

# Détection et Réponse Automatisées

## Contre les Attaques de Mouvement Latéral

Utilisant CALDERA et le Framework MITRE ATT&CK

**INF 808 Laboratoire #1**

Benn1101 & Benazzouz Nedjm Eddine

# Le Problème

- Le mouvement latéral est la 3e phase de la chaîne d'attaque
- Utilise les services légitimes (WinRM, RDP, SMB) → difficile à détecter
- 9 techniques dans MITRE ATT&CK TA0008 Mouvement Latéral
- **Défi** : Détecter + réagir en < 60 secondes

# Notre Solution

## 1. Émuler

Utiliser CALDERA pour exécuter 4 techniques

## 2. Détecter

Règles SIEM corréler les signatures

## 3. Réagir

Playbooks SOAR isolent & désactivent

# Objectifs du Projet

- **Détection** :  $VP \geq 95\%$ ,  $FP < 3\%$  sur 50+ runs
- **Réponse** : Confinement automatisé en  $< 60$  secondes
- **Reproductibilité** : Déployer en  $< 30$  minutes
- **Couverture** : 4 techniques MITRE ATT&CK documentées

# Architecture du Lab

## Infrastructure

- DC01 (Windows Server)
- 3x WIN10 clients
- CALDERA (Ubuntu)
- SIEM & SOAR

## Services Clés

- Active Directory
- WinRM, SMB, RDP
- Logging Sysmon
- Agents Sandcat

# T1021.006 : Gestion Distante Windows

Que se passe-t-il ?

- Attaquant utilise des credentials valides via WinRM (5985/5986)
- Exécute des commandes PowerShell arbitraires sur hôtes distants
- Pas de session interactive requise—invisible à l'utilisateur

# WinRM : Détection & Réponse

## Signaux de Détection :

Event IDs 6/91 + PowerShell 4103/4104 + commandes (whoami, net user)

## Actions de Réponse :

Isoler la source, désactiver le compte, terminer WinRM sur la cible

# T1021.002 : Partages Administrateur SMB

Que se passe-t-il ?

- Attaquant accède aux partages C\$, ADMIN\$ via SMB (445)
- Copie des payloads malveillants vers le système distant
- Exécute via tâche planifiée, WMI ou création de service



# SMB : Détection & Réponse

## Signaux de Détection :

Event ID 5140 (accès partage) + création processus + binaires inhabituels

## Actions de Réponse :

Bloquer SMB, terminer processus, mettre en quarantaine, révoquer credentials

# T1550.002 : Pass the Hash

Que se passe-t-il ?

- Extraire les hachés NTLM du système compromis
- Utiliser le hash directement pour l'authentification (pas de mot de passe)
- Contourne la politique de mot de passe—fonctionne hors ligne

# PtH : Détection & Réponse

## Signaux de Détection :

Event ID 4624 + 4672 + signature Mimikatz + accès LSASS

## Actions de Réponse :

Réinitialiser mot de passe, forcer Kerberos, isoler source, activer MFA

# T1021.001 : Protocole Bureau à Distance

Que se passe-t-il ?

- Attaquant se connecte via RDP (port 3389) avec credentials valides
- Obtient une session interactive comme une connexion utilisateur normale
- Peut escalader les privilèges, voler des fichiers, exécuter malware

# RDP : Détection & Réponse

## Signaux de Détection :

Event ID 4624 LogonType 10 + IPs inhabituelles + connexions hors heures

## Actions de Réponse :

Bloquer RDP, terminer session, désactiver compte, activer MFA

# Pipeline de Détection & Réponse

1. CALDERA  
Émule Attaque

2. Logs → SIEM  
Sysmon, WinRM, SMB

3. Détection  
Règle Déclenchée

4. SOAR  
Confinement < 60s

# Résultats de Détection (50 runs/technique)

## WinRM

VP: 48/50 (96%)

FP: 1/20 (5%)

## SMB

VP: 47/50 (94%)

FP: 0/20 (0%)

## PtH

VP: 46/50 (92%)

FP: 1/20 (5%)

## RDP

VP: 49/50 (98%)

# Temps de Réponse Automatisée

## WinRM

Moy: 31s

Max: 52s

## SMB

Moy: 38s

Max: 58s

## PtH

Moy: 42s

Max: 65s

## RDP

Moy: 29s



# Ce Qui a Bien Marché

- **Détection WinRM** : Corrélation EventID 6/91 + PowerShell fiable (96% VP)
- **Baseline RDP** : Détecte anomalies heures/IPs (98% VP)
- **Partages SMB** : Accès admin rare en légitime → zéro FP
- **Automatisation** : Playbooks SOAR < 60 secondes

# Défis & Limitations

- **Pass the Hash** : Plus difficile (92% VP)—nécessite EDR kernel
- **Obfuscation** : Lab n'a pas testé l'obfuscation PowerShell
- **Bruit** : Réseaux réels ont plus de trafic qu'en lab
- **Abus NTLM** : Systèmes legacy force NTLM, crée du bruit

# Apprentissages Clés

- **Corrélation > Signature** : Règles multi-événements supérieures
- **Baseline Critique** : Fondamentale pour RDP & authentification
- **Automatisation Essentielle** : < 60s exige intégration API
- **Accepter l'Imperfection** : Connaître les lacunes de détection

# Livrables

## Code

170 lignes YAML

300 lignes PowerShell

400 lignes Vagrant

## Détection

4 règles SIEM (KQL)

4 techniques couvertes

95% VP global

## Tests

200 attaques exécutées

80 événements bénins

Métriques timing

# Travaux Futurs

- Intégrer EDR (Defender, Crowdstrike) pour PtH
- Ajouter détection d'anomalies basée sur ML
- Étendre à autres techniques TA0008
- Tester contre evasion : obfuscation PowerShell
- Chaos engineering : résilience SOAR validée

# Conclusion

Une chaîne de détection bien conçue peut identifier et contenir des mouvements latéraux réalistes en moins de 60 secondes.

**95% détection | < 60s réponse | Entièrement reproductible**