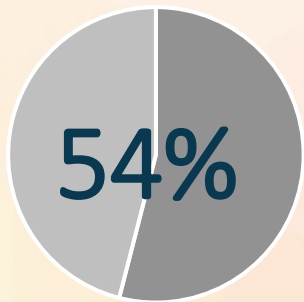
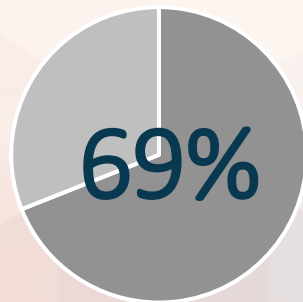




BUBO.
CYBERSEC



En France, près d'une entreprise sur 2 a été visé par une cyberattaque en 2021



69% des entreprises victimes sont des TPE/PME

50 000 €

Coût médian d'une cyberattaque

- Interruption du business
- Détérioration du matériel informatique
- Fuite de données nécessaire aux opérations
- Impact sur la notoriété



+255%

d'attaques par ransomware en 2021



94% des logiciels malveillants sont délivrés par e-mail



23 jours

Période pendant laquelle l'organisation ciblée est paralysée lors d'une attaque



Toutes les 11 secondes

Prévision concernant les attaques contre des entreprises



Dirigeants, DSI, RSSI, DPO, ... Pouvez vous répondre à ces questions ?

Suis-je en mesure de pouvoir me positionner par rapport aux standards actuels (normes, exigences...) ?

Comment puis-je répondre aux garanties de sécurité numérique imposées par mes clients et les rassurer ?

Je veux savoir si Mr Dupont peut accéder au dossier RH.

Je veux savoir qui a créé l'utilisateur toto la semaine dernière.

Je veux savoir si j'ai des systèmes vulnérables sur mon infrastructure.

Je n'ai pas d'expert en cybersécurité dans mon entreprise, comment puis-je traiter les problématiques cybersécurité.

Je veux savoir qui a effectué cette commande/action sur mes systèmes.



BUBO
CYBERSEC

Une solution de tableau de bord de cybersécurité



SENTRY

Ensemble des tableaux de bord de sécurité facilement lisibles et compréhensibles pour la gestion de la sécurité de l'information. Le cyberscore Bubo, les organisations thématiques ou la visibilité de la conformité rendent notre solution accessible et facile à utiliser.

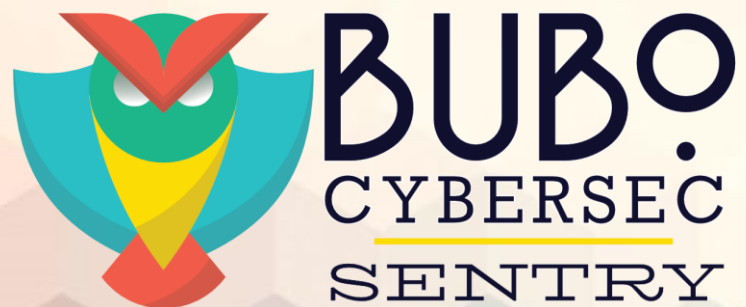
Un système clé en main de gestion des informations et des événements de sécurité



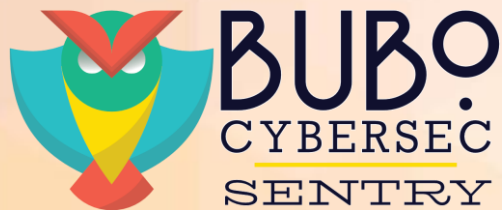
HUNT

Un moyen simple et abordable pour construire un SIEM. Notre solution intègre un système de gestion des journaux, des alertes, le suivi des indicateurs de compromission et des tableaux de bord thématiques.

Des solutions pensées et conçues en apportant une réponse aux attentes des PME et ETI sur le marché français et intègrent des solutions Open source afin de fournir une solution rentable pour gérer les fondamentaux de la sécurité de l'information.



PILOTEZ VOTRE CYBERSÉCURITÉ



BUBO
CYBERSEC
SENTRY

Une solution de tableau de bord de cybersécurité

Pensé, conçu et adapté aux besoins des **PME** ou **ETI**, Bubo Cybersec SENTRY est une solution clé en main.

Tous les indicateurs de sécurité sont construits de façon identique.

Score sécurité : Visualisez la situation en un coup d'œil pour chaque thématique. Une note de A à F pour vous permettre de surveiller facilement et rapidement les actions à mettre en place.

Aide à la décision :

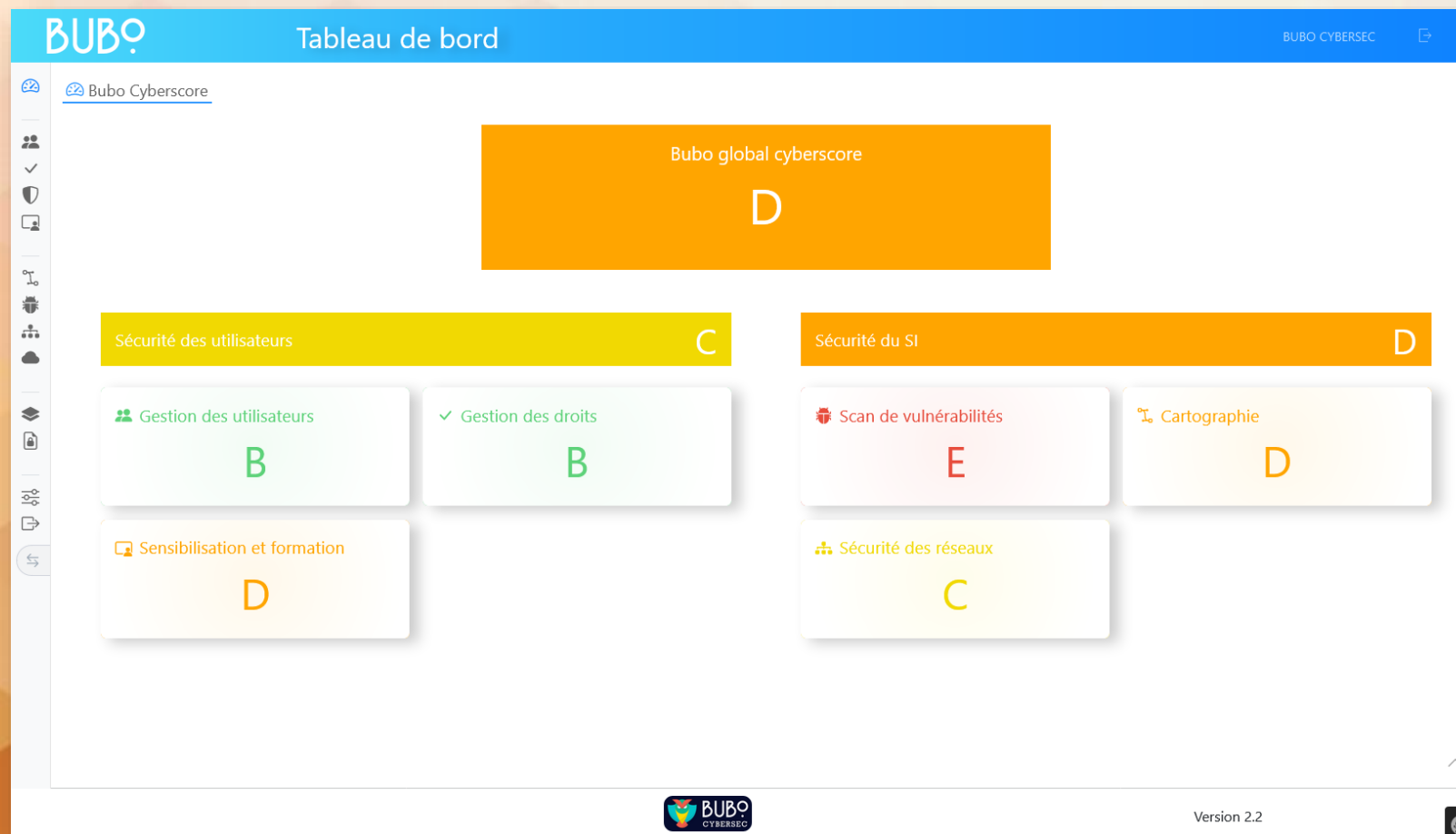
À travers les métriques, les tableaux et graphiques présents sur toutes les thématiques, Bubo Cybersec SENTRY permettra d'identifier les non-conformités et d'agir pour améliorer votre score.

L'ensemble des métriques des différents indicateurs de sécurité sont définies à partir des bonnes pratiques (**ISO 27001, ANSSI, NIST**).

Pour chaque thématique, un rapport de normes et bonnes pratiques est généré permettant de mettre les métriques que vous surveillez et piloter à travers Bubo Cybersec.

Bubo Cybersec SENTRY est installé sur une **machine virtuelle** déployée sur votre SI.

Déjà installées, configurées et paramétrées, les premières notes se mettront à jour automatiquement en quelques minutes.

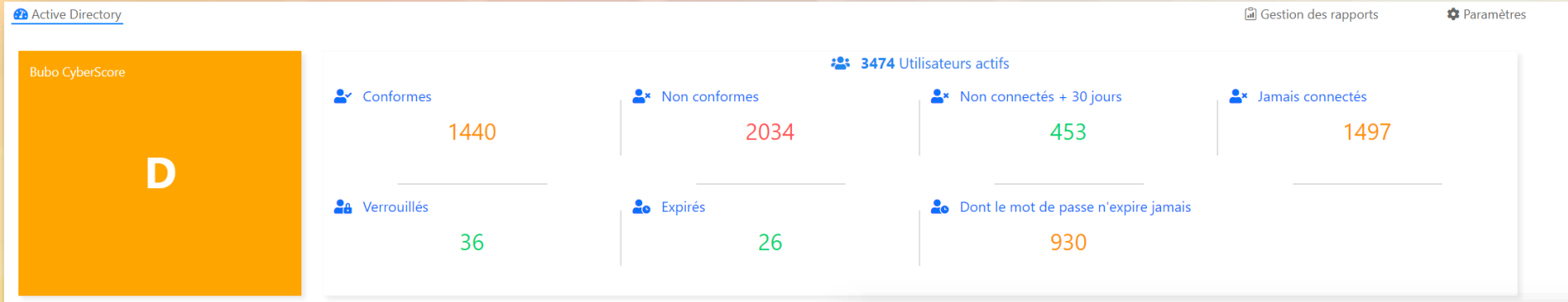


Bubo Cybersec SENTRY

Le Bubo Cyberscore permet de visualiser rapidement les priorités et les actions à mettre en place.
Concentrez-vous sur les fondamentaux de la sécurité de votre SI

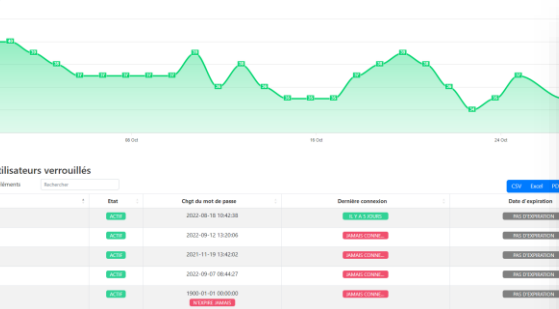
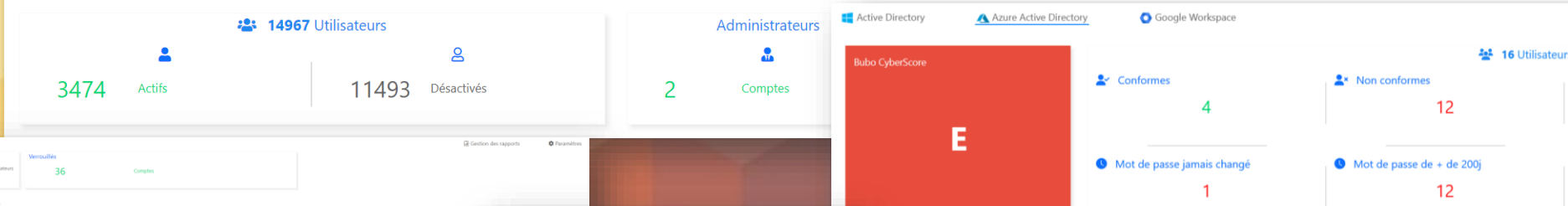
Sécurité des utilisateurs

Gestion des utilisateurs



L'indicateur « Gestion des utilisateurs » se connecte à l'Active Directory.

Tous les métriques mises en avant sont ceux recommandés par le guide l'hygiène de l'ANSSI ou ISO.



Détails utilisateurs

Identité

Nom: N/A
 Identifiant de connexion: TRUF_003
 Description: Compte MATTHEW MARETS TRUFAUT

Statut

État du compte: **ACTIF**
 Expiration du compte: **NE PAS EXPIRER**
 Date de création: 2022-04-08 10:33:16
 Dernière modification: 2022-04-08 10:33:16
 Dernière connexion: **INACTIF (COMPTES)**

Droits

Compte administrateur: **NON**
 OU: PARTENAIRES/Utilisateurs/SPR
 Exclure: **EXCLURE**

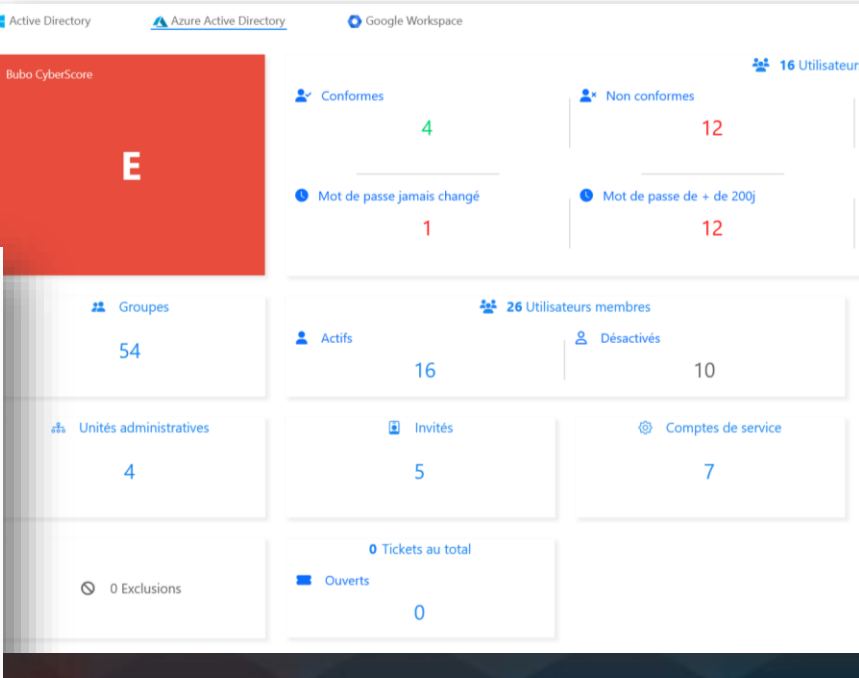
Mot de passe

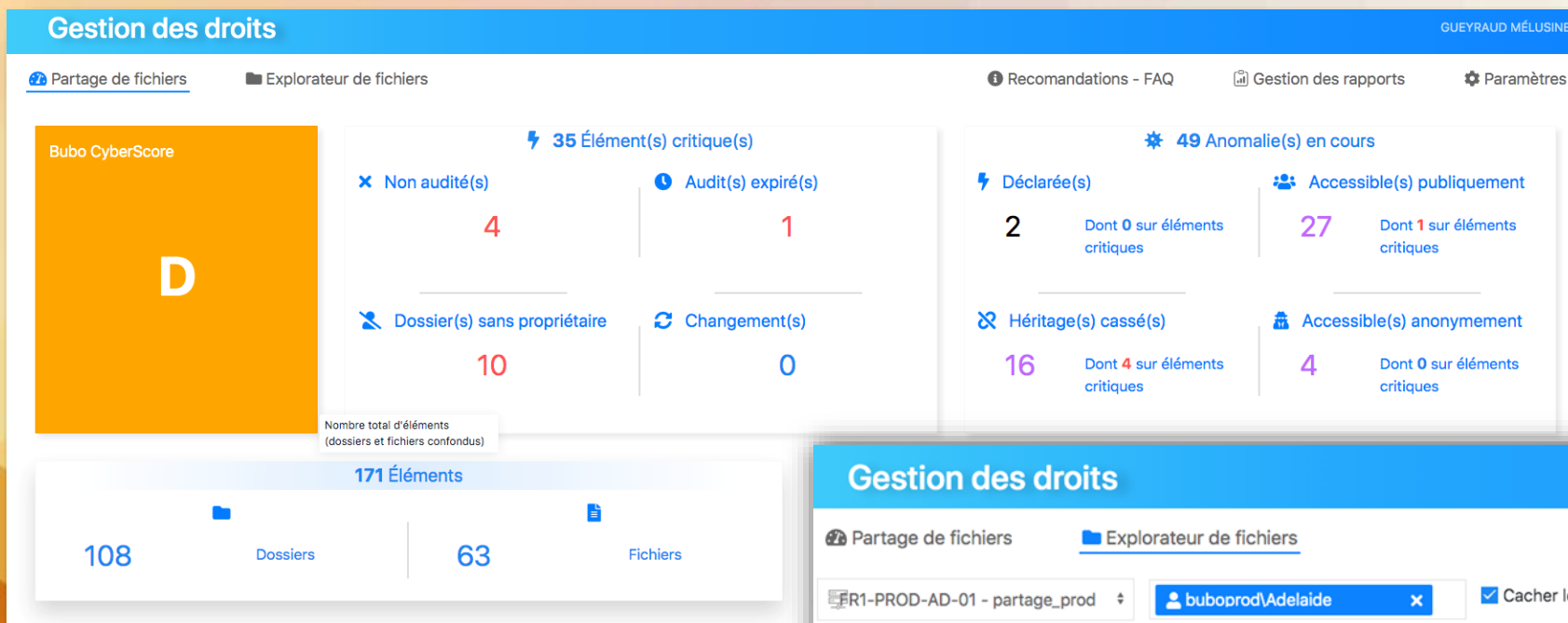
Dernière mise à jour: 2022-04-08 10:33:16
 Expiration du mot de passe définie: **15 JOURS (ACTIF)**
 Mot de passe expiré: **NON**

Liste des utilisateurs verrouillés

Afficher: 10 éléments

Identifiant	Etat	Chgt du mot de passe	Dernière connexion	Date d'expiration
950016\admin	ACTIF	2022-08-18 16:42:38	2022-08-18 16:42:38	NE PAS EXPIRER
950075	ACTIF	2022-09-12 13:20:06	2022-09-12 13:20:06	INACTIF (COMPTES)
950080	ACTIF	2021-11-19 13:42:50	2021-11-19 13:42:50	NE PAS EXPIRER
950059	ACTIF	2022-09-07 08:44:27	2022-09-07 08:44:27	NE PAS EXPIRER
951239	ACTIF	1900-01-01 00:00:00	1900-01-01 00:00:00	NE PAS EXPIRER





Gestion des droits GUEYRAUD MÉLUSINE

Partage de fichiers | Explorateur de fichiers | Recommandations - FAQ | Gestion des rapports | Paramètres

Bubo CyberScore

D

Nombre total d'éléments (dossiers et fichiers confondus)

35 Élément(s) critique(s)

Non audité(s)	Audit(s) expiré(s)
4	1
Dossier(s) sans propriétaire	Changement(s)
10	0

49 Anomalie(s) en cours

Déclarée(s)	Accessible(s) publiquement
2 <small>Dont 0 sur éléments critiques</small>	27 <small>Dont 1 sur éléments critiques</small>
Héritage(s) cassé(s)	Accessible(s) anonymement
16 <small>Dont 4 sur éléments critiques</small>	4 <small>Dont 0 sur éléments critiques</small>

171 Éléments

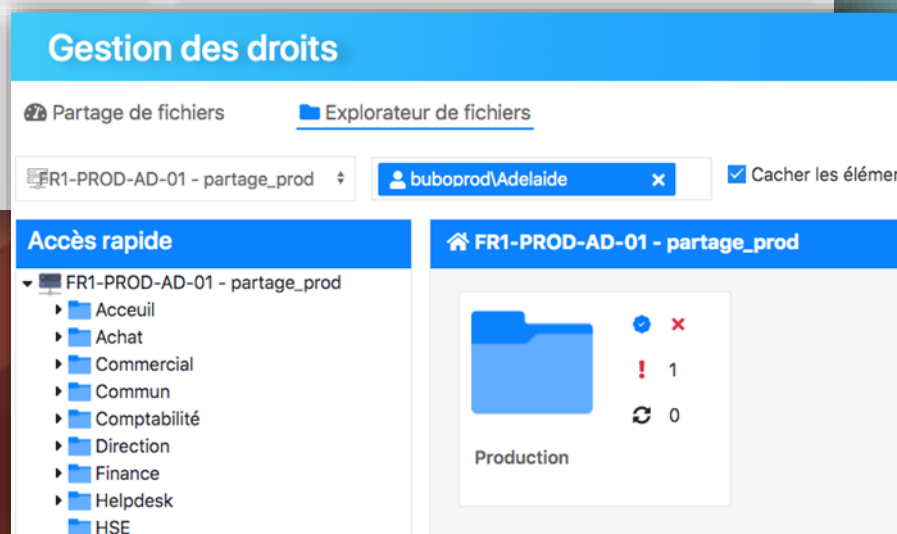
108 Dossiers	63 Fichiers
--------------	-------------

L'indicateur « Gestion des droits » se connecte à votre serveur de fichier Microsoft.

Un explorateur de fichier permet de rechercher simplement et rapidement les informations recherchées :

- Qui a accès au dossier Production ?
- À quel dossier « Adelaïde » peut accéder ?
- ...

Bubo Cybersec SENTRY, vous accompagne dans la réalisation de vos audits de droits sur vos fichiers.



Gestion des droits

Partage de fichiers | Explorateur de fichiers

FR1-PROD-AD-01 - partage_prod | buboprodAdelaide | Cacher les éléments

Accès rapide

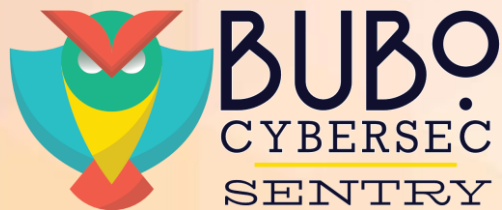
- FR1-PROD-AD-01 - partage_prod
 - Acueil
 - Achat
 - Commercial
 - Commun
 - Comptabilité
 - Direction
 - Finance
 - Helpdesk
 - HSE

FR1-PROD-AD-01 - partage_prod

Production

! 1

🔄 0



Une solution de tableau de bord de cybersécurité

Sécurité du SI

Gestion des vulnérabilités systèmes

Vulnérabilités systèmes | 42 Vulnérabilité(s)

Bubo CyberScore **E**

- Critique(s): 2
- Haute(s): 4
- Moyenne(s): 30
- Basse(s): 6

6 Système(s) vulnérable(s)

- Avec vulnérabilité critique(s): 1
- Avec vulnérabilité haute(s): 1
- Avec vulnérabilité moyenne(s): 6
- Avec exploit public: 0

Évolution des vulnérabilités

- Nouvelle(s) (7 jours): 0
- Corrigée(s) (7 jours): 0
- Composant(s) vulnérable(s): 9
- Faux positifs: 0

Caractéristiques de la vulnérabilité

Nom: Microsoft SQL Server End Of Life Detection

NOCVE: NOCVE

AVN/AcL/Au/N/C/C/C/C/C

The Microsoft SQL Server version on the remote host has reached the end of life and should not be used anymore. An end of life version of Microsoft SQL Server is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Checks if a vulnerable version is present on the target host.

The "Microsoft SQL Server 2000" product on the remote host has reached the end of life. CPE: cpe:/a:microsoft/sql_server:2000 EOL version: 2000 EOL date: unknown

1433/tcp

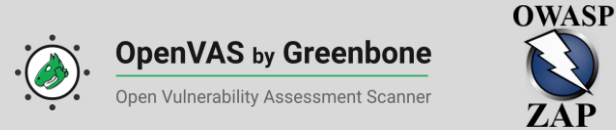
VendorFix: Update the Microsoft SQL Server version on the remote host to a still supported version.

Adresse IP	FQDN	Dernier scan
172.21.41.145		2022-10-05 17:12:07

Vulnérabilités

Vulnérabilités Systèmes ET Web

Deux scanners de vulnérabilités Open source déjà configurés et paramétrés pour vous permettre de surveiller vos vulnérabilités.



Une description est fournie pour chacune des vulnérabilités identifiées.

Nombre de vulnérabilités ces 30 derniers jours

Actifs systèmes avec vulnérabilités

Nom	Famille	Système	Adresse IP
DCL/RPC and MSRPC Services Enumeration Reporting	Windows	P06ADCCD-01	172.22.8.15
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	SSL and TLS	P06ADCCD-01	172.22.8.15
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	SSL and TLS	P06ADCCD-01	172.22.8.15
DCL/RPC and MSRPC Services Enumeration Reporting	Windows	P06ADDDCCD-01	172.22.9.1
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	SSL and TLS	P06ADDDCCD-01	172.22.9.1
DCL/RPC and MSRPC Services Enumeration Reporting	Windows	P06ADDDCCD-03	172.22.13.15
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	SSL and TLS	P06ADDDCCD-03	172.22.13.15
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	SSL and TLS	P06ADDDCCD-03	172.22.13.15
DCL/RPC and MSRPC Services Enumeration Reporting	Windows	GECCODAGE-PRO	172.21.41.145
Microsoft SQL Server End Of Life Detection	Databases	GECCODAGE-PRO	172.21.41.145
Microsoft SQL Server End Of Life Detection	Databases	GECCODAGE-PRO	172.21.41.145

Gestion des vulnérabilités web

Vulnérabilités systèmes | **Vulnérabilités web** | 96 Vulnérabilité(s)

Bubo CyberScore **D**

- Haute(s): 0
- Moyenne(s): 21
- Basse(s): 75

2 Actif(s) web vulnérable(s)

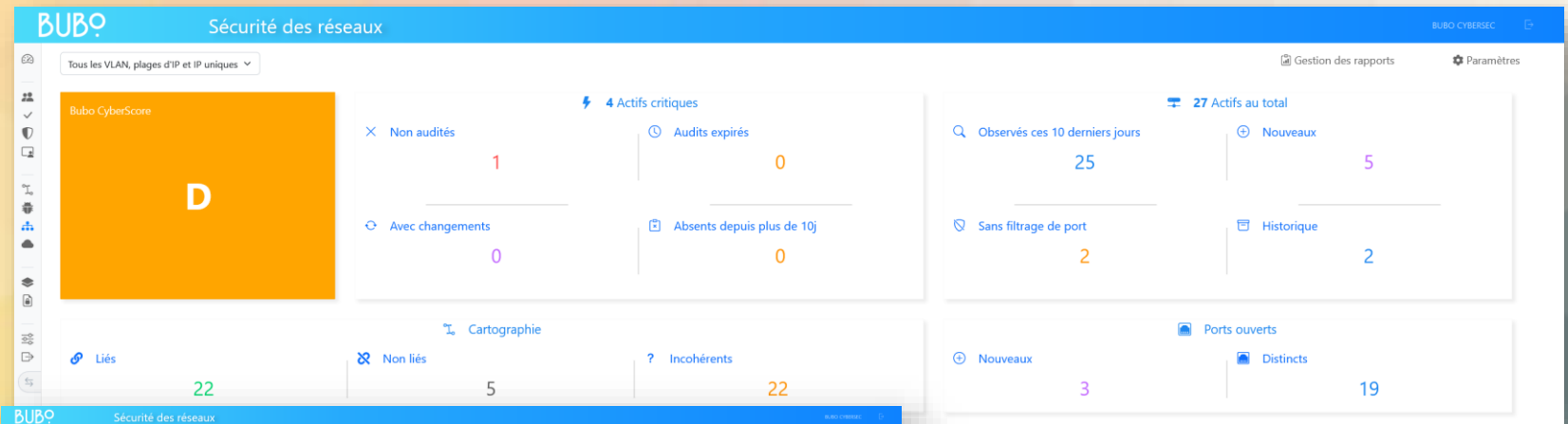
- Avec vulnérabilité haute(s): 0
- Avec vulnérabilité moyenne(s): 2
- Avec vulnérabilité basse(s): 2

Évolution des vulnérabilités

- Nouvelle(s) (dernier scan): 67
- Corrigée(s) (dernier scan): 0
- Informative(s): 41
- Faux positif(s): 0

Sécurité du SI

Sécurité des Réseaux



BUBO Sécurité des réseaux

Tous les VLAN, plages d'IP et IP uniques

Bubo CyberScore: **D**

4 Actifs critiques

- Non audités: 1
- Audits expirés: 0
- Avec changements: 0
- Absents depuis plus de 10j: 0

27 Actifs au total

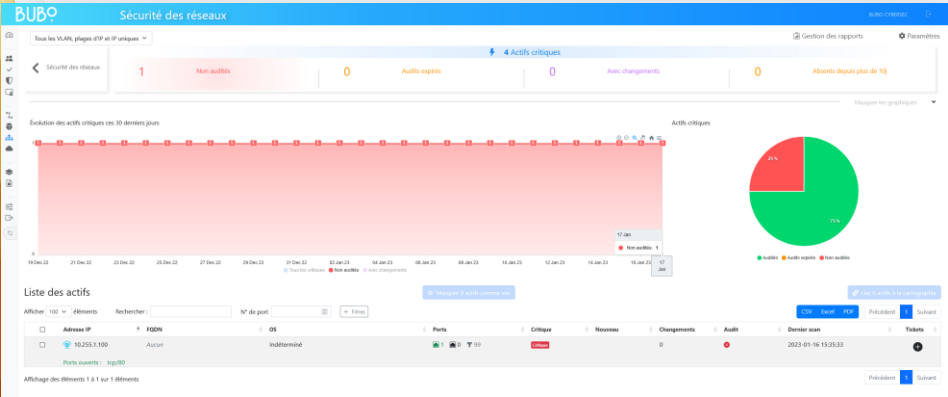
- Observés ces 10 derniers jours: 25
- Nouveaux: 5
- Sans filtrage de port: 2
- Historique: 2

22 Liés, 5 Non liés, 22 Incohérents

3 Nouveaux, 19 Ports ouverts

Sécurité des réseaux

Ce scanner de réseau intégré dans BUBO CYBERSEC, vous permet d'auditer vos actifs, d'importer les actifs dans votre cartographie ou d'identifier les ports ouverts et fermés.



BUBO Sécurité des réseaux

1 Non audités, 0 Audits expirés, 0 Avec changements, 0 Absents depuis plus de 10j

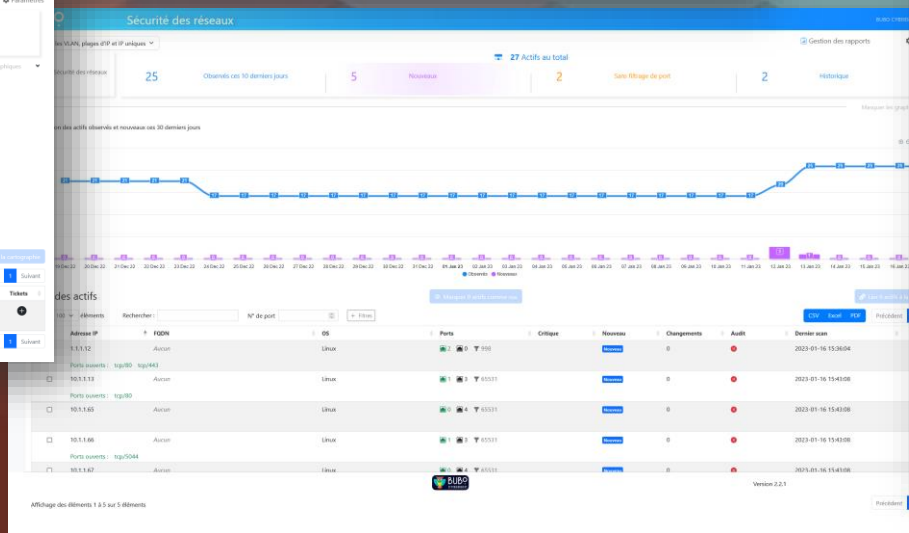
4 Actifs critiques

Evolution des actifs critiques ces 30 derniers jours

Actifs critiques

Liste des actifs

Adresse IP	FQDN	OS	Ports	Critique	Nouveaux	Changements	Audit	Dernier scan
10.255.1.100	Aucun	Indéterminé	80, 443	Non	Non	Non	Non	2023-01-16 15:35:33

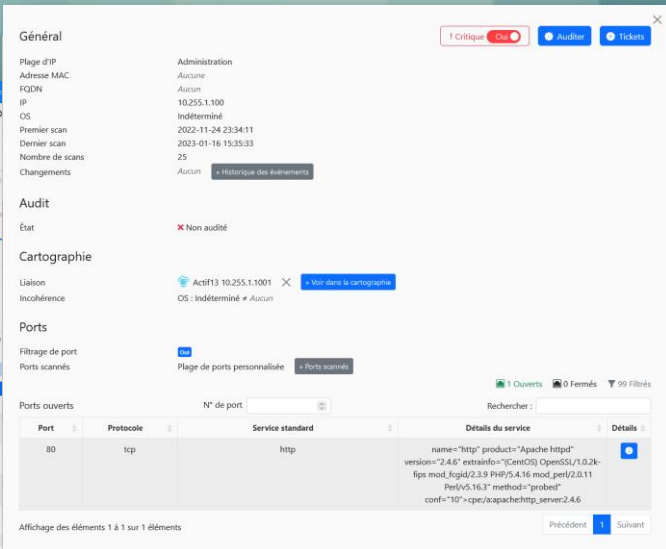


BUBO Sécurité des réseaux

25 Observés ces 10 derniers jours, 5 Nouveaux, 2 Sans filtrage de port, 2 Historique

des actifs

Adresse IP	FQDN	OS	Ports	Critique	Nouveaux	Changements	Audit	Dernier scan
10.255.1.100	Aucun	Linux	80, 443	Non	Non	Non	Non	2023-01-16 15:36:04
10.255.1.101	Aucun	Linux	80, 443	Non	Non	Non	Non	2023-01-16 15:43:08
10.255.1.102	Aucun	Linux	80, 443	Non	Non	Non	Non	2023-01-16 15:43:08
10.255.1.103	Aucun	Linux	80, 443	Non	Non	Non	Non	2023-01-16 15:43:08
10.255.1.104	Aucun	Linux	80, 443	Non	Non	Non	Non	2023-01-16 15:43:08



Général

- Plage d'IP: Aucune
- Adresse MAC: Aucun
- FQDN: 10.255.1.100
- IP: Indéterminé
- OS: Indéterminé
- Premier scan: 2022-11-24 23:34:11
- Dernier scan: 2023-01-16 15:35:33
- Nombre de scans: 25
- Changements: Aucun

Audit

- État: Non audité

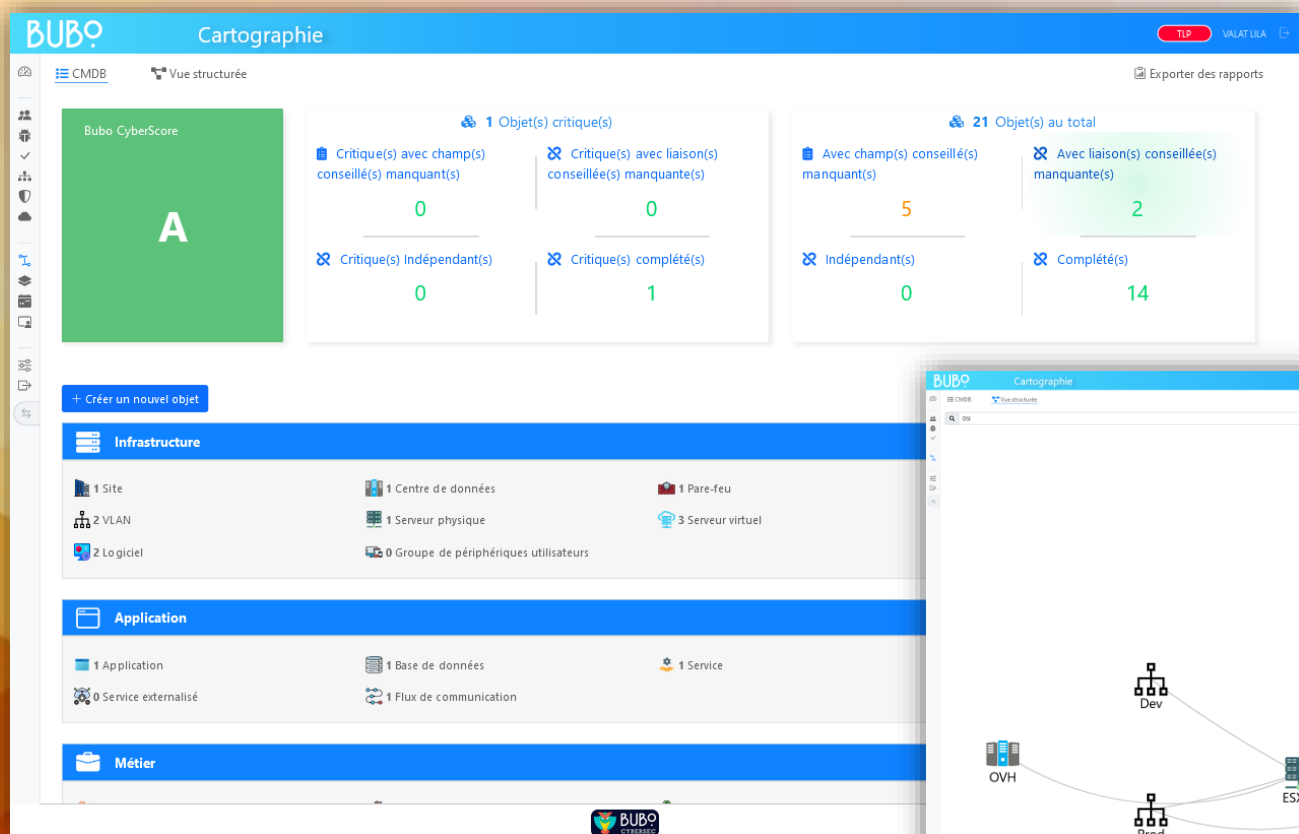
Cartographie

- Liaison: Incohérence
- Actif13 10.255.1.1001
- OS: Indéterminé

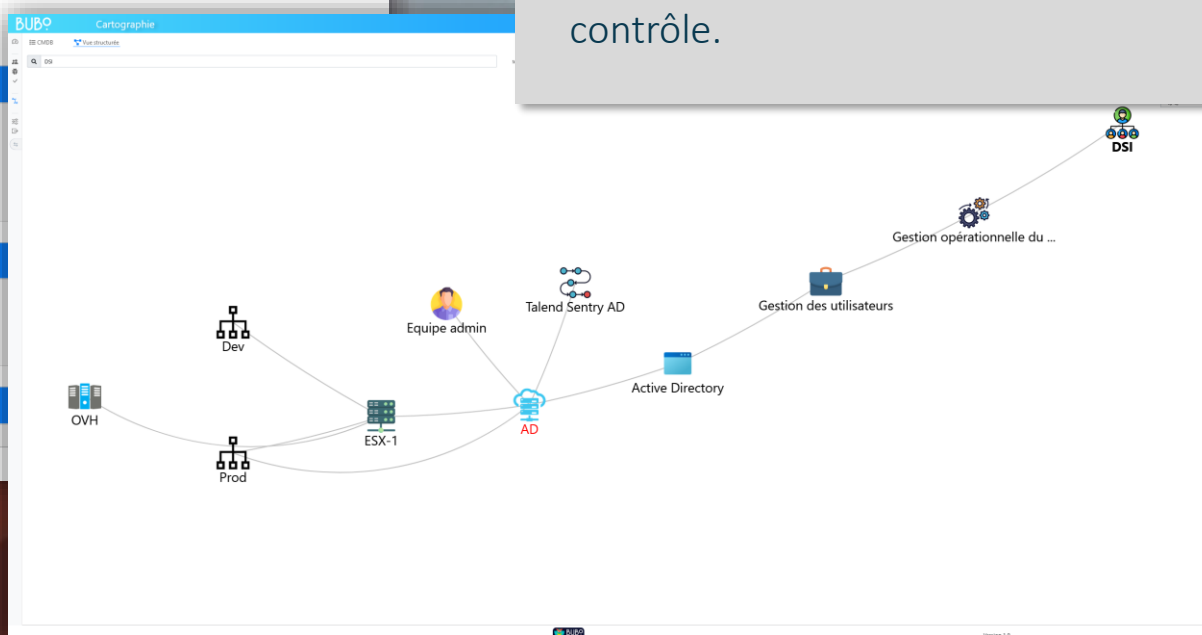
Ports

Ports ouverts

Port	Protocole	Service standard	Détails du service
80	tcp	http	name="http" product="Apache httpd" version="2.4.6" extrainfo="CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3" method="probes" conf="10" -cpe:/a:apache:http_server:2.4.6



Outil indispensable à la maîtrise de son système d'information, la cartographie du SI permet de connaître l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité, et donc un meilleur contrôle.



Déploiement de BUBO SENTRY

1 mois

Evaluation sécurité et conformité

Approfondissement

Restitution

4 demi-journées

STANDARD

Abonnement

Engagement sur 2 ans

4 800€ HT/an

Maintenance – Support (obligatoire)

- Appels/Tickets et supports de l'applications
- Mise à jour des versions mineurs

1 200€ HT/an

FAS (année 1)

- Déploiement de la VM sur le SI client
- Configuration et paramétrages des différents indicateurs
- Transfert de compétences (1 à 2 utilisateurs)

2 500€ HT

MULTI

Abonnement

- Module de supervision centralisé
- Engagement sur 2 ans

+ 3 600€ par SENTRY déployé/an

Maintenance – Support (obligatoire)

- Appels/Tickets et supports de l'applications
- Mise à jour mineurs
- + 900€ par sentry déployé

+ 900€ par SENTRY déployé/an

FAS

- Déploiement de la VM sur le SI client
- Configuration et paramétrages des différents indicateurs
- Transfert de compétences (1 à 2 utilisateurs)
- FAS à 1 250€ par SENTRY supplémentaire

+ 1 250€ par SENTRY déployé

SENTRY Managé

Nos équipes opèrent pour vous

Standard

- Surveillance hebdomadaire des métriques et anomalies
- Qualification, assistance et escalade auprès des équipes concernées (internes ou externes)
- 1 rapport par mois

12 000 € HT/an

Multi

- Surveillance hebdomadaire des métriques et anomalies
- Qualification, assistance et escalade auprès des équipes concernées (internes ou externes)

+ 6 000€ par SENTRY déployé/an

Audit Flash

- Prise en compte du contexte
- Evaluation sécurité et conformité
- Approfondissement
- Restitution
- Déploiement de BUBO SENTRY pour 1 mois
- 4 demi-journées
- Maximum 250 employés

5 000€ HT



SURVEILLER LA SÉCURITÉ DE VOTRE SI



Surveiller la sécurité de votre SI

Un système clé en main de gestion des informations et des événements

- ✓ Récupérer les événements de mon SI
- ✓ Visualiser et traiter mes événements grâce à des tableaux de bord personnalisés pour mon entreprise
- ✓ Avoir une corrélation de mes événements avec de la détection de comportement anormal
- ✓ Avoir une solution de déclenchement d'alerte de sécurité liée aux règles de détection
- ✓ Permettre un enrichissement des événements grâce à des données Cyber Threat Intelligence
- ✓ Bénéficier d'un service centralisé de gestion des indicateurs de compromission



Grâce à OpenSearch, HUNT est un moyen simple et abordable pour construire un **SIEM**.

Notre solution intègre un système de gestion des journaux, des alertes, le suivi des indicateurs de compromission et des tableaux de bord thématiques.



OpenSearch est un Fork
Elasticsearch développé par AWS.

Ce que comprend HUNT

Intégration

Intégration et configuration de la solution OPEN SEARCH sur votre SI



Clé en main

Récupération des Logs

Mise en œuvre des parseurs pour découper les données

Création de tableaux de bord

Mise à disposition de tableaux de bord construits selon les bonnes pratiques (ANSSI, Microsoft ...)

Indicateur de compromission

Enrichissement de vos données à partir d'un service centralisé de gestion des indicateurs de compromission



Abonnement annuel

BUBO HUNT intègre les évènements selon vos besoins :

Infrastructure

- AD
- Windows
- Linux

Collaboratif

- Office 365
- Google Workspace

Sécurité

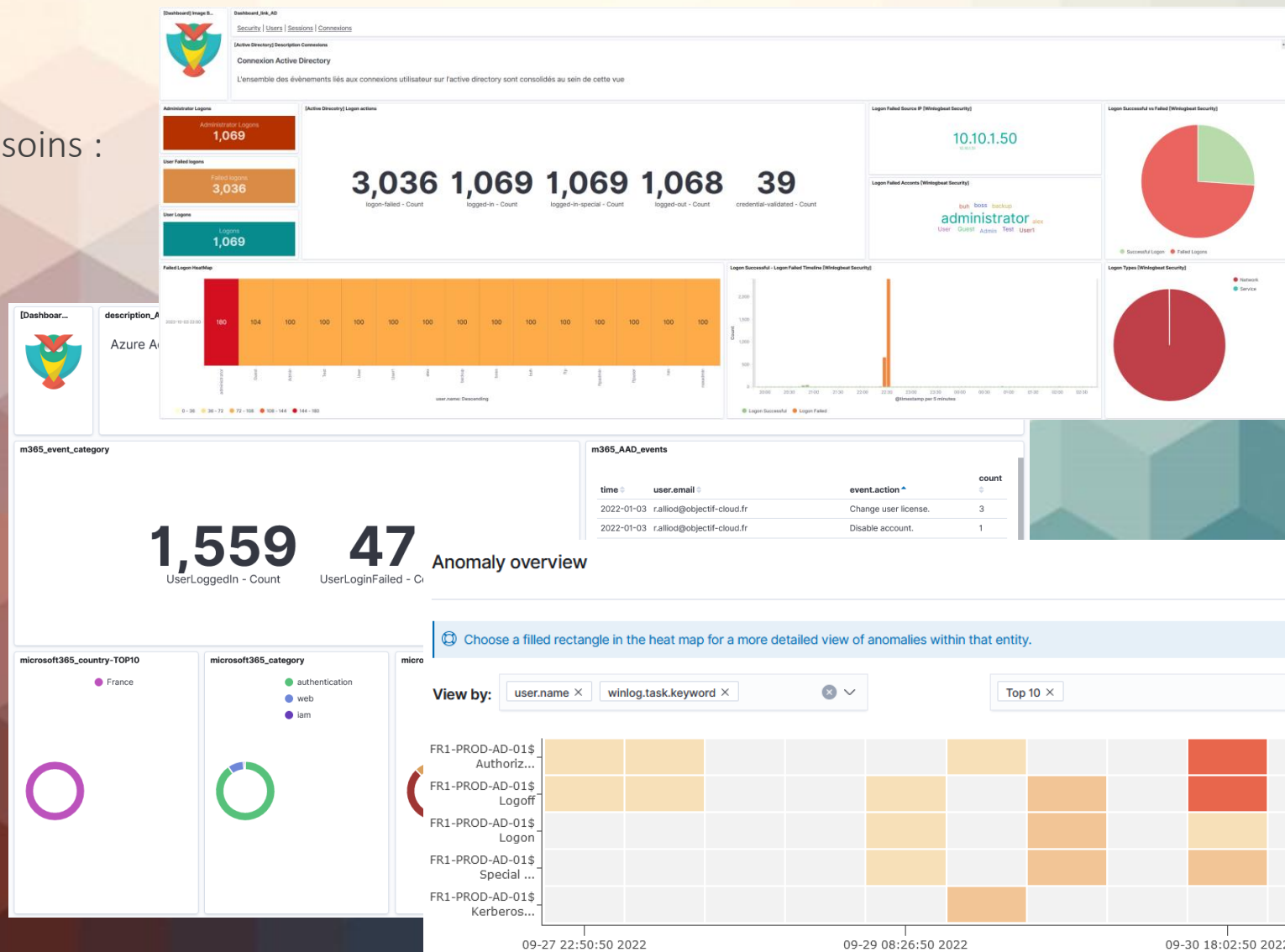
- Anti-virus
- Firewall UTM

Applicatif web

- Apache
- IIS

CUSTOM

- EDR, DLP, Réseau, autres applicatifs



1 Déploiement HUNT

Déploiement 'LIGHT'

Intégration et configuration de la solution OPEN SEARCH sur votre SI

À partir de 1 500€ HT

Déploiement 'FULL'

- Intégration et configuration de la solution OPEN SEARCH sur votre SI
- Déploiement des agents sur 10 actifs
- Collecte des logs de 10 actifs
- Transfert de compétences auprès 1 ou 2 utilisateurs
- Réunion de préparation et qualification
- Réunion de suivi au bout d'un mois
- Support pendant 1 mois
- Maximum 3 VM

5 000€ HT

2 Abonnement HUNT

- L'accès à notre Feed MISP
- Mise à disposition des tableaux de bord BUBO HUNT et parseurs associés
- Mise à disposition de nos règles d'alerting et de configuration d'IA.

Pack Infrastructure
AD, Windows et Linux

1 500€ HT/an

Pack Collaboratif
Office 365, Google Workspace

1 500€ HT/an

Pack Sécurité
Antivirus, Firewall UTM

1 500€ HT/an

Pack Applicatif Web
Apache, IIS

1 500€ HT/an

Pack Custom
EDR, DLP, Réseau, autres applicatifs

Sur devis

3 Support HUNT

Standard

Support FAQ

inclus dans les abonnements

Premium

Support ticket – GTI J+1
3 UO fournis

5 000€ HT/an

Business

Support ticket et/ou téléphonique – GTI
H+4
6 UO fournis

10 000€ HT/an

4 Prestation à la carte

Vous pouvez prendre à la demande des packages ou Unités d'œuvre

1 unité d'oeuvre	500€ HT
Pack de 5 unités d'oeuvre	2 000€ HT
Pack de 20 unités d'oeuvre	7 000€ HT

Durée de validité d'une unité d'oeuvre : 1 an

Catalogue de demande :

- Ajouter une technologie : 1 UO
- Déployer 10 agents de collecte : 1 UO
- Une journée d'assistance technique sur OpenSeach : 2 UO
- Intervention à demande : Sur devis
- Prestation (configuration, déploiement, paramétrage) : Sur devis
- Conseil/assistance : Sur devis
- ...



BUBO

CYBERSEC

Contact – Bubo Initiative
Lila Valat
06 12 06 45 54
l.valat@bubo-cybersec.com