Sentinel Starter Kit

Assurez une analyse de sécurité intelligente sous Microsoft Sentinel

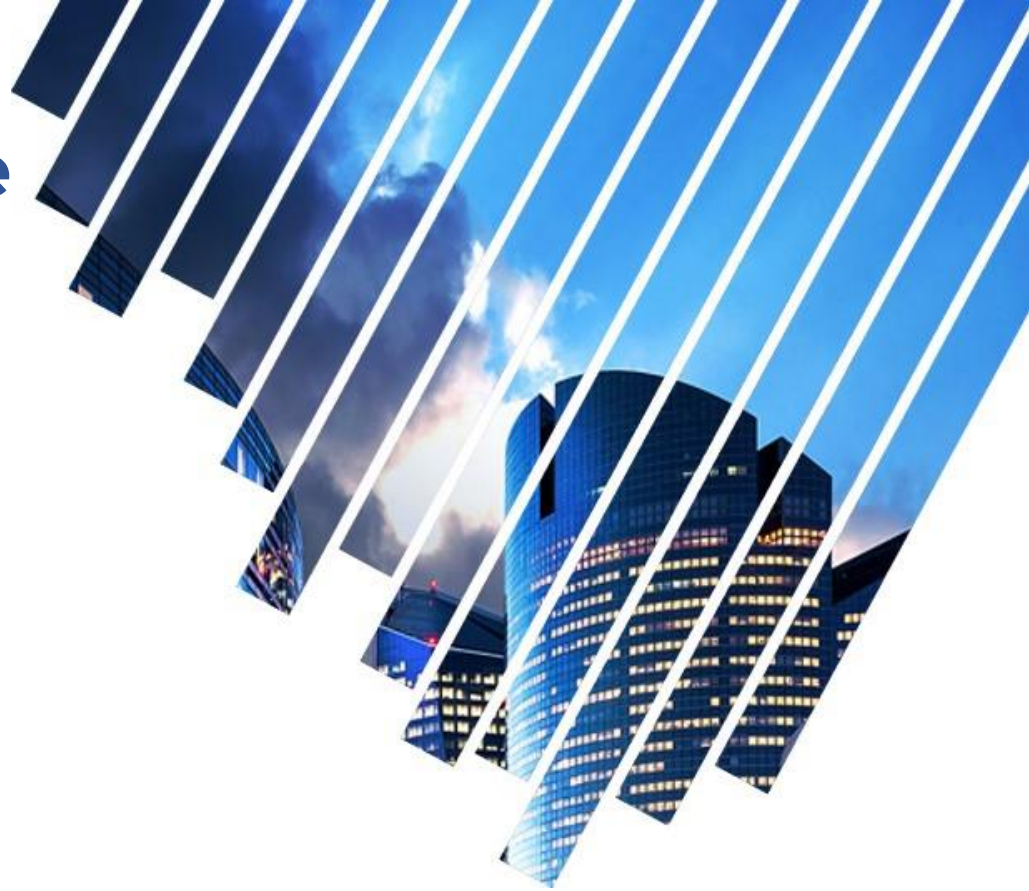
14/02/2022 V1.0

I-TRACING
CYBERSECURITY EXPERT

Microsoft Partner
Microsoft

Gold Security
Silver Cloud Platform
Silver DevOps
Silver Data Platform
Silver Windows and Devices

Premiers pas avec Azure Sentinel pour une surveillance cyber complète et performante



I-TRACING, pure player de la cyber sécurité depuis 2005
Un modèle intégré de bout en bout, un accompagnement global & engageant depuis le conseil technique et l'ingénierie jusqu'au services managés.

Azure Sentinel Starter Kit

L'accompagnement d'un expert du SIEM et du CyberSOC pour votre déploiement d'Azure Sentinel.

Que doit-on surveiller prioritairement ?
Quels sont nos principaux risques ? Quels événements redoutés dois on impérativement couvrir ? Quelques exemples de questions auxquels les experts I-TRACING vous aideront à répondre.

Quelle architecture de collecte doit-on déployer ? Comment collecter des sources non Microsoft ? Quelle rétention ?
Les experts I-TRACING vous aideront à y voir clair.

Que politique de détection ? Peut-on automatiser certaines activités ?
Comment limiter les faux positifs ? Que faire en cas d'alerte ?
Les experts I-TRACING sont là pour optimiser votre plate-forme, proposer une surveillance proactive et vous accompagner dans le traitement des incidents de sécurité.

I-TRACING
CYBERSECURITY EXPERT

Microsoft Partner
Microsoft
Gold Security
Silver Cloud Platform
Silver DevOps
Silver Data Platform
Silver Windows and Devices

Azure Sentinel Starter Kit

Vos enjeux

Surveillance de vos environnements sensibles, infrastructure & métiers

Surveillance active en lien avec vos scénarios de risque redoutés

Capacité de réaction face aux incidents & crises cyber

Notre réponse

Conseil sur la stratégie de surveillance

Mise en œuvre de la surveillance sur un périmètre initial

Accompagnement à l'extension du périmètre de surveillance (OPTION)

Surveillance active CYBERSOC & réponse à incidents

Mise en œuvre de Sentinel

Définition de l'architecture de collecte

Définition de la politique de surveillance

Activation & configuration initiale de l'instance Azure Sentinel

Déploiement de l'architecture de collecte et mise en œuvre des collectes pour 3 sources

Mise en place de playbook XSOAR (4)

Cyber SOC (en option)

Analyse des alertes / déviations / détections (patterns)

Investigation des root causes et initialisation de la réponse à incident

Customisation des politiques / règles à partir des patterns SOC ITR

Surveillance proactive de menaces (Threat hunting), Recherche d'IOC système

Réponse à incidents / Forensics

I-TRACING
CYBERSECURITY EXPERT