



Project plan

Jonas Willems - Monin NV

Inhoud

- Het bedrijf
- Opdracht
- Huidige situatie
- Verwachtingen
- Onderzoeken
- Planning
- Initiatiefase
- Realisatiefase
- Rapportering en communicatie



MONIN
Database Managed Services

Monin is een bedrijf gespecialiseerd in Database Managed Services. Ze richten zich op het opzetten, beheren, optimaliseren en migreren van databases voor hun klanten.



Gelegen te Edegem



±20 werknemers



Stagementor: Dries Moelans &
Kristof Vangeenderhuysen

Opdracht

- **Ethical Hacking**

- Doel: Onderzoeken van pentest tools al dan niet zelf gemaakt en procedures voor databasebeveiligingstests bij klanten.
- Het maken van handleidingen voor hackingtools ”
- Resultaat: Evaluatie of verdere beveiligingsmaatregelen vereist zijn of dat de huidige databasebeveiliging voldoet bij klanten.

Huidige situatie

- **Geen beveiligingstools**
 - Ontbreken van hacking/pentest tools en procedures voor databasebeveiligingstests.
 - Geen handleiding om te volgen om een security audit te doen.
- **Beperkt Inzicht in gevoelige gegevens**
 - Geen systematische aanpak om gevoelige gegevens in databases te identificeren voor verschillende database technologieën.
- **Geen Database Active Monitoring**
 - Ontbreken van geavanceerde database-activiteitenmonitoring.
 - Verhindert vroege detectie van verdachte toegang of activiteiten.
 - Risico van vertraagde opsporing van beveiligingsincidenten en inbreuken.

Verwachtingen

1. **Verbeterde beveiligingstools**

Implementatie van ethische hacking tools en procedures voor databasebeveiligingstests.

2. **Nauwkeurig inzicht in gevoelige gegevens**

Ontwikkelen van een systematische aanpak voor de identificatie van gevoelige gegevens in databases voor verschillende database technologieën.

3. **Effectieve monitoring**

Geavanceerde database-activiteitenmonitoring om verdachte activiteiten en toegang vroegtijdig te detecteren.

Onderzoeken

- **Ethisch Hacken**
 - Reeds bestaande pentestingtools.
 - Besturingssystemen.
 - Hackingtechnieken al dan niet database gerelateerd.
 - Algemene databasebeveiliging.
- **Opsporen Gevoelige Data**
 - Tools voor gevoelige gegevens: Identificatie.
 - Automatische gegevensdetectie: Persoonsgegevens in databases.
 - Wat is gevoelige data?
- **Database Activity Monitoring**
 - Tools voor activiteitenmonitoring.
 - Indicatoren van verdachte activiteit: Effectieve detectie.
 - Aanpassing aan databaseplatforms en Real-time waarschuwingen.

Planning



Initiatiefase

- **Bedrijfsverkenning en doelstellingen**
 - Kennismaking met het bedrijf en projectdoelen.
- **Onderzoek tools**
 - Beschikbare tools voor databasebeveiligingstests, gevoelige data discovery en database activity monitoring.
- **Opzetten omgeving**
 - Om hacking tools ethisch te testen.
 - Configuratie van testomgeving met diverse database technologieën en besturingssystemen.

Realisatiefase

- **Security Tools/Procedures**
 - Python tool en procedures ontwikkelen om databasebeveiligingstests uit te voeren.
 - Inclusief: port scanning, beveiligingsoordelen en ethische hacking.
- **Opsporen gevoelige data**
 - Beschikbare tooling onderzoeken voor gevoelige gegevensdetectie en installeren in testomgeving.
 - Bv. DataSunrise
- **Database Active Monitoring**
 - Beschikbare tooling onderzoeken voor gevoelige gegevensdetectie en installeren in testomgeving.
 - Bv. DataSunrise
- **Testen Binnenin de Testomgeving**
 - De ontwikkelde tool en procedures, evenals de database active monitoring tools, worden getest in de testomgeving.
- **Terugkommoment en evaluatie**
 - Terugkommoment 1: woensdag 11/10
 - Terugkommoment 2: woensdag 8/11
 - Tussentijdse evaluatie: voor stageweek 7
 - Eindevaluatie

Rapportering en communicatie



Wekelijks stageverslag via Outlook Mail.
Elke vrijdag of zondag een mail over wekelijkse activiteiten.



Communicatie via Slack en mail.