METSYS

Threat Management – Modern SIEM & xDR

xDR & SIEM - Un device sécurisé pour toutes les tailles d'entreprise

- Les domaines : xDR, SIEM/Sentinel, Cybersécurité / Zero Trust, Home Office, Modern Management, SMC, ...

Renforcer la sécurité des devices « à la base », avec Microsoft Defender for Endpoint et Intune

Accompagner les DSI dans la transformation et la sécurisation du Modern Device avec une approche de services managés Cyber / SOC

Home Office

Modern Device (Windows 10/11, iOS, Android)

Cybermenaces (ransomware, Active Directory, ...)

Environnement Modern Device sécurisé

Threat Protection

Démarche Zero Trust

Approche SOC / microSOC

- Etude et mise en œuvre d'un environnement de sécurité renforcée Microsoft Defender for EndPoint
- Réflexion sur les scenarii de sécurisation des devices – xDR / Unified EndPoint Management / Hardening Windows 10
- Intégration du xDR MDE dans un SIEM (Sentinel) & UEM (Intune)
- Accompagnement sur la mise en œuvre d'une démarche globale Zero Trust
- Gestion des vulnérabilités
- Approche SOC / MicroSOC
- Cyber résilience en cas d'attaques – Résistance aux menaces

Modern SIEM & xDR – Un accompagnement de bout en bout

Use Cases

Savoir d'où l'on part en terme de maturité	Définir une cible et identifier la trajectoire de transformation	Sécuriser le EndPoint avec le xDR	Sécuriser le EndPoint avec le xDR & Intune	Sécuriser le EndPoint avec le MicroSOC xDR	Focus SMC : xDR & SIEM « all inclusive »
Y	Y	Y	Y	Y	Y
Zero Trust Maturity Evaluation	Journey to Modern SIEM & xDR	Microsoft Defender for EndPoint Starter Kit	Microsoft Defender for EndPoint Premium Kit	Microsoft Defender for EndPoint MicroSOC	SMC EndPoint Threat Protection « from zero to hero »
Tous segments					SMC

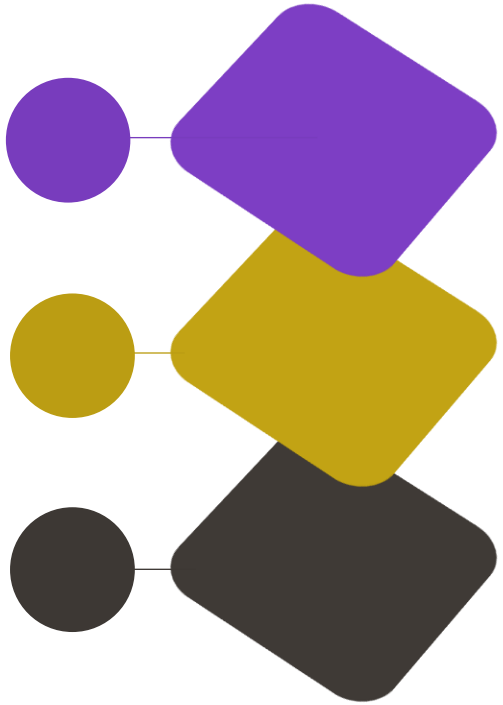
Modern SIEM & xDR – Technologies mises en œuvre

Périmètre des solutions Microsoft

Treat Protection
- Microsoft Defender for EndPoint
- Microsoft Windows Enterprise E3/E5 (credential / Application / device / exploit guard, ...)
- EndPoint Detection & Response
- Attack Surface Reduction
- Microsoft Threat Experts

Zero Trust
- Device Security Enforcement
- Unified EndPoint Management
- Threat & vulnerability Management

SIEM & SOC
- Microsoft Sentinel (solution opérée par SOC Metsys)
- Azure Logs Analytics



Journey to Secure Device

METSYS Microsoft

Microsoft 365 E3/E5
Windows 10
Microsoft Security
Intune
Office 365
Azure Active Directory

1 **Windows Hardening & hybrid join**
- Etude de hardening Windows 10 Enterprise : Exploit / credential / application Guard, Windows Hello for business, Windows Firewall, ...
- Mise en oeuvre Azure AD hybrid join

2 **Windows Compliance**
- Mise en œuvre co-management si SCCM/MEMCM
- Intégration modèle de conformité dans Intune (bascule GPO AD le cas échéant)
- Mise en œuvre patch Management - Windows Update for Business + Delivery Optimization dans Intune
- Mise en œuvre du servicing Windows 10/11 dans Intune
- Règles d'accès conditionnel pour Windows

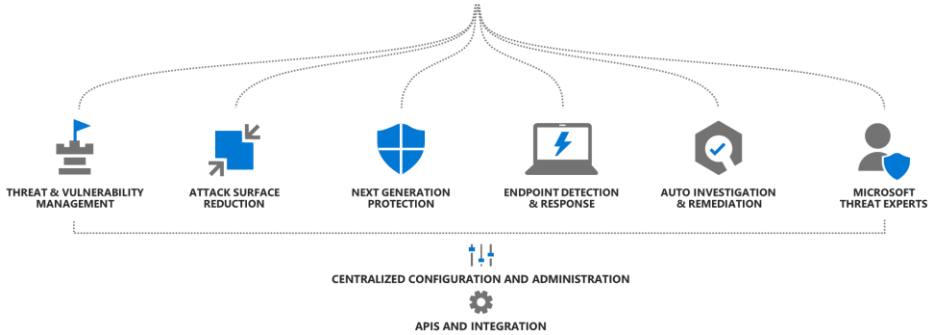
3 **Windows Threat Protection**
- Etude et mise en œuvre des fonctionnalités EDR avec Microsoft Defender for EndPoint
- Intégration SIEM / SOC / MicroSOC

4 **Extend to Device**
- Gestion des devices iOS, Android (profils BYOD ou entreprise / « fully managed ») avec Intune : stratégies de conformité, profils de configuration, ...
- Déploiement Intune sur MacOS, Linux ?
- Déploiement Defender sur les devices
- Régles d'accès conditionnel pour les devices

Continuous Improvment / Delivery

Secure Device Super Hero

Microsoft Defender for Endpoint
Built-in. Cloud-powered.



Notre ambition : un device sécurisé pour nos clients

Résistance aux menaces de type ransomware, solution de xDR avec Microsoft Defender for EndPoint pour les devices iOS/Android/Windows 10/11/Windows Server, Modern Management avec Intune, services managés Cyber de type MicroSOC avec le SIEM Microsoft Sentinel

METSYS

@metsysgroup

/company/metsys/

/metsysgroup/

metsysgroup

/company/metsys/