Documentation de l’Architecture Supervisée, des Sources et des Types de Données

Client : DUNDER MIFFLIN, INC

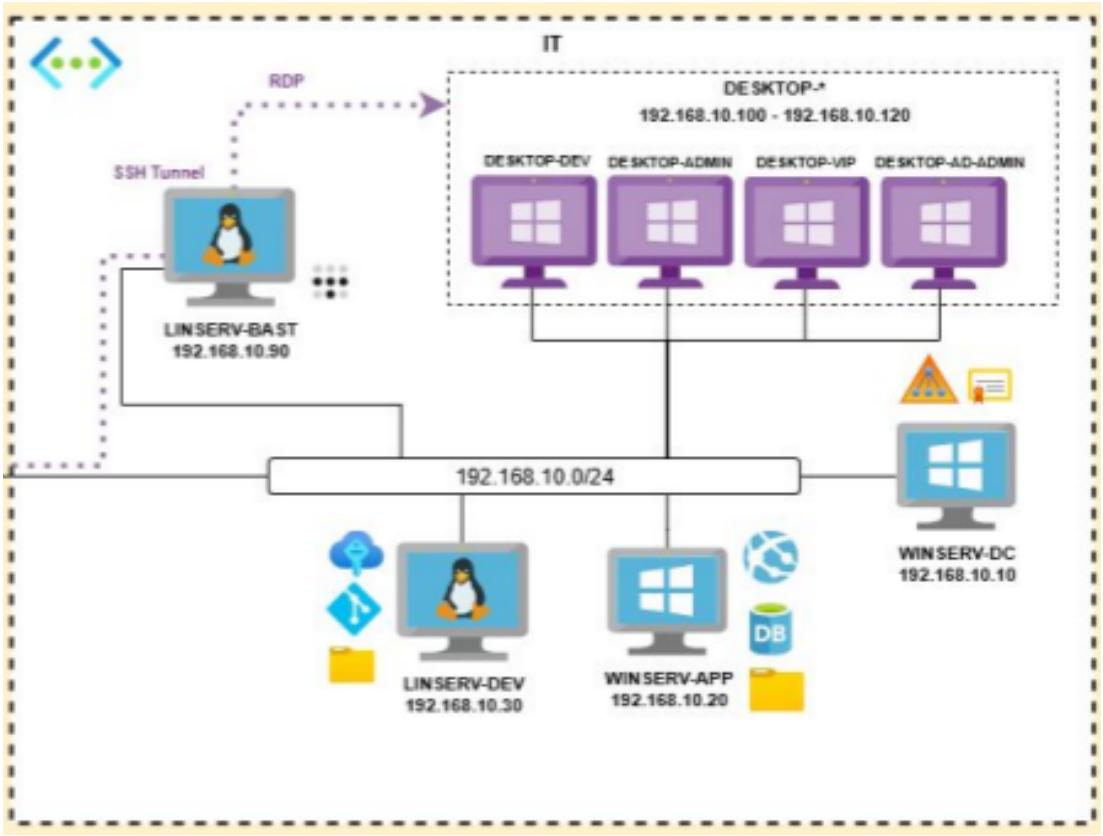
Mini-SOC : AEGIS CyberProtect

1. Contexte général

Le Mini-SOC AEGIS CyberProtect supervise l’infrastructure de Dunder Mifflin dans le cadre d’un service de détection et réponse orienté TPE/PME. L’objectif est de fournir une supervision efficace à faible coût, à l’aide d’un SIEM (Splunk), d’un IDS réseau (Suricata), et d’agents unifiés (Sysmon, Kunai).

2. Architecture supervisée

L'environnement IT supervisé repose sur un réseau interne non exposé. L'accès distant se fait via Tailscale vers un bastion Linux. Les systèmes supervisés incluent :
• Bastion Linux (LIN-SERV-BAST)
• Postes Admin / VIP / DevOps
• Contrôleur de domaine WIN-SERV-DC
• Serveur applicatif WIN-SERV-APP
• Serveur de développement LIN-SERV-DEV



3. Sources de données ingérées

a. Windows (Postes & Serveurs)

Sources collectées :
• Sysmon (Sysmon Modular)
• Windows Security (4624, 4625, 4768, 4769, 4771…)
• Windows System (7045, 1102…)
• PowerShell logs
• DNS Client logs *Types d'événements :*
– Process creation (Sysmon 1)
– Network connections (Sysmon 3)
– LSASS access (Sysmon 10)
– Registry modifications (Sysmon 12–13)
– Service installation (7045)
– Auditpol changes (4719)
– Event logs cleared (1102)

b. Active Directory

• Directory Service Changes / Replication • Security Group Management • Kerberos Authentication / Ticketing • Account Lockout / Logon / Special Logon

c. Linux

Collecte via journald, rsyslog et Kunai :
• auth.log
• sudo logs
• exécutions shell
• accès fichiers sensibles
• informations système et réseau

d. Réseau

Suricata EVE JSON :
• DNS (requêtes, réponses)
• HTTP
• TLS
• Alertes IDS (signatures)

Firewall :
• Flux entrants/sortants
• Détection de scans réseau

4. Types de données supervisées (alignées sur les règles Sigma)

a. Identité / AD / Privilege Escalation

Détections associées :
• DCSync
• Shadow Credentials
• AS-REP Roasting
• Kerberoasting
• Délégation Kerberos suspecte
• Dump NTDIS.dit
• Ajout à un groupe critique
• Modification auditpol
• Effacement de logs
Données nécessaires : AD Security logs, Sysmon, DS Replication.

b. Credential Access

• LSASS dump (via outils natifs ou Python)
• Lecture de fichiers sensibles
• Password loot dans fichiers
• Enumérations d'historique
Données : Sysmon 1/10, Security 4624–4625, audit Linux.

c. Execution / Persistence / Lateral Movement

• schtasks suspects
• Création de services suspects
• Run Key / Reg Add
• Utilisation de LOLBIN
• Processus système anormaux
• Commandes d'énumération Linux
Données : Sysmon 1/12/13, journald.

d. Network / Exfiltration

• DNS tunneling (TXT execution, Base64)
• TOR usage (Linux & Windows)
• Beaconing C2
Données : Suricata DNS/TLS/HTTP, Sysmon 3.

Conclusion

Cette documentation synthétise l'architecture supervisée, les sources de données collectées et les types d'événements nécessaires pour alimenter les règles Sigma déployées dans le cadre du service SOC fourni à Dunder Mifflin par AEGIS CyberProtect.