analisten
- Managed threat response zoals isolatie van geïnfecteerde endpoints
- Integratie van het unieke Threat Intelligence Datalake van Orange Cyberdefense en XDR rules op maat
- Monitoring van endpoint, firewall en identity logs

Wat krijgt u?

- Volledig beheerde platform operations
- Real-time analyse van incidenten en actieve reactie op endpoints
- Maandelijkse rapportage
- Optionele Cyber Threat Hunting

Intelligence-led detectie: voordelen

Orange Cyberdefense
Intelligence Backbone

- Kennis van MDR, CERT, CSIRT operations
- Externe data
- Samenwerking met handhaving
- Eigen R&D

Interne activiteiten

- Detectie van verdachte activiteiten
- Analyseren en classificeren van incidenten
- Melding en rapportage

Betere threat detectie

- Geavanceerde kennis van IoC’s
- Identificatie van legitieme processen, die toch gecompromitteerd kunnen zijn (bijv. middels supply chain)
- Vaststelling van de ernst van de situatie
- Anticipatie op en vroege detectie van grootschalige campagnes
- Superieure analyse en correlatie
- Efficiënte filtering van “ruis” en false positives
- 24x7 MicroSOC

For more information check
www.orangecyberdefense.nl

Orange Cyberdefense
Orteliuslaan 1001, 3528 BE Utrecht

info@nl.orangecyberdefense.com
+31 88 1234 200