OpenKAT voor educatie & trainingen

OpenKAT geeft inzicht in de kwetsbaarheden binnen een organisatie of omgeving. Daarnaast kan OpenKAT ook worden gebruikt voor educatie en trainingsdoeleinden. Dit document beschrijft enkele voorbeelden van trainingsdoeleinden, hoe het zou kunnen werken en wat er nodig is om OpenKAT in te zetten ter ondersteuning van educatie.

Trainingsdoeleinden

Hieronder een overzicht van een aantal voorbeelden waarvoor OpenKAT kan worden ingezet.

- Tijdens sollicitatieprocedures.
- Inwerken van nieuwe medewerkers.
- Discussie mogelijkheid hoe incidenten of bevindingen afgehandeld moeten worden.
- Incident response trainingen om bijv. een ransomware simulatie te genereren en hierbij actie- en reactiescenario's uit te werken.
- Studenten kennis laten maken met de werking van het SOC.
- Demo om (potentiele) klanten te tonen hoe OpenKAT werkt.
- Testen van nieuwe processen of protocollen.

Hoe werkt het?

Door het inladen van ruwe databestanden in de OpenKAT web-interface kunnen specifieke bevindingen, incidenten of scenario's worden ingeladen. Na het inladen kan de data worden geanalyseerd door de deelnemers en kunnen de scenario's worden uitgewerkt. De scenario's kunnen heel breed of over een specifiek onderwerp gaan. Dit is afhankelijk van het doel van de training.

Stel een deelnemer onderzoekt een alarm of bevinding, op basis hiervan moet de deelnemer de keuze maken: gaat het hier om een vals alarm, is er verder onderzoek vereist, of moet dit geescaleerd worden. Afhankelijk van de keuze kunnen er additionele databestanden aangeleverd worden die extra content aan het scenario kunnen geven. Dit kan deelnemers helpen om te leren om niet direct tot conclusies te springen, maar eerst alle feiten te verzamelen.

Andere scenario's zijn natuurlijk ook mogelijk om OpenKAT als educatie-tool in te zetten, er zijn eindeloos veel mogelijkheden.

Wat moet je zelf doen?

Bedenk een scenario en verzamel hier ruwe databestanden of andere logbestanden voor. Dit kan op basis van echte data worden gedaan (denk hierbij wel om eventuele anoniemisering vanwege privacyschendingen), of door het maken van een fictieve casus en hiervoor alerts voor te genereren.

Dit kan zo simpel zijn als het triggeren van 5x een fout wachtwoord invullen bij het inloggen, het opvragen van een bestand waar iemand geen rechten toe heeft, het scannen van het netwerk, installeren van (kwaadaardige software), of een gebruiker die heel veel bestanden opvraagd in een korte tijd. Dit kan mogelijk een eerste indicatie zijn van een ransomwareaanval.

Stappenplan

Beschrijf de training in globale lijnen. Dit helpt om een beeld te geven aan wat er geregeld en uitgewerkt moet worden en in welke mate van zelfstandigheid de deelnemers aan de slag moeten. Werk ten minste de volgende punten uit :

- **Tijdsduur** van de sessie. Hoe lang duurt de training, inclusief eventuele uitleg en uitwerken van de opdrachten.
- Wie is de **doelgroep**? Moeten de deelnemers een technische achtergrond hebben, of juist niet? Welke vaardigheden of randvoorwaarden zijn vereist om deel te nemen aan de training?
- Wat is het **leerdoel** van de training? Maak de volgende zin af: “Deelnemers leren....”. Hieronder enkele voorbeelden:
    - welke taken en activiteiten er op een SOC worden uitgevoerd.
    - welke stappen een SOC medewerker neemt om een alert te analyseren.
    - alarmen verder te onderzoeken en op een adequate manier af te handelen.
    - de eerste signalen van een ransomware aanval te herkennen.
- Welke **benodigdheden** zijn er? Denk aan laptops, internet, toegang tot een VPN of specifiek systeem, accounts, etc.
- **Beschrijving** van de training en/of het scenario. Hoe gaat de training eruit komen te zien? Lever je databestanden aan? Moeten de deelnemers hierom vragen? Wat is het scenario dat ze moeten uitwerken? Hoelang krijgen ze voor eventueel onderzoek.

In ‘Bijlage A – Template beschrijving training’ staan bovenstaande punten als invul-template met additionele vragen uitgewerkt.

Scenario’s

Enkele voorbeelden van scenario’s waaraan gedacht kan worden zijn als volgt:

- Beheerdersaccount die een encoded (base-64) powershell script draait.
- Gebruikersaccount dat zichzelf na meerdere foutieve pogingen heeft buiten gesloten.
- HR/Finance account voert macros uit in een Excel bestand.
- Medewerkersaccount voert een netwerkscan op het netwerk uit.
- Medewerker logt buiten werktijden in op het administratief systeem en voert een actie uit (betaling, opvragen van informatie, uitlezen van een database, etc).

Bijlage A – Template beschrijving training

Tijdsduur

Hoe lang duurt de training, inclusief eventuele uitleg en uitwerken van de opdrachten.

Doelgroep

Beschrijving van achtergrondkennis en het niveau van de deelnemers aan de workshop. Moeten de deelnemers een technische achtergrond hebben, of juist niet? Welke vaardigheden of randvoorwaarden zijn vereist om deel te nemen aan de training?

Leerdoel

Beschrijf wat de deelnemers van de training gaan leren. Probeer dit zo specifiek mogelijk te doen, denk hierbij aan kennis, vaardigheden en/of software. Probeer tussen de 3-5 leerdoelen op te schrijven voor de training. Bij een meerdaagse training is het handig om per dag leerdoelen op te schrijven die aan die trainingsdag gerelateerd zijn.

Hieronder enkele voorbeelden van hoe zo'n leerdoel uitwerking eruit kan zien.

Deelnemers leren....:

- *welke taken en activiteiten er op een SOC worden uitgevoerd.*
- *welke stappen een SOC medewerker neemt om een alert te analyseren.*
- *alarmen te onderzoeken en op een adequate manier af te handelen.*

Deelnemers leren...:

- *Verschillende databronnen te analyseren om een impact in te schatten.*
- *Dat data uit verschillende databronnen bij elkaar kunnen horen en te correleren naar een mogelijke aanval.*
- *de eerste signalen van een ransomware aanval te herkennen.*

Benodigdheden

Welke benodigdheden zijn vereist voor de training? Beschrijf hier ook welke aspecten geregeld moeten worden ter voorbereiding op de training. Moeten er laptops geregeld worden, of nemen de deelnemers deze zelf mee? Is er toegang tot een specifieke machine of deel van het netwerk nodig? Zijn er additioneel VPN of gebruikersaccounts die geconfigureerd moeten worden?

Vergeet hier ook niet te beschrijven welke ruwe databestanden er voor de training gebruikt worden, zodat van te voren gecontroleerd kan worden of deze nog aanwezig zijn.

Beschrijving training en/of scenario

Hoe ziet de training eruit? Krijgen de deelnemers eerst uitleg en daarna opdrachten om aan te werken? Lever je databestanden aan? Moeten de deelnemers hierom vragen? Wat is het scenario dat ze moeten uitwerken? Hoelang krijgen ze voor eventueel onderzoek of opdrachten? Creeer je nog onverwachte situaties of chaos gedurende de training om reacties te polsen? Op welke momenten doe je dit? Hoe de-escaleer je deze situaties vervolgens?