« Sensibilisation, remédiation & sécurisation de l'AD dans les hôpitaux - cas d'usage métier »

- Rachida Majeri : Territory Account Manager
- Mathieu Vialetay : Responsable Avant-Vente

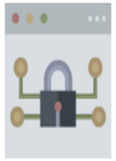
Phase 1: sensibilisation la sécurisation de l’AD dans les hôpitaux

2 principes simples trop vite oubliés

Les défenseurs doivent avoir connaissance des milliers de manières d’être compromis. Les attaquants peuvent utiliser une seule attaque, une seule fois

Les attaquants doivent connaître des milliers de façons de passer inaperçu. Les défenseurs doivent pouvoir repérer en une seule fois ce qui ne va pas

AD: Centre névralgique du SI



90 %

des organisations utilisent l'Active Directory comme mécanisme d'identification et d'authentification*

l de sécurisation
irectory ?

est un annuaire
er des informations
et aux ressources
fournissant des
ntification et
n sécurisant l'accès
re AD est **le centre**
e d'information (SI),
nt critique. Il est

50%

des entreprises ont subi des **attaques AD** au cours des 2 dernières années

CERT Santé

AGENCE DU NUMÉRIQUE EN SANTÉ

ars Agence Régionale de Santé

Comment optimiser l'efficacité de la solution ?

- Application automatique de certaines mesures de remédiation (application de correctif, verrouillage des comptes inutilisés, etc.).

Quelles autres solutions celle-ci peut-elle compléter ?

- Un EDR (Endpoint Detection and Response) qui est capable d'analyser les mouvements et actions suspectes de comptes utilisateurs potentiellement compromis.

Services associés

Accompagnement possible par un tiers pour :

- L'exploitation de l'outil (maintien en condition opérationnelle).
- La configuration de l'outil (machines à auditer, contrôles à effectuer, alertes, etc.).
- La mise en œuvre des actions de remédiation.
- Le traitement des alertes en temps réel.

Définition des Rôles:

- **Équipe d'intégration** nécessaire pour la configuration de l'outil et le démarrage de l'analyse (machines à auditer, contrôles à effectuer, configuration des alertes, etc.)

- **Équipe sécurité (interne ou externe)** pour le suivi des indicateurs d'audit et des alertes.
- **Équipe d'exploitation (interne ou externe)** pour la conception et la mise en œuvre des plans de remédiation.
- **Équipe sécurité (interne ou externe)** pour la surveillance en temps réel des menaces liées à l'AD.
- **Administrateur système** pour le maintien en condition opérationnelle de l'outil.
- **Support** disponible par l'éditeur.

Les attaquants ciblent l’identité des utilisateurs

65%
Des utilisateurs utilisent le **même mot de passe** sur différents comptes

80%
des incidents d'applications Web ont été attribués à un **vol d'identifiants**

63%
des attaques d'ingénierie sociale ont compromis des **identifiants**

50%
des entreprises ont subi des **attaques AD** au cours des 2 dernières années

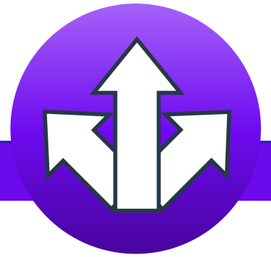
42%
des attaques AD **ont réussi**

86%
des entreprises envisagent d’augmenter la sécurité de l'identité

La bataille s’est déplacée à l’intérieur du réseau

Les attaquants partent d’un Endpoint et cherchent à se déplacer latéralement

<5 Heures pour s’infiltrer
15 heures pour exfiltrer
78 jours pour détecter



4.5 heures pour détonner
60% se déplace latéralement
64% reviendront

Avantage du temps
Élément de surprise
Accès à l'information

Détection complète

Réduction temps de détection

Intelligence exploitable

Notre pensée et notre approche doivent évoluer

Comment les attaquants exploitent les données de l’AD?

- Quel utilisateur est une cible de grande valeur ?
- Qui a l'accès souhaité ?
- Quels serveurs hébergent les données critiques ?
- Quels serveurs exécutent un service spécifique vulnérable à un exploit ?

Découverte

- Quel est le chemin le plus court vers un système avec accès surélevé ?
- Quelles sont les relations d'approbation entre les forêts ?
- Qui sont les membres des groupes de domaines étrangers ?
- Où se trouvent ces informations d'identification ?
- Quel est le chemin vers ces terminaux ?

Déplacement

- Quelles erreurs de configuration existent dans l'environnement ?
- Quels sont les mécanismes de persistance disponibles pour éviter les notifications ?
- Quelle mauvaise configuration peut aider à élever les privilèges ?
- Qui est sur-privilégié ?
- Quel utilisateur dispose d'un accès administrateur local ?

Compromission

SentinelOne™

Phase 2: Face à ce constat, quelles solutions?

Pourquoi Sécuriser votre AD?

- Solutions permettant de réaliser un **audit en continu** de son annuaire, de détecter les attaques et de **limiter le risque de compromission totale de son SI**.
- L'annuaire AD étant l'un des éléments **les plus critiques d'un SI**, la valeur ajoutée d'une solution de ce type est importante.
- **Intégration facile et rapide** de la solution à côté de l'AD.
- Solution adaptée pour une organisation de **maturité basique**.

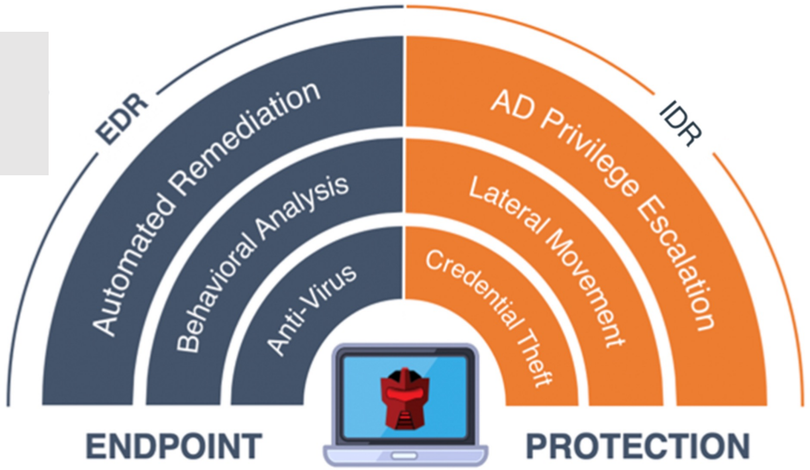
Menaces couvertes

Compromission du SI (vulnérabilité dans l'architecture, mauvaise configuration)

Les cybermenaces organisationnelles nécessitent une convergence

Centrée sur le Endpoint

Protéger, détecter et répondre



Centrée sur l'Identité

Protéger, détecter et répondre

CONVERGENCE DES CONTRÔLES DE SÉCURITÉ DES ENDPOINTS ET DES IDENTITÉS

CONTRÔLES DE SÉCURITÉ ORGANISATIONNELS

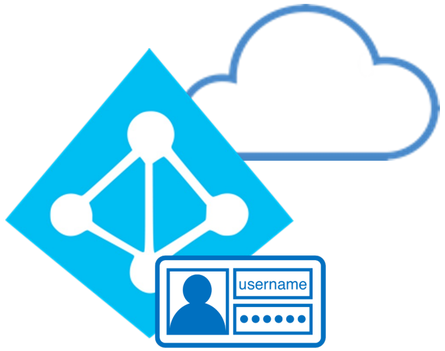
Pouquoi Gérer/Provisionner ne veut pas dire Sécuriser

1 Protection Endpoint

Endpoint

Prévenir l'utilisation abusive identifiants et mouvements latéraux

2 Sécurité identité



Sécurité identité

Sensibilisation permanente et détection des attaques

3 Protection des accès

Gestion des accès

Garantir les moindres privilèges et droits

Lacunes en matière de détection + complexité opérationnelle


NATIVE DATA
EPP / EDR
XDR
Cloud
Identity
IR & MDR
Singularity Platform
Security DataLake
Powered by DataSet
INGEST DATA FROM ANY SOURCE
IDENTITY
EMAIL
CASB
SASE
WEB
THREAT INTEL
SANDBOX
FIREWALL
CASE MGMT
LOG INGEST
3RD PARTY DATA INGEST
Singularity Marketplace
LOG DATA INGEST

Identity Protection

IAM, PAM, IGA + ID Attack Surface Management & Identity Threat Detection & Response (ITDR)

Access Management

Identity Attack Surface Management

Identity Detection & Response (ITDR)

Provisioning Identities

IGA

- Identity Life Cycle Management
- Access Requests
- Entitlement Provisioning

Connecting Identities

IAM

- Authentication
- Authorization
- SSO
- MFA

Controlling Identities

PAM

- Control privileged Identities
- Just in Time Access
- Least Privilege Access

Securing Identities

ID ASM

- AD Database Vulnerabilities
- Attack Paths
- Credential Exposures
- Least Privileges

ITDR

- AD Domain Enumeration/Exploitation
- Identity Privilege Escalation
- Credential Protection
- Cloud Entitlement

Singularity™ Identity

Active Directory renforcé

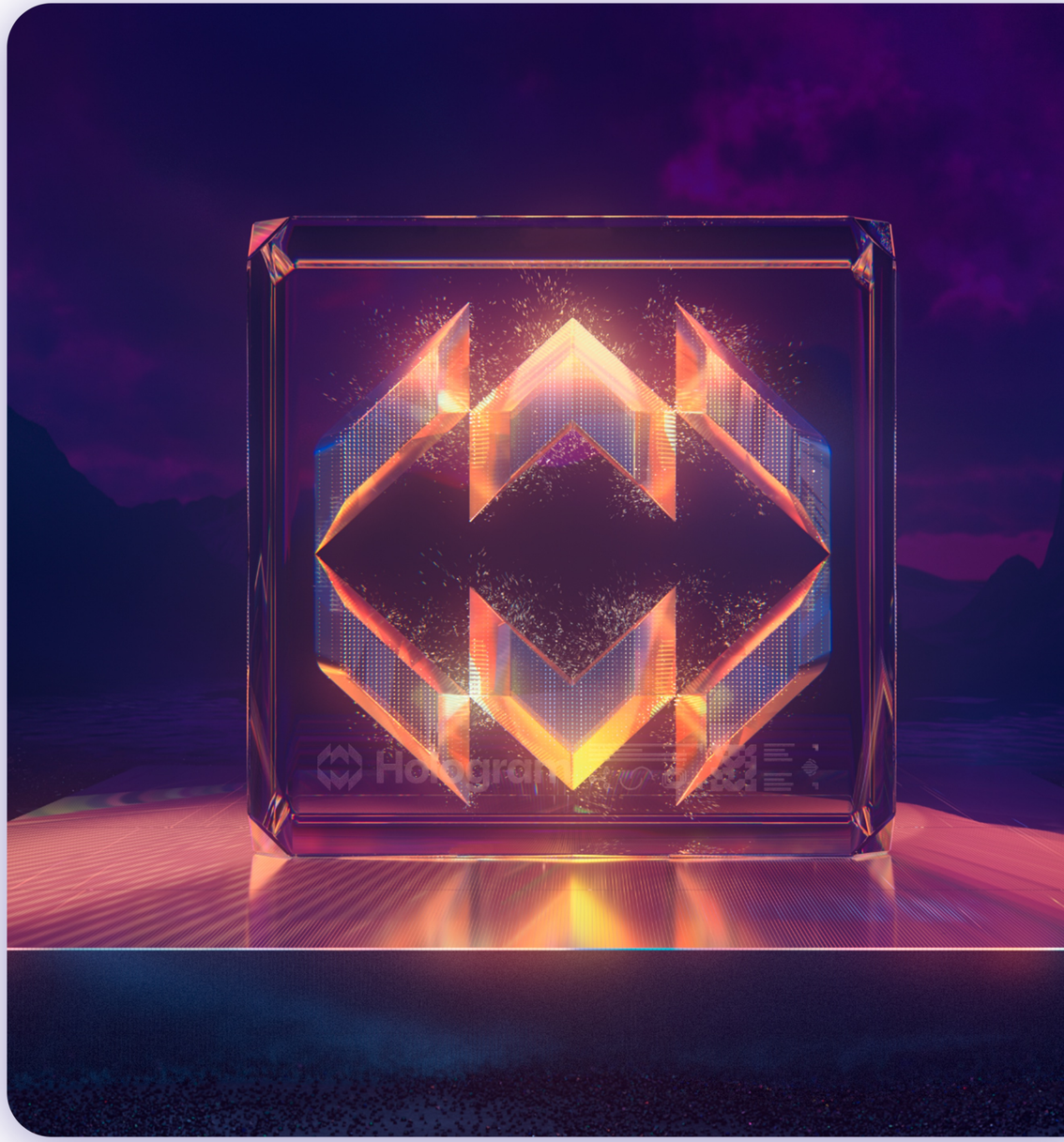
Protégez vos magasins d'identité, identifiez et corrigez les expositions à risque et les vulnérabilités

ITDR | Identity Threat Detection & Response

Prévenir les attaques liées à l'identité, la collecte d'informations d'identification, la reconnaissance et les mouvements latéraux

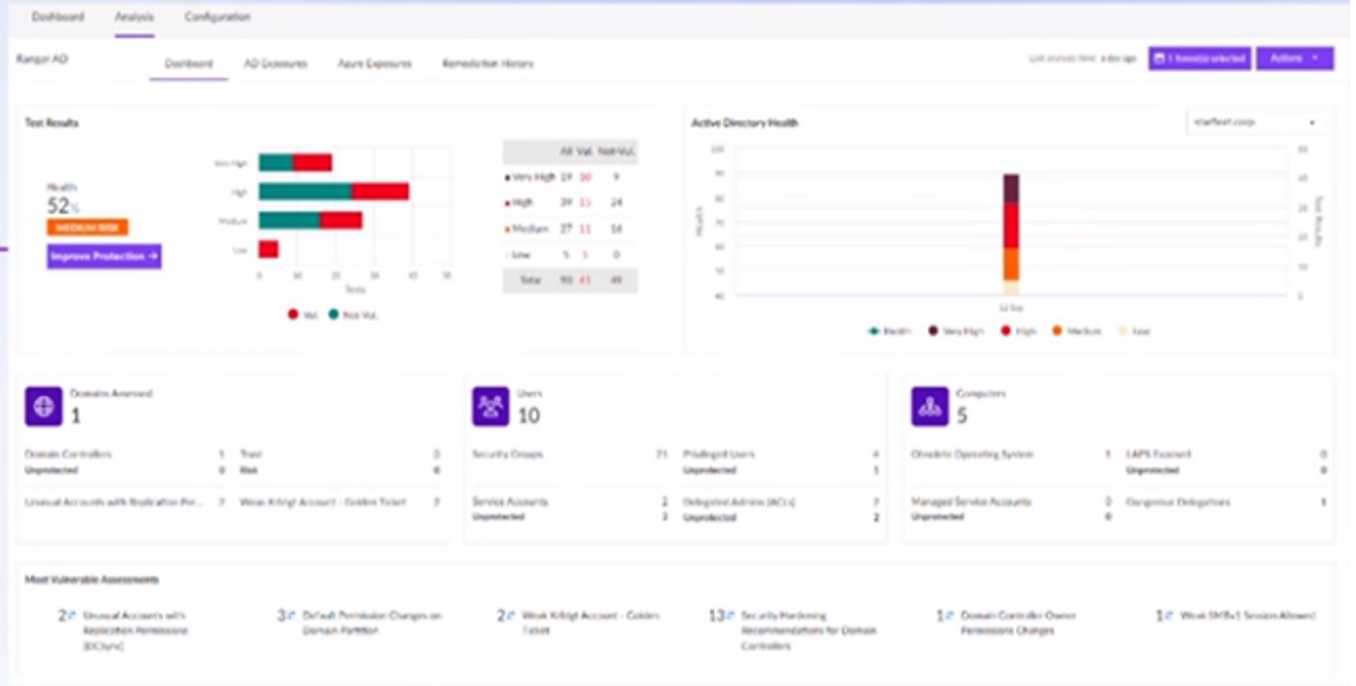
Déjouer les adversaires

Les leurres engagent les attaquants s’ils veulent obtenir des informations



Analyse de l'Active Directory

SentinelOne réduit la surface d'attaque d'Active Directory en identifiant les erreurs de configuration et les vulnérabilités de l'infrastructure d'identité dans Active Directory On prem et Azure AD.



Résultats

- Surveiller en permanence Active Directory et Azure AD pour détecter les mauvaises configurations et les vecteurs exploitables.
- Obtenir des informations exploitables pour corriger les expositions
- Rester informé des événements suspects de changement d'AD et des droits surprovisionnés

Conformité

Un seul service à gérer

Expositions au niveau du domaine

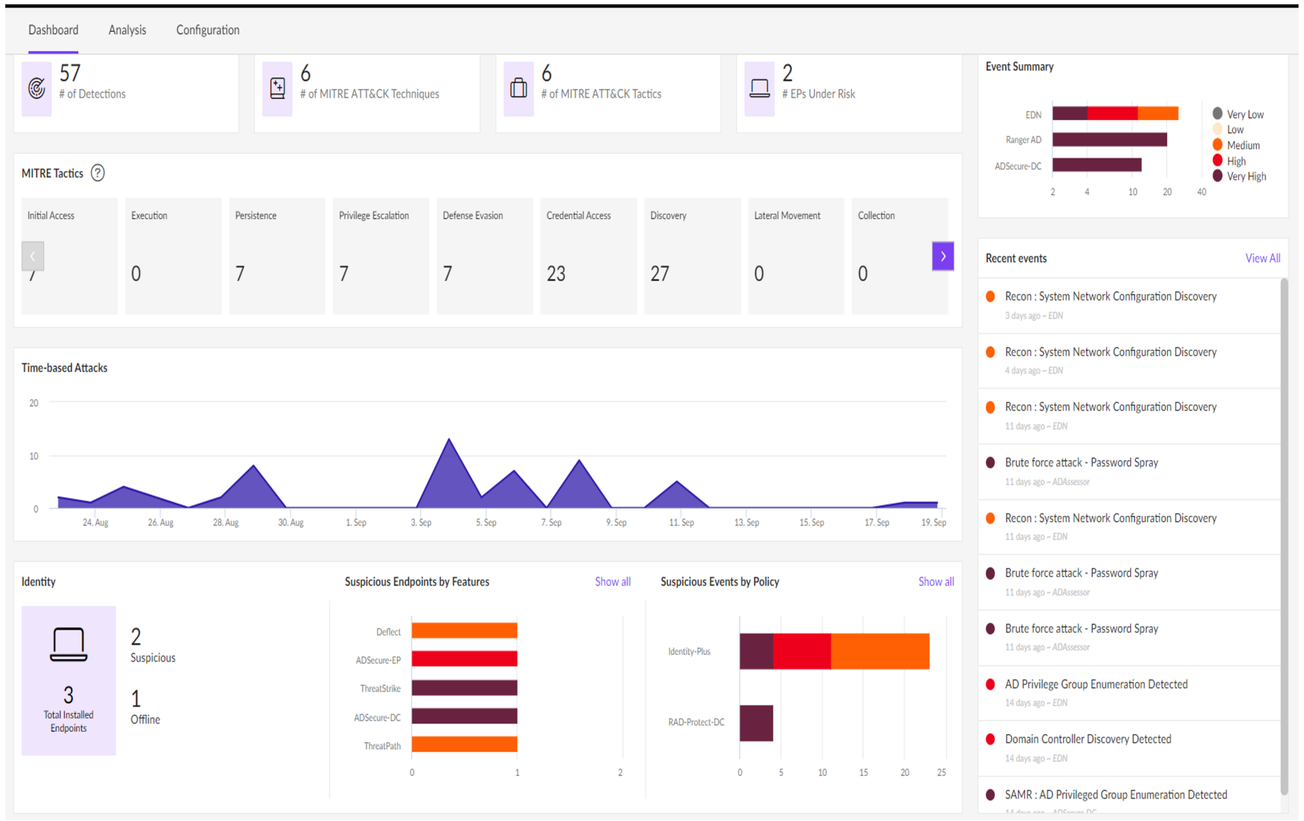
Expositions au niveau des appareils

Expositions au niveau de l'utilisateur

Activité Suspecte

Protection de l’Active Directory

SentinelOne enables détecte et protège en temps réel les attaques contre l’Active Directory avec l’ITDR comme la reconnaissance d’AD, DCSync, Golden Ticket etc



Résultats

- Prévenir les mauvaises utilisations au niveau AD
- Rendre les mouvements latéraux difficiles
- Se protéger contre tout types de devices même IoT
- S’associe à l’analyse des configurations pour une couverture plus approfondie de la sécurité de l'infrastructure AD

Détection contre tous les devices

Déploiement On-Prem et Azure AD

Technique de déception pour leurrer les attaquants

Réduction de la surface d’attaque

Zero Trust

Recommandation & sécurisation de votre infrastructure d’Identité

Etape initiale

Optimisation

Réduire la surface d’attaque

Protection de l’ infrastructure d’Identité

Détection d’attaques réseau et atténuation des menaces internes

Convergence et mutualisation avec la plateforme XDR

Singularity Identity - solutions

Commencez ici

Aller au-delà

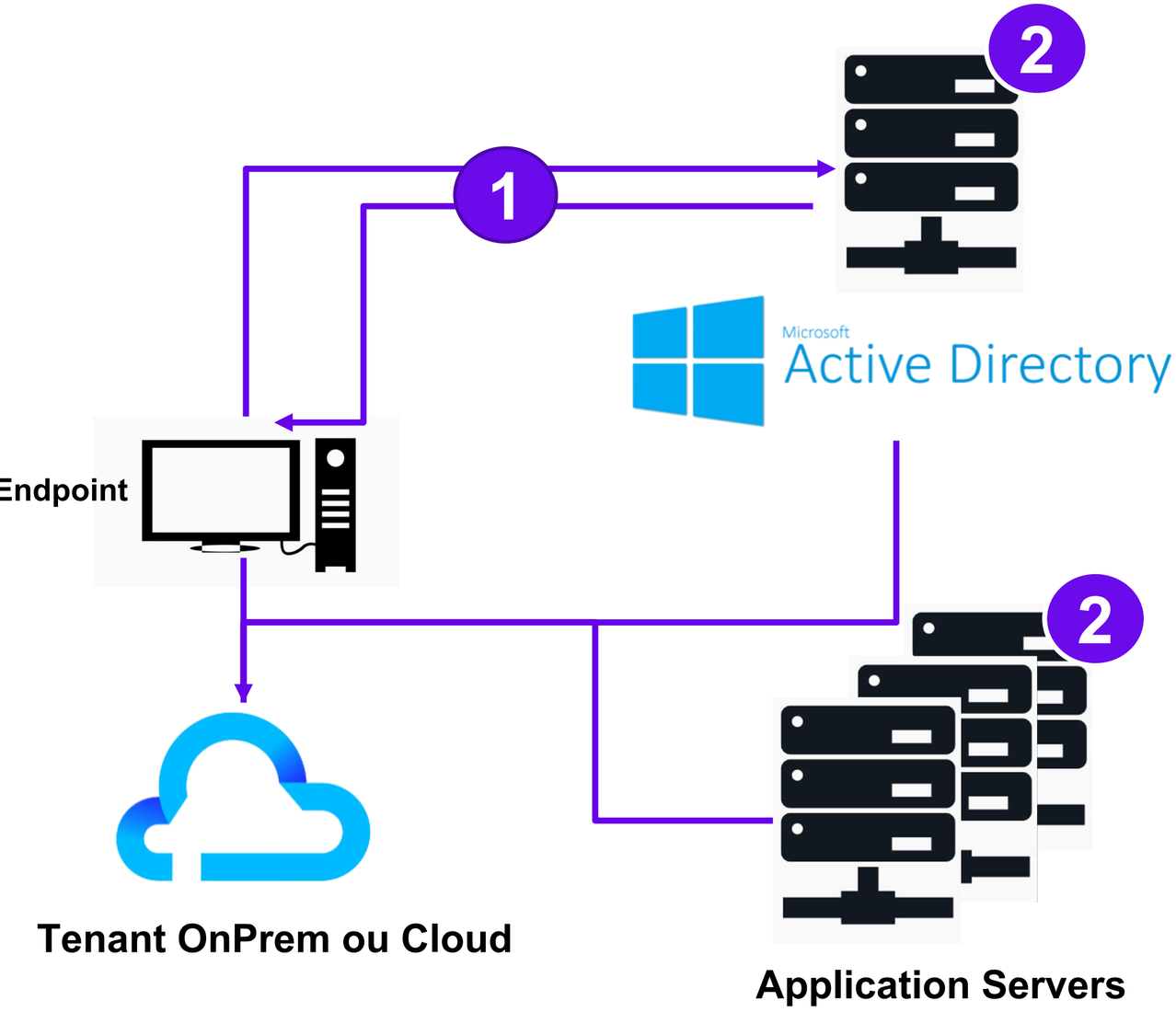
Singularity RangerAD

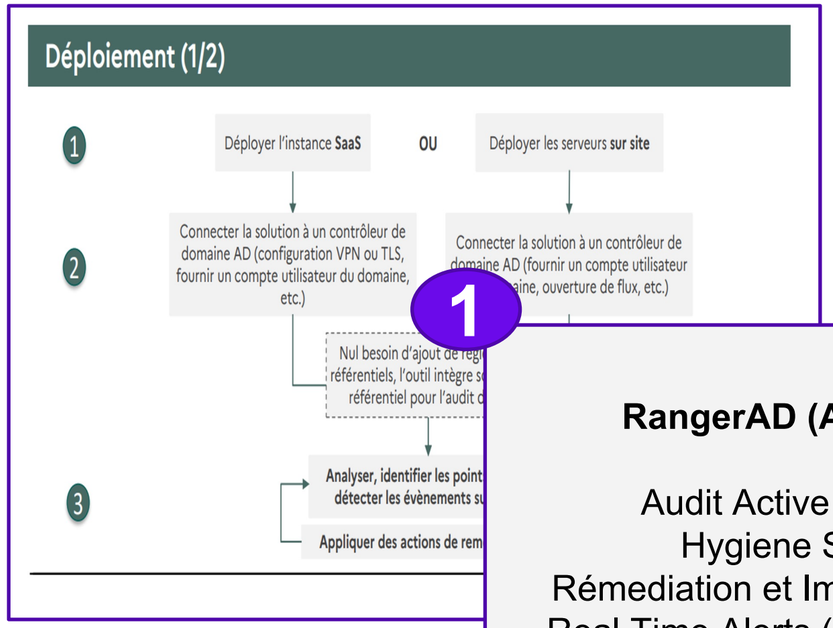
Singularity Identity

Singularity Hologram

Singularity Platform

Modèles Architectures





1

RangerAD (Agentless)

Audit Active Directory
Hygiene Scoring
Rémediation et Impact Guidance
Real Time Alerts (10 event types)

2

Identity – DC (Agent Based)

Advanced Real Time AD Attack Detection

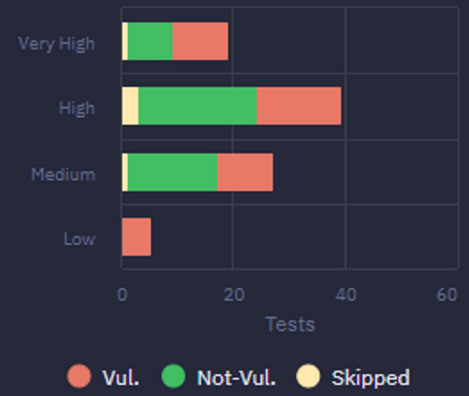
Detect AD Scans and Reconnaissance
Golden Ticket
Silver Ticket
Skeleton Key
Pass the Hash
REP Roasting
Overpass the Hash
+ many more

sor

Dashboard | AD Exposures | Azure Exposures

Last analysis time: 4 days ago | PRODUCTION... | Actions

sults



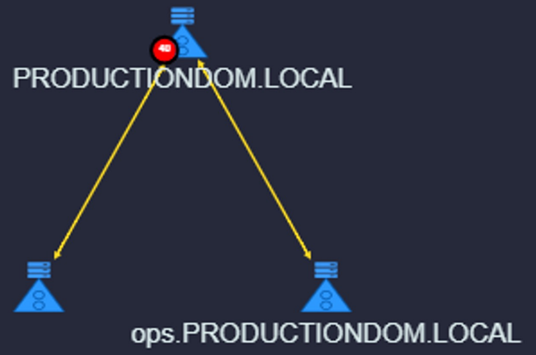
UM RISK

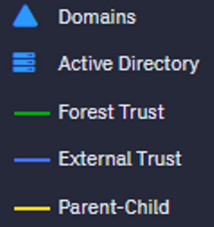
ve Protection →

	All	Vul.	Not-Vul.	Skipped
Very High	19	10	8	1
High	39	15	21	3
Medium	27	10	16	1
Low	5	5	0	-
Total	90	40	45	5

Domain View

Topology View





Domains Assessed
1

Controllers	4	Trust	3
ted	0	Risk	3
Accounts with Repli...	12	Unprivileged Users in AdminS...	1

Users
262

Security Groups	52	Privileged Users	51
		Unprotected	0
Service Accounts	3	Delegated Admins (ACLs)	12
Unprotected	0	Unprotected	9

Computers
162

Obsolete Operating System	23	LAPS Exposed	0
		Unprotected	0
Managed Service Accounts	2	Dangerous Delegations	1
Unprotected	0		

lnerable Assessments

2 Unusual Accounts with Replication Permissions (DCSync)

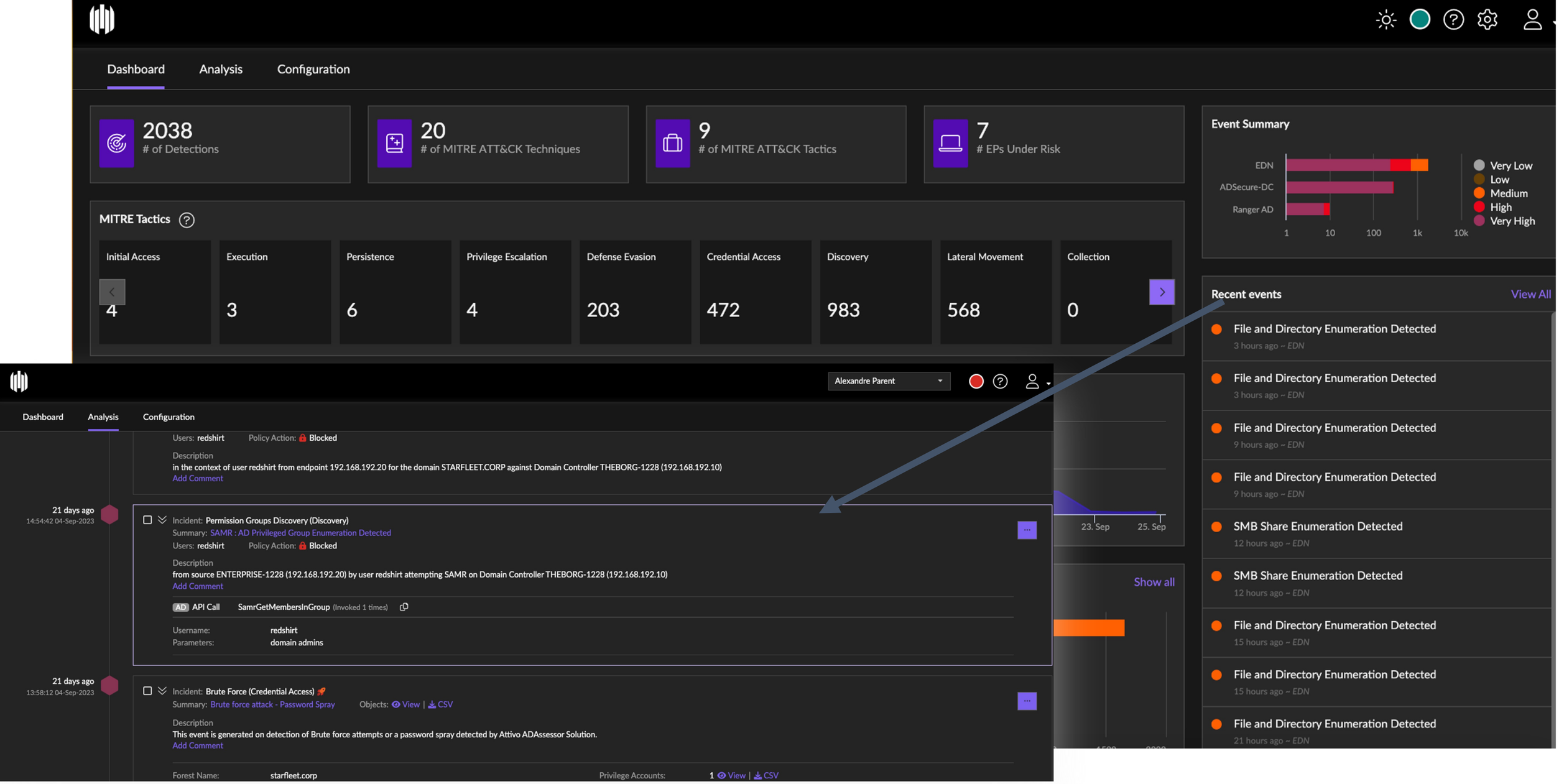
1 Unprivileged Users in AdminSDHolder ACL

8 Default permissions changes on Domain Partition

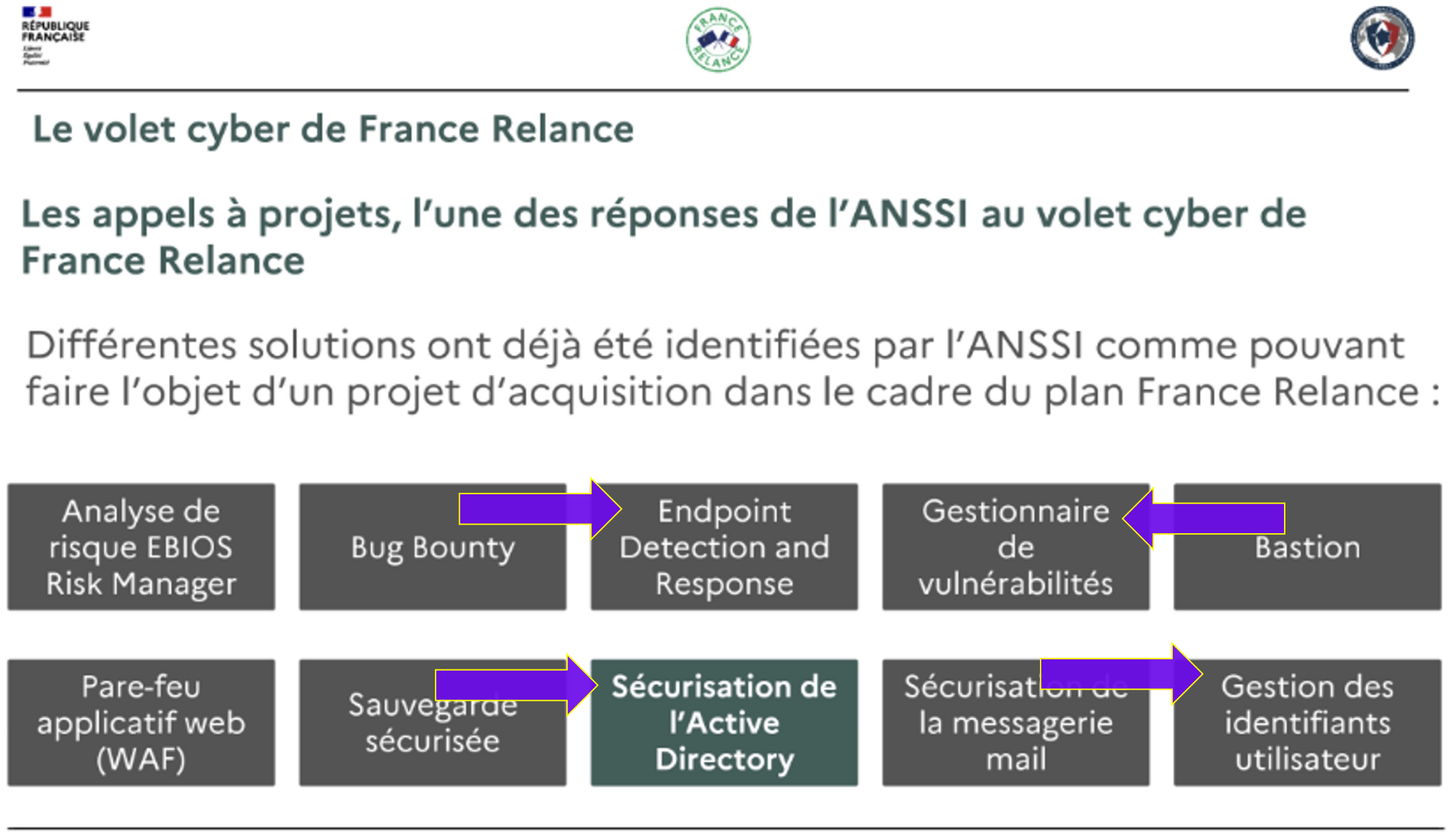
1 Weak KRBTGT Account - Golden Ticket

17 Security Hardening Recommendations for Domain Controllers

1 Zerologon vulnerable Domain Controllers


Dashboard
Analysis
Configuration
2038
# of Detections
20
# of MITRE ATT&CK Techniques
9
# of MITRE ATT&CK Tactics
7
EPs Under Risk
MITRE Tactics
Initial Access
4
Execution
3
Persistence
6
Privilege Escalation
4
Defense Evasion
203
Credential Access
472
Discovery
983
Lateral Movement
568
Collection
0
Event Summary
EDN
ADSecure-DC
Ranger AD
1
10
100
1k
10k
Very Low
Low
Medium
High
Very High
Recent events
View All
File and Directory Enumeration Detected
3 hours ago ~ EDN
File and Directory Enumeration Detected
3 hours ago ~ EDN
File and Directory Enumeration Detected
9 hours ago ~ EDN
File and Directory Enumeration Detected
9 hours ago ~ EDN
SMB Share Enumeration Detected
12 hours ago ~ EDN
SMB Share Enumeration Detected
12 hours ago ~ EDN
File and Directory Enumeration Detected
15 hours ago ~ EDN
File and Directory Enumeration Detected
15 hours ago ~ EDN
File and Directory Enumeration Detected
21 hours ago ~ EDN
Alexandre Parent
Dashboard
Analysis
Configuration
Users: redshirt
Policy Action: Blocked
Description
in the context of user redshirt from endpoint 192.168.192.20 for the domain STARFLEET.CORP against Domain Controller THEBORG-1228 (192.168.192.10)
Add Comment
21 days ago
14:54:42 04-Sep-2023
Incident: Permission Groups Discovery (Discovery)
Summary: SAMR : AD Privileged Group Enumeration Detected
Users: redshirt
Policy Action: Blocked
Description
from source ENTERPRISE-1228 (192.168.192.20) by user redshirt attempting SAMR on Domain Controller THEBORG-1228 (192.168.192.10)
Add Comment
AD API Call
SamrGetMembersInGroup (Invoked 1 times)
Username: redshirt
Parameters: domain admins
23. Sep
25. Sep
Show all
21 days ago
13:58:12 04-Sep-2023
Incident: Brute Force (Credential Access)
Summary: Brute force attack - Password Spray
Objects: View | CSV
Description
This event is generated on detection of Brute force attempts or a password spray detected by Attivo ADAssessor Solution.
Add Comment
Forest Name: starfleet.corp
Privilege Accounts: 1 View | CSV

SentinelOne et les projets Cyber de France Relance…



https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-securisation_ad.pdf