Stageopdracht

Plan van aanpak

Reno Goeyvaerts & Robbe Sas | 2023-2024

vanroey

INHOUDSTAFEL

vanroey

Inleiding

In deze stageopdracht staat de vergelijking tussen Microsoft Defender en SentinelOne centraal, waarbij we niet alleen de traditionele EDR-functies bekijken, maar ook de volledige XDR-mogelijkheden onder de loep nemen. De focus ligt op het in kaart brengen van de verschillende SKU's en hun features, het onderzoeken van de mogelijkheden voor centraal beheer en het vergelijken van de deployment-methoden van beide producten. Daarnaast zal er getest worden op de effectiviteit van de producten tegen verschillende dreigingen, waaronder een evaluatie van het threat hunting proces en de gebruiksvriendelijkheid van de portals. Verder wordt aandacht besteed aan de vergelijking tussen S1 RangerAD en Defender for Identity, en aan de integratiemogelijkheden met Intune, Entra ID, en andere systemen. Optionele uitbreidingen van de opdracht omvatten het implementeren van CIS-Benchmarks op Windows Server en het afstemmen van de producten op het CyberFundamentals Framework.

Situatieschets

Aanleiding

De klant komt vragen bij VanRoey voor het gehele bedrijf op IT-vlak te beveiligen. Er wordt dus onrechtstreeks gevraagd naar een XDR-oplossing. Op het moment zijn er veel van deze XDR-oplossingen beschikbaar op de markt. Daarom is het ook belangrijk om hierin de juiste keuze te maken naargelang de productkwaliteit en de behoeftes van de klant.

Hoofdvraag/deelvragen

Wij gaan twee van deze XDR-vendoren onderzoeken en hieruit conclusies trekken, namelijk Microsoft Defender en SentinelOne. Zo kan er op de vraag "Welke XDR-vendor past het beste?" geantwoord worden. Eerst moeten wij natuurlijk bekend raken met deze technologieën vooraleer er een definitieve conclusie gemaakt kan worden. Dit gaat dan ook verder dan gewoon het product op grote schaal te bekijken, maar ook welke integratiemogelijkheden er ter beschikking zijn en deze zelf testen.

Het ideale eindresultaat

Onze stage loopt voor de volle 13 weken. Binnen deze periode willen wij natuurlijk een mooi resultaat leveren waar zowel wij als het stagebedrijf tevreden mee zullen zijn. Daarvoor willen wij het uiteindelijke beeld al eens schetsen. Hierdoor krijgen wij, maar ook jullie, een goede visualisatie van wat we nu juist willen realiseren.

Hoofddoel

Het voornaamste doel van deze opdracht is om op de vraag “Is Microsoft Defender of SentinelOne de meest gepaste oplossing?” te kunnen antwoorden gebaseerd op de grote en vereisten van de klant in kwestie. Hiervoor zullen wij, aan de hand van een eigen opgezette sandbox omgeving, de nodige situaties nabootsen zodat wij hierop een duidelijk en correct antwoord kunnen geven. Wij willen uiteindelijk zowel de grootte, maar ook zeker de minder duidelijk verschillen aankaarten zodat wij hier de voordelen en nadelen uit kunnen concluderen. Dit zal gedaan worden in perspectief van de beheerder naar de klant toe. Ook zal er uitgelegd worden wat de mogelijkheden zijn voor de beheerder. Dit zal ondersteund worden met behulp van een demonstratie. Tijdens

deze demonstratie zullen wij ook tonen wanneer er een product door het systeem wordt tegengehouden, aanvullend met Threat Hunting. Maar ook de integratiemogelijkheden met onder andere Intune en Entra ID.

Uitbreiding

Wanneer we klaar zijn met de hoofdopdracht, kunnen wij nog aan de slag met extra uitdagingen. Eén van deze uitdagingen is het onderzoeken van CIS-Benchmarks binnen Windows Servers. Deze benchmarks bevatten een reeks regels die worden toegepast op een systeem om de beveiliging te evalueren. We onderzoeken wat deze benchmarks wel en niet kunnen en waar er zeker rekening mee gehouden moet worden. Dit zal opnieuw uitbundig getest worden door ons zodat wij hier een mooie conclusie van kunnen maken.

Verder is er nog een uitdaging voorzien. Deze houdt in dat we aan de hand van het CyberFundamentals Framework[1] kijken of VanRoey deze implementaties intern heeft geïmplementeerd. Dit framework stelt maatregelen op voor bedrijven om zo de kans op cyberaanvallen te verkleinen. Zij beweren tussen de 82% en 100% van aanvallen te kunnen tegenhouden door middel van hun fundamentele guides naarmate welk level je kiest. Je hebt keuze uit Basic, Important en Essential. Wij gaan tenslotte elk van deze maatregelen overlopen en indien deze niet worden toegepast, documenteren we de nodige implementaties die moeten worden toegepast.

Onderzoek

In het begin van onze stageopdracht duiken we diep in de wereld van Microsoft Defender en SentinelOne. We zijn bezig met het onderzoeken van allerlei aspecten van beide programma's, zodat we straks een goed geïnformeerde vergelijking kunnen maken.

1. Stock Keeping Units (SKU's):
    - Beschikbare SKU's voor elke oplossing
    - Functies en mogelijkheden per SKU
    - Prijsstelling en licentiestructuur voor elke SKU
2. Features
    - Detectie- en preventiemogelijkheden (bijv. malware, ransomware, zero-day threats)
    - Beheerfuncties voor bedreigingen (bijv. quarantaine, blokkering, herstel)
    - Geavanceerde analysemogelijkheden (machine learning, threat hunting)
    - Rapportage- en dashboardfunctionaliteit
3. Management
    - Centrale beheerconsole en gebruikersinterface
    - Rollen en machtigingen voor gebruikersbeheer
    - Integratie met bestaande beheertools (bijv. Microsoft Intune, Entra ID)
4. Deployment
    - Beschikbare deployment modellen
    - Implementatieprocessen en vereiste infrastructuur
    - Schaalbaarheid en flexibiliteit van de oplossing

[1] 'CyberFundamentals Framework', atwork.safeonweb.be

5. Integratie
    - Ingebouwde integraties met Microsoft Intune en Entra ID
    - Mogelijkheden voor integratie met 3rd party tools (bijv. SIEM, SOAR)
    - Open API's voor custom integraties
6. Protection
    - Beschermingsmogelijkheden voor verschillende endpoints (bijv. Windows, macOS, Linux, servers)
    - Mobile device management (MDM) en beveiligingsfuncties
    - Databeveiliging en privacy-aspecten

Vergelijking:

Na het verzamelen van alle informatie, zullen we een gedetailleerde vergelijking maken van beide oplossingen. We beoordelen de sterke en zwakke punten van elk platform op basis van de onderzochte criteria door middel van zowel websites en documentatie dat online te vinden is en ons eigen onderzoek.

Testing

In deze fase van onze stageopdracht verdiepen we ons in de praktische werking van Microsoft Defender en SentinelOne. We configureren en testen beide oplossingen in een gecontroleerde omgeving om hun functionaliteit en prestaties te evalueren.

1. Opstelling van testomgeving:
    - Twee groepen van Windows virtuele machines (VM's) worden gecreëerd op Azure.
    - Twee on-premise Windows 11 laptops
    - Een tenants opgesplitst in:
        - Groep 1: Microsoft Defender XDR
        - Groep 2: SentinelOne XDR
2. Te testen criteria
    - Features
        - Detectie- en preventiemogelijkheden (malware, ransomware)
        - Beheersfuncties voor bedreigingen (quarantaine, blokkering, herstel)
        - Geavanceerde analysemogelijkheden (machine learning, threat hunting)
        - Rapportage- en dashboardfunctionaliteit.
    - Management
        - Gebruiksgemak van de control panel
        - Role based access control
    - Integratie
        - Intune
        - Entra ID
        - 3rd party tools (SIEM, Soar)
        - API's voor custom integraties
    - Deployment
        - Eenvoudigheid van het implementatieproces

        - Schaalbaarheid en flexibiliteit van de oplossing
3. Uitvoering van tests:
    - Simulatie van realistische cyberaanvallen op beide VM-groepen
    - Observatie en analyse van de detectie- en responstijden van beide oplossingen
    - Beoordeling van de bruikbaarheid en efficiëntie van de management tools
    - Evaluatie van de integratiemogelijkheden met Entra ID en 3rd party tools
4. Documentatie van bevindingen

Documentatie

In deze cruciale fase van het project consolideren we alle bevindingen uit de voorgaande stadia en komen we tot een weloverwogen keuze voor de XDR-oplossing die het best aansluit bij de behoeften, budget en grootte van de klant.

1. Analyse van verzamelde data:
    - We herzien de bevindingen uit de onderzoeks- en testingfase.
    - We analyseren de features, beheer, integratie, deployment en beschermingsmogelijkheden van beide XDR-oplossingen.
    - We vergelijken de prestaties van Microsoft Defender en SentinelOne op basis van de uitgevoerde tests.
2. Beoordeling op basis van klantcriteria:
    - We nemen de specifieke noden van de klant in overweging, inclusief:
        - Bedrijfstak en potentiële bedreigingen
        - Aantal gebruikers en apparaten
        - Beschikbare budget en technische expertise
        - Integratievereisten met bestaande systemen
        - Beveiligingsbehoeften en gewenste functionaliteiten

Begripsdefinities

XDR

XDR (Extended Detection and Response) is een geïntegreerde cybersecurity-oplossing die gegevens verzamelt en correleert over meerdere beveiligingslagen, zoals e-mail, endpoints, servers, cloud-workloads en netwerken. Dit zorgt voor snellere detectie van bedreigingen en verbeterde onderzoeks- en reactietijden door middel van beveiligingsanalyse[2]. XDR is een krachtige verdediging tegen geavanceerde aanvallen, dit doet hij door naar subtiele indicatoren te kijken, het gebruik van geavanceerde bedreiging en detectietechnieken, het automatiseren van reacties en het integreren met andere beveiligingstools[3] . Het werkt door gegevens van verschillende beveiligingstools te verbinden met één groot platform. Zo staat het securityplatform dat de endpoints beveiligd in verbinding met de identity beveiliging.

[2] 'What is XDR', trendmicro.com
[3] 'What Is Extended Detection and Response', paloaltonetworks.com

Stock Keeping Units

Standalone Stock Keeping Units verwijst naar een vooraf gedefinieerde sjabloon die gebruikt wordt voor het uitgeven van individuele softwarelicenties. Het schetst een beeld over alle essentiële aspecten van een licentie:

- Product versie
- Features
- Omgeving (standalone, network, device specific or cloud)
- Levenscyclus (licentie)

Deployment

Deployment in IT verwijst naar het proces om software of updates beschikbaar te maken voor de beoogde gebruikers. Dit omvat een reeks stappen, waaronder het uitbrengen van software, installatie, configuratie, testing, uitrollen en prestatiemonitoring.[4]

Protection

Met Protection bedoelen wij de verschillende inbegrepen features en tools die gebruikt worden om de IT-omgeving veiliger te maken.

Meeting

We hebben op vrijdag 08/03 een meeting met Roel Van Looy over de verschillende subscriptions die VanRoey aanbiedt van Microsoft Defender XDR en SentinelOne XDR zodat we in onze vergelijkingen en het onderzoek een duidelijk beeld krijgen naar wat we moeten kijken.

Finalisatie

In deze fase gaan we de besluiten van de onderzoeksfase en de sandboxfase met elkaar vergelijken en hieruit een algemeen besluit trekken bepaald door het budget, de grote en de eisen van het bedrijf in kwestie.

Conclusie

In conclusie streven we ernaar dit project succesvol af te ronden en een resultaat te behalen waar zowel onze opdrachtgever als wijzelf tevreden mee zijn. We zetten ons volledig in om de doelstellingen van het project te bereiken door middel van nauwkeurige planning en toegewijde uitvoering. Door samen te werken en voortdurend te streven naar verbetering, geloven we dat we een oplossing kunnen vinden die aan de verwachtingen voldoet en waar alle betrokken partijen profijt van hebben.

[4] 'What is Deployment', umbraco.com

Bronnen

CyberFundamentals Framework. (z.d.). SafeOnWeb. Geraadpleegd op 29 februari 2024. van https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

Discover what software deployment is. (2023, 20 december). Sumo Logic. Geraadpleegd op 29 februari 2024. van https://www.sumologic.com/glossary/software-deployment/#:~:text=Software%20deployment%20includes%20all%20of,of%20manual%20and%20automated%20processes.

What is Deployment. (2021, 27 augustus). Umbraco. Geraadpleegd op 29 februari 2024. van https://umbraco.com/knowledge-base/deployment/

What is software deployment. (2023, 26 juni). PagerDuty. Geraadpleegd op 29 februari 2024. van https://www.pagerduty.com/resources/learn/what-is-software-deployment/