De selectie van een SIEM oplossing voor het centraliseren van de beveiliging

Onderzoeksvoorstel Bachelorproef 2021-2022

Wout Engels[1]

Samenvatting
In dit onderzoek zal er gezocht worden hoe men de beveiliging van een bedrijf kan verbeteren met behulp van een SIEM (Security Information and Event Management) oplossing. Met de toenemende groei in het gebruik van Cloud services komt automatisch ook een toename in de mogelijkheden voor hackers. Dit vergt dus logischer wijs ook een toename in de beveiliging van je services. We gaan verschillende SIEM oplossingen bekijken en deze beoordelen op verscheidene criteria die belangrijk zijn voor een bedrijf dat handelt met gevoelige gegevens. Daarnaast gaan we bekijken of er tekortkomingen zijn in huidige SIEM oplossingen en of er verbeteringen nodig zijn aan bepaalde onderdelen. Ik verwacht dat de SIEM oplossingen een hoop problemen gaan oplossen rond het centraliseren van beveiliging en de snelheid waarmee gaat kunnen gehandeld worden op mogelijk beveiligingsrisico's.

Sleutelwoorden
Onderzoeksdomein. Systeembeheer — Netwerkbeheer — SIEM

Co-promotor
Dennis Wagelaar[2] (Corilus NV)

Contact: [1] wout.engels@student.hogent.be; [2] dennis.wagelaar@corilus.be;

Inhoudsopgave

1. Introductie

Beveiliging in je infrastructuur is meer en meer een prioriteit aan het worden binnen bedrijven. Men ziet dagelijks in het nieuws voorbeelden van hoe het fout kan lopen en welke gevolgen dit kan hebben voor een bedrijf. Dit kan gaan van enorme extra kosten tot schade aan het bedrijfsimago. In bedrijven met complexe infrastructuur kan het onoverzichtelijk worden voor beveiligingsspecialisten om alle waarschuwingen manueel te blijven bekijken. Misschien zijn er bepaalde onderdelen die nood hebben aan verbetering? Zijn er gewoonweg tekortkomingen? Dit ga ik proberen uitzoeken door een gepaste SIEM oplossing te zoeken voor Corilus NV. Door middel van een implementatie van SIEM zullen we dus waarschijnlijk meer duidelijkheid scheppen in waarschuwingen door context rijke logbestanden en zo tijd en geld besparen.

2. State-of-the-art

Veel SIEM oplossingen bieden een gebruiksvriendelijke omgeving aan. Visualisatie en reactievermogen zijn echter nog gelimiteerd om met de enorme hoeveelheid data om te kunnen gaan. Deze oplossingen bieden goede data opslag, maar vaak ten kosten van een hogere prijs. Elastic SIEM[1] oplossingen worden gezien als een veelbelovend alternatief voor dit probleem. (González-Granadillo e.a., 2021)

Bescherming van kritische infrastructuur is één van de belangrijkste uitdagingen van de afgelopen jaren. Security Information and Event Management (SIEM) systemen worden hiervoor al veel gebruikt. Hiermee kunnen ze realtime monitoring uitvoeren. SIEM oplossingen zijn een combinatie van de eerdere heterogene product categorieën Security Information Management (SIM) en Security Event Management (SEM). SEM dient voor de aggregatie van gegevens tot een beheersbare hoeveelheid informatie. Met deze informatie kunnen beveiligingsproblemen dan onmiddellijk opgelost worden. SIM dient voornamelijk om historische data te analyseren om de effectiviteit en efficiëntie van informatiebeveiligingsinfrastructuur op lange termijn te verbeteren. (Garofalo e.a., 2014)

Een van de voornaamste kenmerken van de SIEM oplossingen zijn hun geavanceerde mogelijkheden voor logbeheer. Logboek management is het proces van het omgaan met grote hoeveelheden computer gegene-

[1] https://www.elastic.co/siem/

reerde logberichten. De belangrijkste problemen met logbeheer is meestal het enorme volume van de loggegevens en de diversiteit van de logs. Een SIEM oplossing correleert, analyseert en rapporteert informatie van verschillende gegevensbronnen zoals netwerkapparaten, besturingssystemen, applicaties,... Het eindresultaat is een holistische kijk op informatiebeveiliging binnen het bedrijf.
(Cerullo e.a., 2014) en (Mavroeidis & Jøsang, 2021)

Uit de eerdere citaten blijkt dat er al heel wat onderzoek is gedaan naar SIEM. Velen concluderen dat er toch een aantal tekortkomingen zijn. SIEM werkt op homogene data maar kan niet goed rekening houden met data die uit meerdere lagen. Daarnaast zijn er vaak nog context problemen waardoor er geen duidelijkheid is over de ernst van de waarschuwingen. We gaan onderzoeken welke SIEM oplossing het best is voor gebruik in een bedrijfsomgeving met gevoelige gegevens.

3. Methodologie

Voor dit onderzoek zullen enkele simulaties uitgevoerd worden. Bij elke simulatie ga ik een andere SIEM oplossing gebruiken. Als er duidelijke tekortkomingen zijn, zal er gezocht worden naar een bijhorende tool om dit te verhelpen. Er zal getest worden op basis van volgende criteria:

- Gebruiksvriendelijkheid
- Kosten
- Duidelijkheid van context
- Mogelijkheid tot automatisatie
- Snelheid van verwerken data

Een aantal tools die getest zullen worden zijn Elastic SIEM met Kibana[2], Wazuh[3] met Kibana. Andere tools die misschien gebruikt gaan worden zijn SolarWinds Security Event Manager[4] en Datadog Security. Monitoring[5]

We zullen deze lokaal testen met een aantal VM's die de infrastructuur van een klein bedrijf simuleren.

4. Verwachte resultaten

Tussen de verscheidene tools zelf kan ik nog niet genoeg onderscheidt maken om al te zeggen welke oplossing het beste resultaat gaat geven voor de verschillende criteria. Dit zal wellicht volgen uit de simulaties. De snelheid van het verwerken van de data en de duidelijkheid van de verkregen context zullen niet optimaal zijn wanneer er een grote hoeveelheid homogene data gebruikt wordt.

[2]https://www.elastic.co/kibana/
[3]https://wazuh.com/
[4]https://www.solarwinds.com/security-event-manager
[5]https://www.datadoghq.com/dg/security-monitoring/

5. Verwachte conclusies

Er wordt verwacht uit de eerdere onderzoeken dat de Elastic SIEM oplossing een veelbelovende optie is. Daarnaast zullen er zeker bepaalde tekortkomingen zijn in bijna alle tools. Wel verwachten we dat er zekere oplossingen gaan bestaan om zelfs de beste SIEM oplossing nog te verbeteren.

Referenties

Cerullo, G., Formicola, V., Iamiglio, P. & Sgaglione, L. (2014). Critical Infrastructure Protection: having SIEM technology cope with network heterogeneity. CoRR, abs/1404.7563. http://arxiv.org/abs/1404.7563

Garofalo, A., Sarno, C. D., Matteucci, I., Vallini, M. & Formicola, V. (2014). Closing the loop of SIEM analysis to Secure Critical Infrastructures. CoRR, abs/1405.2995. http://arxiv.org/abs/1405.2995

González-Granadillo, G., González-Zarzosa, S. & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 21(14). https://doi.org/10.3390/s21144759

Mavroeidis, V. & Jøsang, A. (2021). Data-Driven Threat Hunting Using Sysmon. CoRR, abs/2103.15194. https://arxiv.org/abs/2103.15194