OFFRE COMMERCIALE C2S BOUYGUES

SUPERVISEZ ET GEREZ VOS ALERTES SECURITE AVEC MICROSOFT AZURE SENTINEL

C2S BOUYGUES
construisons votre avenir digital

AGENDA

- C2S Bouygues
- Offre
- Améliorez votre cyber sécurité !
- Success Stories

C2S BOUYGUES

C2S BOUYGUES

construire votre avenir digital

Depuis plus de 20 ans, C2S Bouygues, filliale à 100% de Bouygues SA, accompagne ses clients avec succès dans leurs projets de transformation digitale

NOUS METTONS LE DIGITAL AU SERVICE DU PROGRÈS HUMAIN

32 M€	**+250**	**4**	**1**
CA 2019	Collaborateurs	Localisations	Innovation Spot

Nos 6 domaines d’expertise

DIGITAL TRANSFORMATION

CYBERSECURITY

SMART BUILDING,
SMART CITY & IOT

SOFTWARE & AI

INFRASTRUCTURE,
CLOUD & NETWORK

OPERATIONS &
MANAGED SERVICES

C2S Bouygues, Microsoft Gold Partner

Microsoft Partner

Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Collaboration and Content
Gold Application Development

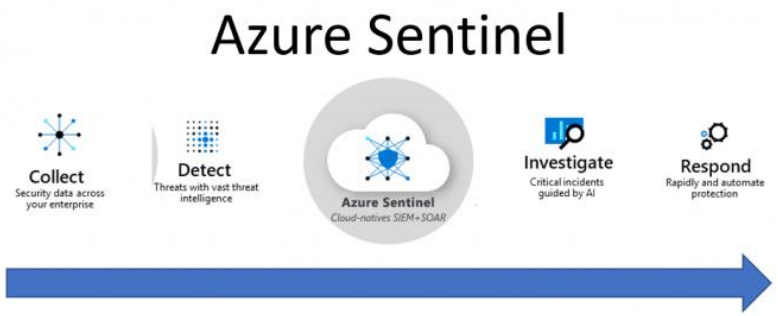
Microsoft Azure

Windows

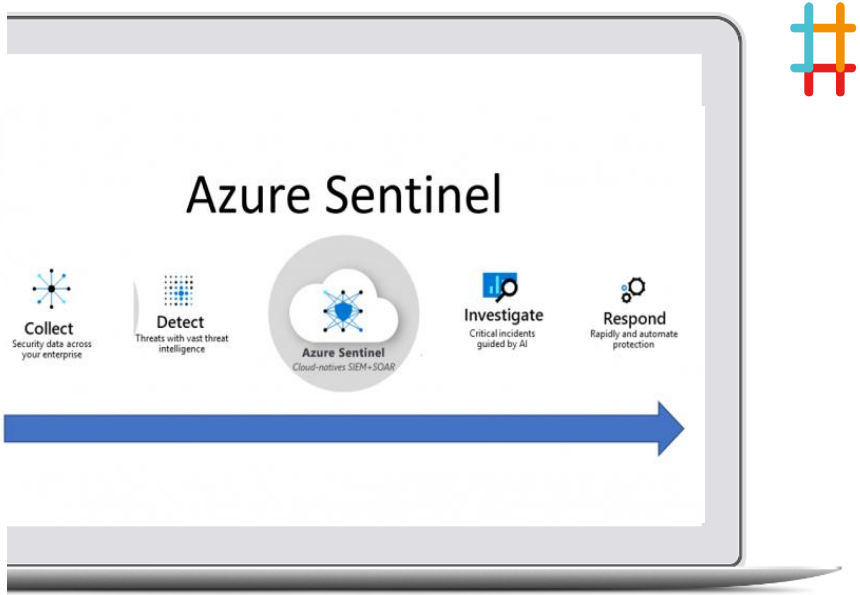
Office 365

- C2S Bouygues est l'un des **partenaires Français les plus reconnus de Microsoft** depuis 2004.
- Nos 15 collaborateurs certifiés nous offre l'avantage d'avoir un **suivi personnalisé et une proximité privilégiée** avec les équipes commerciales et techniques de Microsoft.
- **Depuis plus de 15 ans,** C2S Bouygues couvre totalement le catalogue d'offre de Microsoft.

Ils nous font confiance



FOCUS SUR LA GESTION DES INCIDENTS DE SÉCURITÉ



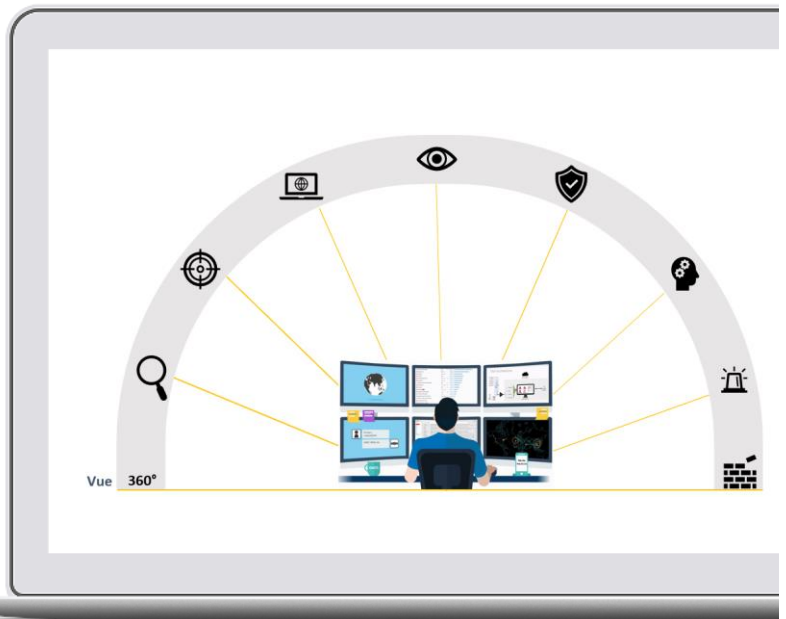
Microsoft Azure Sentinel: qu'est ce que c'est ?

Azure Sentinel est un SIEM (Security Information and Event Management) et un SOAR (Security Orchestrated Automated Response) qui permet de :

- Collecter les données de sécurité sur l'ensemble des utilisateurs, infrastructures, équipements et applications on premise et issue des Cloud publics ou privés des clients.
- Agréger et corréler les logs afin de détecter les menaces
- Investiguer pour repérer l'activité suspecte
- Faciliter et accélérer la réponse aux incidents au travers d'une orchestration et automatisation intégrée

Un SOC (Security Operation Center) : qu'est ce que c'est ?

Un SOC désigne une division qui assure la sécurité de l'organisation et de l'information sur un périmètre donné.



Un SOC est :

- Une organisation
- Des process
- Des outils de collecte et d'analyse
- Des workflows

Son rôle est de :

- Surveiller les équipements et applications de l'entreprise
- Gérer les incidents de sécurité préalablement identifiés et analysés
- Permettre de détecter les Cyberattaques ou intrusions
- Déterminer s'il s'agit d'une menace réelle et malveillante
- Répondre aux incidents

Intégrer le SIEM Sentinel dans un SOC

Azure Sentinel (SIEM) permet une supervision centralisée de gestion, de management et d'analyse de la sécurité.

Collecte

Azure Sentinel

Agrégation
Normalisation
Corrélation
Archivage
Reporting

Analyse

Équipe d'experts SOC

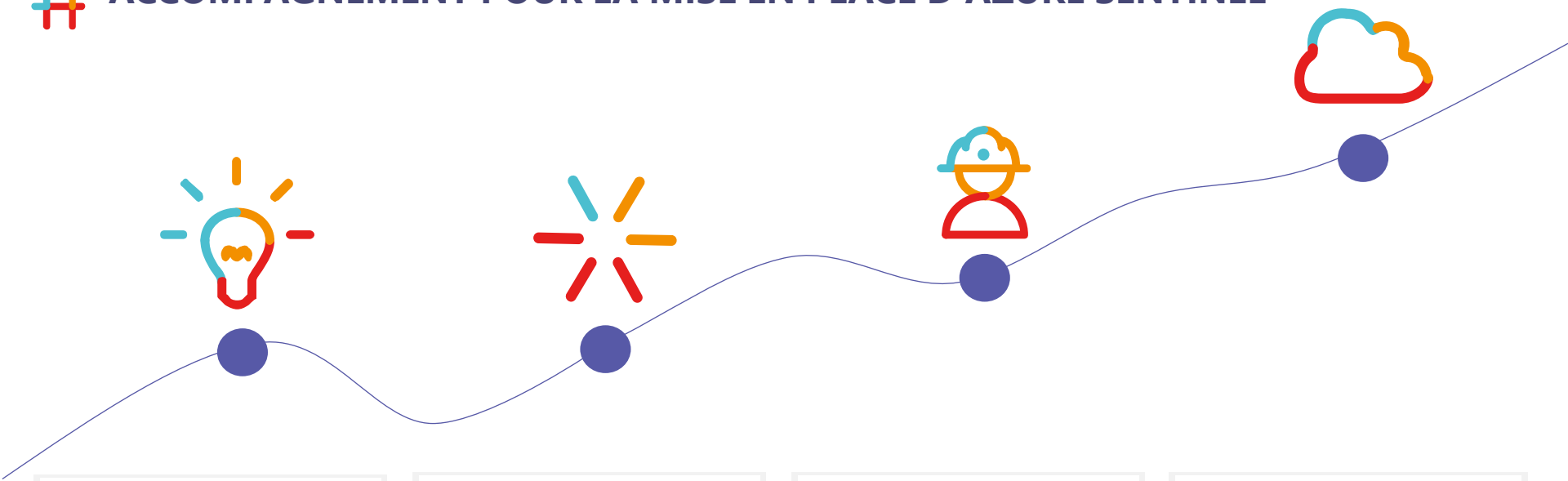
Assurent la sécurité de l'information et des actifs de l'entreprise

- Déclenchement et qualification d'alerte
- Suivi de l'incident
- Notification et communication Client
- Réponse aux incidents de sécurité

AMELIOREZ VOTRE CYBER SECURITE !

AUGMENTEZ LA DETECTION DES MENACES SUR VOTRE SI
IMPLEMENTONS ENSEMBLE MICROSOFT AZURE SENTINEL

ACCOMPAGNEMENT POUR LA MISE EN PLACE D'AZURE SENTINEL



CADRAGE

Identification
&
Définition du projet

ETUDE

Etude
&
Analyse du périmètre
et
des risques

BUILD & PRE-RUN

Implementation de la solution
&
Démarrage Pré-Run

RUN

Industrialisation, surveillance personnalisée, amélioration continue
&
Suivi des KPI

OFFRE C2S – AZURE SENTINEL

Etude

- Accompagnement pour l'identification et la définition du projet
- Etude et analyse du périmètre
- Analyse de risques macro et des scénarios de cyberattaque redoutés
- Accompagnement sur les aspects licence (tarification, revente)
- Elaboration d'un plan projet global
- (Organisation, ressource, planning, procédures et couts complets)

Mise en œuvre

- Collecte et centralisation de l'ensemble des logs du périmètre
- (Au besoin avec un log manager)
- Prévoir un périmètre itératif
- Pilotage de la mise en place d'Azure Sentinel Branchement des connecteurs des sources on premise ou cloud
  - Paramétrage des règles de détection et corrélation
  - Interface avec l'outil de management des alertes C2S pour le traitement et pilotage des remédiations
  - Tests
  - Développement du reporting
  - Mise en place des playbooks

Supervision Managée

- Elaboration et validation de tous les éléments contractuels de la prestation de services managés
  - Plages de supervision
  - Sévérité des alertes
  - Niveau d'escalade
  - SLAs en fonction de la sévérité
- Comitologie de la prestation
- Amélioration continue de la détection et du pilotage de la réaction
- Adaptation du reporting
- Extension du périmètre du SOC aux enjeux cyber

SUCCESS STORIES

AVEC NOS 3 MARCHÉS PRIVILÉGIÉS

Digital & IT Market

Automation of HR tasks
SharePoint list
Power BI Dashboard
Enhance Onboarding capabilities
Use of the power of Outlook

Holding d'un groupe du CAC 40

300 employées

Contexte et enjeux client :

Le client constate la multiplication des menaces et des cyber attaques dans le monde et aussi bien en France. Il est conscient de son exposition aux risques cyber au regard de ses activités stratégiques et de l'impact potentiel sur la confiance de ses partenaires et de ses clients B2B et B2C.

La mise en place d'un SOC permet de détecter au plus tôt les incidents de sécurité et de réduire leur impacts à travers une remédiation efficiente.

Périmètre du client et choix d'AZURE SENTINEL :

- Le client utilise fortement la suite Microsoft 365 dans toutes ses composantes.
- Un benchmark a permis d'établir la pertinence de la solution AZURE Sentinel comme SIEM versus les autres solutions du marché (on premise ou cloud).
    - Absence de projet technique d'infrastructure du SIEM car Sentinel est une solution SAAS
    - Connecteurs natifs dans le cloud M365
    - Facilité de collecte des logs on premise
    - Rapidité de mise en œuvre avec une bonne documentation en ligne
    - Maitrise des couts
    - Dashboarding de qualité

Valeur apportée au client :

- Un service de SOC de qualité et évolutif pour contenir les risques cyber.
- Enrichissement continu de nouvelles features sécurité de la part de Microsoft sur l'ensemble de son écosystème AZURE.
- Une intégration de la solution dans le contrat Microsoft du client

Méthodologie :

- Démarche itérative et agile sur un périmètre pilote de log et de use case
- Amélioration continue

MERCI

C2S BOUYGUES
construisons votre avenir digital

CONTACT COMMERCIAL

C2S BOUYGUES
construire votre avenir digital

ANISSA LABED
alabed@c2s.fr
07 64 38 34 22

www.c2s-bouygues.com