Whitepaper

Cybersecurity in real-time

Hoe Elastic Security dreigingen detecteert en incidenten voorkomt

1. De onmisbaarheid van real-time cyberbeveiliging

In een wereld waarin cyberdreigingen zich razendsnel ontwikkelen en dagelijks nieuwe aanvalsmethoden ontstaan, is het voor bedrijven van cruciaal belang om hun IT-infrastructuur proactief te beveiligen. Traditionele beveiligingssystemen die achteraf reageren en niet proactief zijn, zijn niet langer voldoende om schade te voorkomen. Elastic Security biedt een oplossing door real-time dreigingsdetectie, incidentrespons en geavanceerde monitoring, waardoor bedrijven potentiële dreigingen kunnen zien aankomen en aanvallen kunnen voorkomen voordat ze ernstige schade aanrichten.

Waarom Elastic Security?

Elastic Security is ontworpen om grote hoeveelheden data te verwerken en maakt gebruik van geavanceerde SIEM (Security Information and Event Management) om afwijkend gedrag en dreigingen in real-time te detecteren. Met deze technologie kunnen organisaties hun beveiligingsinspanningen uitbreiden en tegelijkertijd voldoen aan complexe compliance-eisen, zoals de AVG/GDPR.

In dit whitepaper

In dit whitepaper ontdek je hoe Elastic Security bedrijven beschermt tegen cyberdreigingen door middel van real-time dreigingsdetectie en incidentrespons. We behandelen de belangrijkste functies van Elastic Security, waaronder SIEM en endpoint security, en geven inzicht in de technische architectuur en schaalbaarheid van het platform.

De impact van deze dreigingen kan variëren van datalekken en productiviteitsverlies tot forse reputatieschade en financiële boetes.

2. Het cyberdreigingslandschap

Cyberaanvallen worden steeds geavanceerder, met hackers die gebruikmaken van nieuwe technieken zoals ransomware, phishing, DDoS-aanvallen, en social engineering. Zelfs de meest beveiligde netwerken kunnen kwetsbaar zijn, zonder een adequate, proactieve aanpak.

Cyberdreigingen: wat staat er op het spel?

Cyberaanvallen vormen een directe bedreiging voor bedrijven van elke omvang. Van datalekken tot operationele stilstand: de impact van een aanval kan verwoestend zijn en de reputatie en continuïteit van een organisatie ernstig schaden. Wat zijn de meest voorkomende dreigingen waarmee bedrijven vandaag de dag worden geconfronteerd?

- **Ransomware:** Aanvallen waarbij hackers toegang verkrijgen tot cruciale bedrijfsinformatie en deze versleutelen, om vervolgens losgeld te eisen.
- **Phishing:** Gerichte aanvallen via e-mail waarbij vertrouwelijke gegevens worden buitgemaakt door middel van valse communicatie.
- **DDoS-aanvallen:** Aanvallen die systemen overspoelen met verzoeken, waardoor diensten onbeschikbaar raken.
- **Insider threats:** Medewerkers of partners die bewust of onbewust toegang verschaffen aan kwaadwillenden.

Waarom traditionele beveiliging faalt

Veel bedrijven vertrouwen nog steeds op traditionele beveiligingssystemen die reactief werken. Deze oplossingen detecteren een aanval pas nadat deze al heeft plaatsgevonden, wat resulteert in verloren data en downtime. Elastic Security doorbreekt dit patroon door dreigingen in real-time op te sporen, nog voordat ze schade kunnen aanrichten.

Elastic Security, jouw schild tegen cyberdreigingen

Elastic Security is een robuust platform dat organisaties in staat stelt om data uit verschillende bronnen te verzamelen, analyseren en te monitoren, voor het detecteren van dreigingen. Elastic Security integreert verschillende beveiligingsfuncties, zoals SIEM, endpoint security, en compliance-tools, om real-time bescherming te bieden tegen cyberdreigingen.

3. Elastic Security-features

De beveiligingsfuncties van Elastic Security om real-time bescherming te bieden tegen cyberdreigingen:

1. SIEM

SIEM is het hart van Elastic Security en biedt een gecentraliseerde oplossing voor het verzamelen, analyseren en monitoren van beveiligingsdata. Het verzamelt logs en gebeurtenissen van verschillende bronnen – zoals netwerkapparatuur, applicaties, en endpoints – en analyseert deze om dreigingspatronen te identificeren.

Elastic SIEM monitort voortdurend netwerkactiviteit en detecteert afwijkend gedrag dat kan wijzen op een dreiging, zoals ongebruikelijke inlogpogingen, verdachte netwerkverzoeken, of wijzigingen in configuraties. Zodra een verdachte gebeurtenis wordt gedetecteerd, genereert SIEM een waarschuwing en stelt teams in staat om direct in te grijpen.

2. Endpoint Security

Endpoint Security biedt bescherming voor alle aangesloten apparaten binnen een netwerk, van laptops tot mobiele apparaten en servers. Deze oplossing beveiligt deze apparaten tegen dreigingen zoals malware, ransomware, en phishing.

Elastic Security monitort elk apparaat in real-time, verzamelt data en detecteert afwijkende activiteiten, zoals ongewone netwerkverbindingen of verdachte bestandsoverdrachten. Het systeem kan automatisch actie ondernemen, zoals het blokkeren van een verdachte verbinding, of het isoleren van een geïnfecteerd apparaat.

Endpoints zijn vaak een toegangspunt voor aanvallen. Het is essentieel om elk apparaat binnen een netwerk actief te monitoren en te beveiligen.

Elastic Security-features

De beveiligingsfuncties van Elastic Security om real-time bescherming te bieden tegen cyberdreigingen:

3. Compliance Management

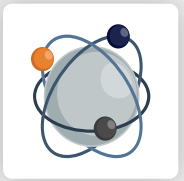
Elastic Security biedt uitgebreide mogelijkheden voor het monitoren en rapporteren van compliance-vereisten, zoals AVG/GDPR, HIPAA of PCI DSS. Door audit trails te genereren en te analyseren, helpt het organisaties om te voldoen aan wettelijke en sectorale voorschriften.

Elastic Security verzamelt gedetailleerde logs over toegangspogingen, dataveranderingen en netwerkactiviteiten. Deze informatie wordt geanalyseerd om ervoor te zorgen dat de juiste procedures worden gevolgd, en dat gevoelige data veilig worden opgeslagen en verwerkt.

4. Threat Intelligence-integratie

Elastic Security kan dreigingsinformatie (Threat Intelligence) integreren om te helpen bij het identificeren van bekende aanvallen, malware en kwaadwillende IP-adressen. Het systeem vergelijkt activiteiten in het netwerk met gegevens van externe bronnen, om kwaadaardige activiteiten sneller te detecteren.

De Threat Intelligence-feed wordt voortdurend geüpdatet met de laatste dreigingsinformatie. Wanneer Elastic Security een patroon herkent dat overeenkomt met een bekende dreiging, wordt het IT-team onmiddellijk gewaarschuwd. Door voortdurend op de hoogte te zijn van de laatste cyberdreigingen, kunnen organisaties preventief maatregelen nemen om aanvallen te voorkomen.



4. Case in de gezondheidszorg

Casus

Een middelgroot bedrijf in de gezondheidszorg had moeite met het beveiligen van zijn groeiende IT-infrastructuur. Het bestaande beveiligingssysteem kon cyberaanvallen niet in real-time detecteren, wat leidde tot meerdere beveiligingsincidenten. Het bedrijf had behoefte aan een oplossing die het proactief kon beschermen tegen dreigingen, en het tegelijkertijd in staat zou stellen om aan strenge regelgeving te voldoen.

Uitdagingen

- Detectie van cyberdreigingen in real-time.
- Behoefte aan endpoint security voor alle aangesloten apparaten.
- Naleving van privacy- en beveiligingsvoorschriften (AVG).

Oplossing

Puur Data implementeerde Elastic Security, inclusief SIEM en endpoint security, waarmee het bedrijf real-time monitoring en bescherming kon realiseren. Elastic Security stelde het IT-team in staat om verdachte activiteiten onmiddellijk te identificeren, en om actie te ondernemen voordat er schade kon ontstaan.

Resultaten

Real-time detectie van dreigingen:
Het bedrijf kon potentieel schadelijke activiteiten identificeren voordat deze tot een incident leidden.

Verbeterde compliance:
Dankzij de uitgebreide logging en monitoring kon het bedrijf voldoen aan alle relevante regelgeving.

Proactieve beveiliging:
Incidenten werden gehalveerd in de eerste zes maanden na implementatie, wat leidde tot een significante vermindering van kosten voor schadeherstel.

5. Jouw voordelen van Elastic Security

Elastic Security biedt tal van voordelen die cruciaal zijn voor organisaties die hun IT-infrastructuur willen beschermen tegen moderne cyberdreigingen:

Real-time inzicht

Door continu dataverkeer en netwerkactiviteiten te monitoren, zorgt Elastic Security voor direct inzicht in mogelijke dreigingen. Dit stelt bedrijven in staat om snel te handelen en cyberaanvallen te voorkomen.

Proactieve beveiliging

Elastic Security geeft bedrijven de tools om cyberdreigingen vroegtijdig te identificeren. Dit voorkomt dat aanvallen escaleren en maakt het mogelijk om snel maatregelen te treffen.

Schaalbaarheid

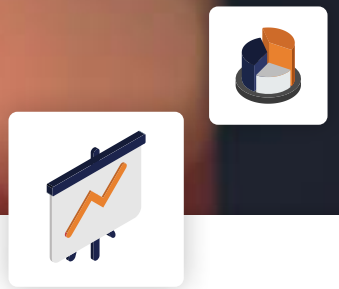
Elastic Security groeit mee met je organisatie, of je nu een kleine IT-omgeving hebt of een uitgebreide, wereldwijde infrastructuur. Het platform is ontworpen om zowel kleine als grote hoeveelheden data te verwerken.

Compliance waarborgen

Voldoen aan regelgeving, zoals de AVG, is essentieel voor bedrijven die persoonlijke en gevoelige gegevens verwerken. Elastic Security biedt uitgebreide audit- en loggingtools om naleving van wet- en regelgeving te waarborgen.

6. Bescherm je organisatie vandaag nog

De toenemende complexiteit van cyberdreigingen vraagt om een proactieve aanpak. Elastic Security biedt de tools om je IT-infrastructuur te beschermen door middel van real-time dreigingsdetectie en krachtige beveiligingsoplossingen. Of je nu wilt voldoen aan strenge regelgeving, zoals de AVG, of je je wilt beschermen tegen de nieuwste cyberaanvallen, Elastic Security helpt je om de controle te houden.



Ondersteuning door Puur Data

Als Elite Partner van Elastic biedt Puur Data niet alleen de technologie, maar ook de expertise om ervoor te zorgen dat je Elastic-omgeving optimaal functioneert. Ons team staat klaar om je te helpen met de implementatie, optimalisatie, en voortdurende ondersteuning van Elastic Security.

Over Puur Data

Puur Data is een toonaangevende Elite Partner van Elastic. Onze missie is om organisaties te helpen meer waarde te halen uit hun data door middel van innovatieve en schaalbare oplossingen. Met onze diepgaande kennis van Elastic-producten, zorgen wij ervoor dat bedrijven optimaal beschermd zijn tegen cyberdreigingen en altijd voldoen aan de strengste compliance-eisen. Puur Data biedt een pragmatische en efficiënte aanpak, afgestemd op de specifieke behoeften van jouw organisatie.

Neem contact op met Puur Data om te ontdekken hoe wij jouw organisatie kunnen helpen met Elastic Security.

Puur Data
Argonstraat 28
6718 WT Ede
T +31 (0)88-7887328
E info@puurdata.nl