

Octobre 2108

**Journées Cyber Sécurité
Tunis JCS'2018**

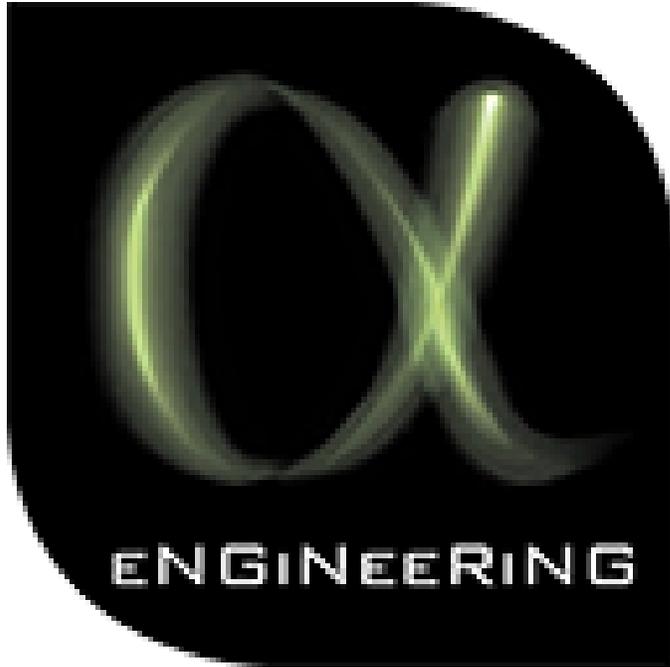
Spingy SIEM



Dr. Wassim Youssef
**ALPHA ENGINEERING &
TECHNOLOGIES**

A Propos de nous

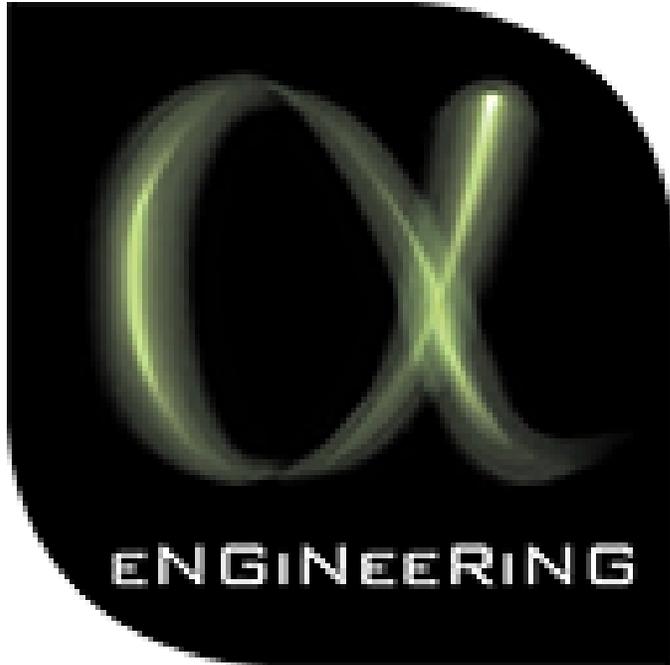
ALPHA ENGINEERING – IT Division



- Société de développement logiciel et services IT
- Créée en 2005 et présentée en Tunisie et France,
- IT Outsourcing, Cloud Computing, IoT, Big data, Solutions de surveillance et de sécurité,
- Des solutions IT avec une vraie valeur ajoutée pour le client.

A Propos de nous

ALPHA ENGINEERING – IT Division



- Monitoring, Gestion des performances et Fault Management
- Editeur d'une solution de supervision unifiée « Alpatron Unified Monitoring Platform »
- Intégration des solutions Open Source à très forte valeur ajoutée
- System Integration
- Cloud Computing

A Propos de nous

NOTRE ENGAGEMENT QUALITÉ

- SMQ mis en place selon ISO 9001 v2008
- Audits réguliers des processus par le RMQ et DQS
- Processus de la Qualité inclus dans le SMQ:
 - Integration on Open Source & 3rd Party Software Solutions
 - TMA, Managed Services, Outsourcing & Support
 - Cloud Computing Service Broker
 - Cloud Computing Managed Services
 - Telecommunication & IT Equipments Integration
 - Telecommunication & IT infrastructure Engineering
 - Telecommunication & IT Equipments Manufacturing



A Propos de nous

NOS CLIENTS

Services, Media & Telecom



Gouvernement et institutions



Industrie, Distribution, Energie



World Wide Projects



Algerie
Allemagne
Burkina Faso
Cote d'ivoire
CANADA
Dubai
France
Gabon
Guinea
Libye
Maroc
Mauritania
Niger
Royaumes unis
Senegal
Togo
Tunisia
U.S.A

1

À propos de nous

2

Métier et sécurité

3

Solution SIEM

4

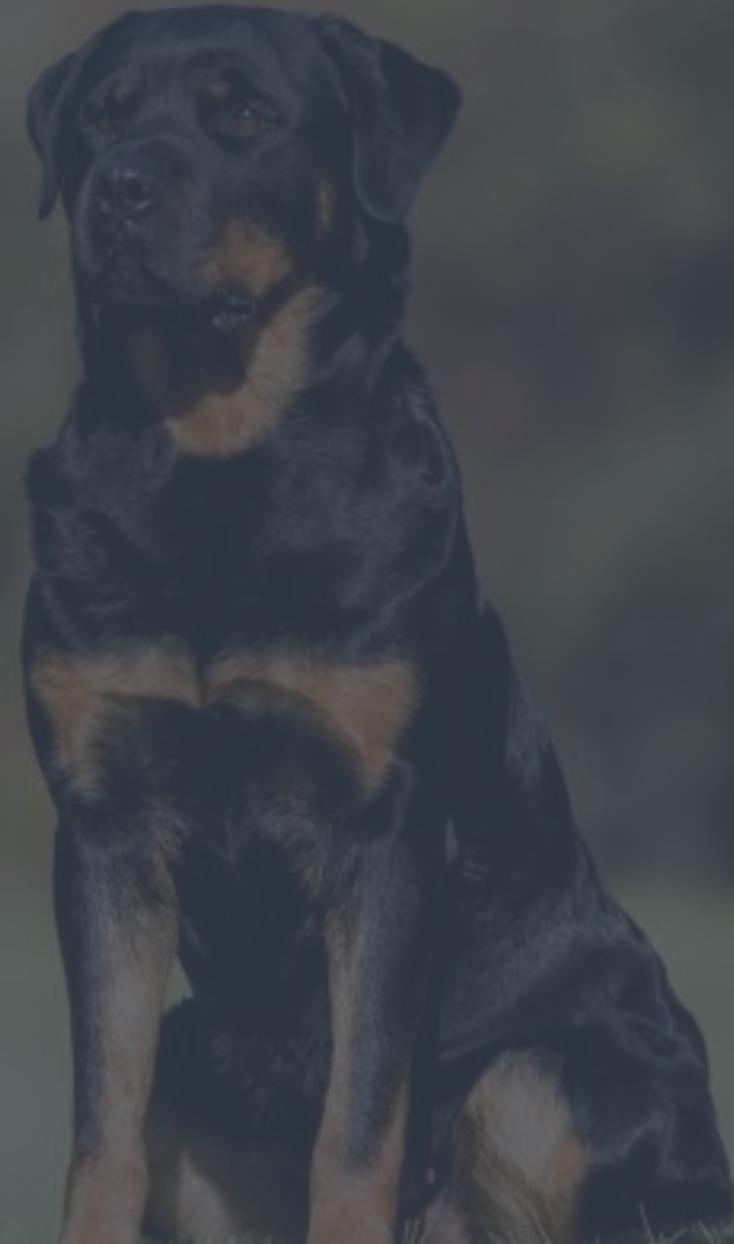
Visite guidée

5

Démo

6

Next Step



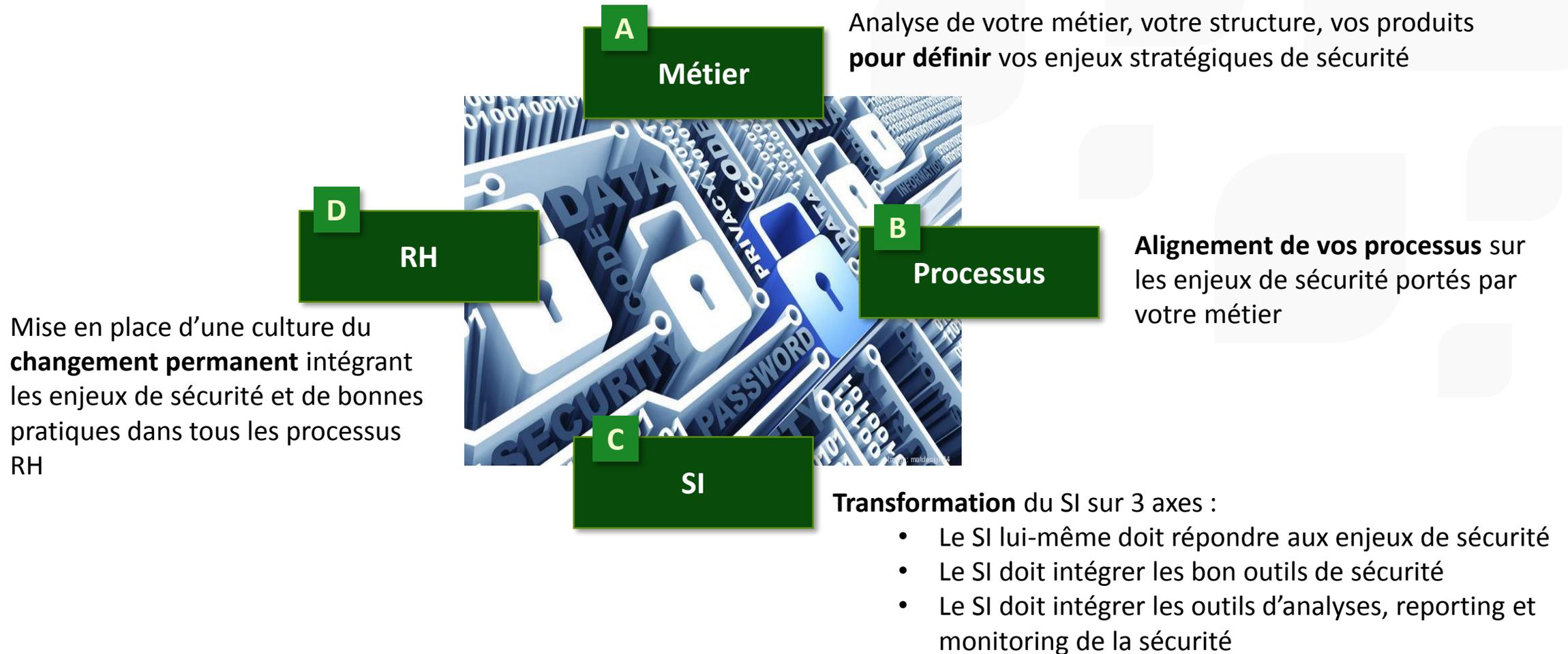
FACTS

- Entreprise : métier composante la plus importante
Le Métier est spécifique
- Données, **maitrise** des données : clés de voute de sucées entreprise, encore plus dans l'ère de la **digitalisation**
- Système d'Information : pierre angulaire pour assurer le métier de l'entreprise

FACTS

- Sécurité des données et du SI est un besoin fonctionnel
- Risques génériques de sécurité
- Risques spécifiques (liées au métiers)
- Besoins d'identifier les risques, prévenir et identifier rapidement les incidents, apporter rapidement une réponse
 - Outils informatiques
 - Processus, notamment RH
 - Diffusion de la culture de sécurité

■ Vision : des missions d'analyse des stratégies de sécurité qui passe par un cercle vertueux du changement



1

À propos de nous

2

Métier et sécurité

3

Solution SIEM

4

Visite guidée

5

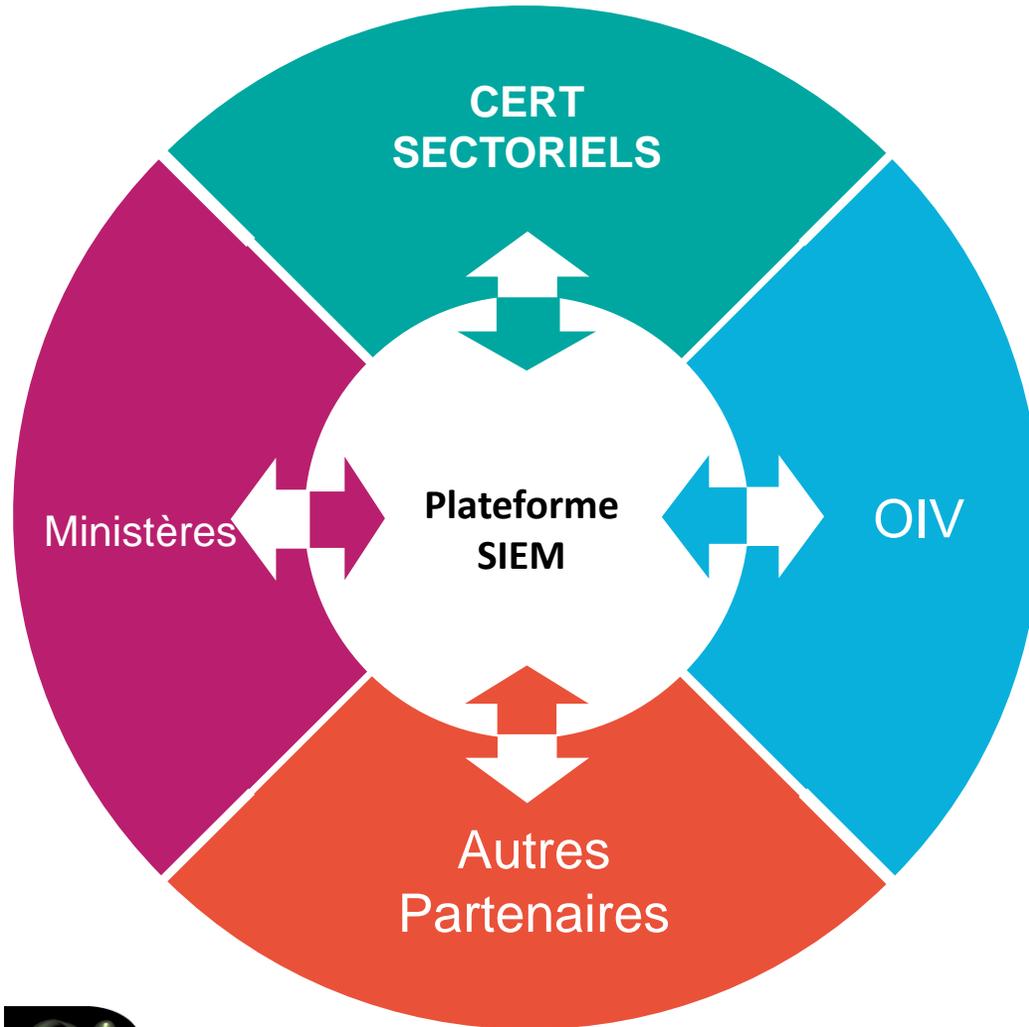
Démo

6

Next Step

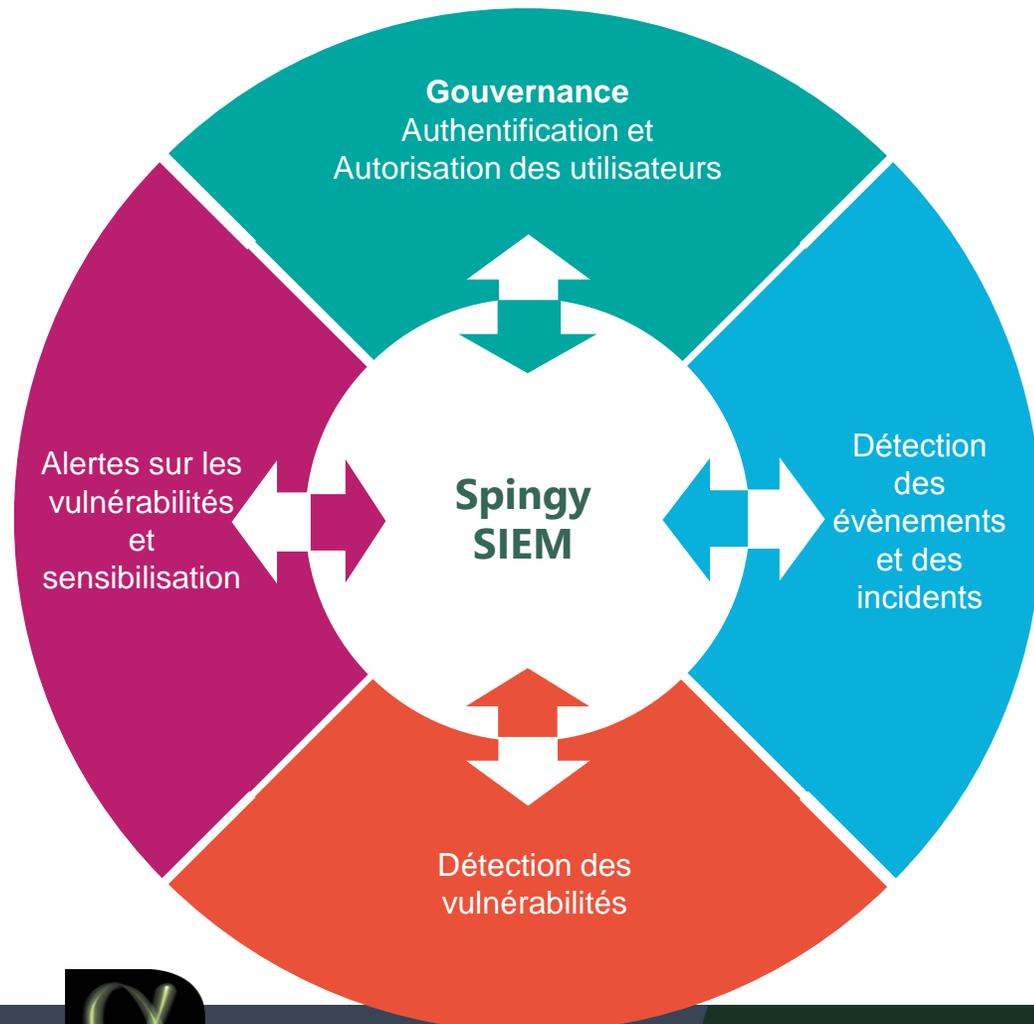


Notre plateforme de services à destination des CERT / CSIRT



- 1 Une plateforme permettant d'orchestrer et d'animer la relation entre le CERT National de l'ANSI et les différents partenaires de la stratégie nationale de Cyber Défense
- 2 Un outil qui permet la mise en œuvre d'une stratégie sur 3 axes :
 1. **La résilience** : permettant de manager la qualité de service et l'amélioration continue
 2. **La réaction rapide** : partagée et collaborative
 3. **L'anticipation** : pour une gestion intelligente et proactive des risques
- 3 Une technologie ouverte qui laisse une totale indépendance aux différents partenaires
- 4 Une philosophie de co-construction itérative de la stratégie en mode agile

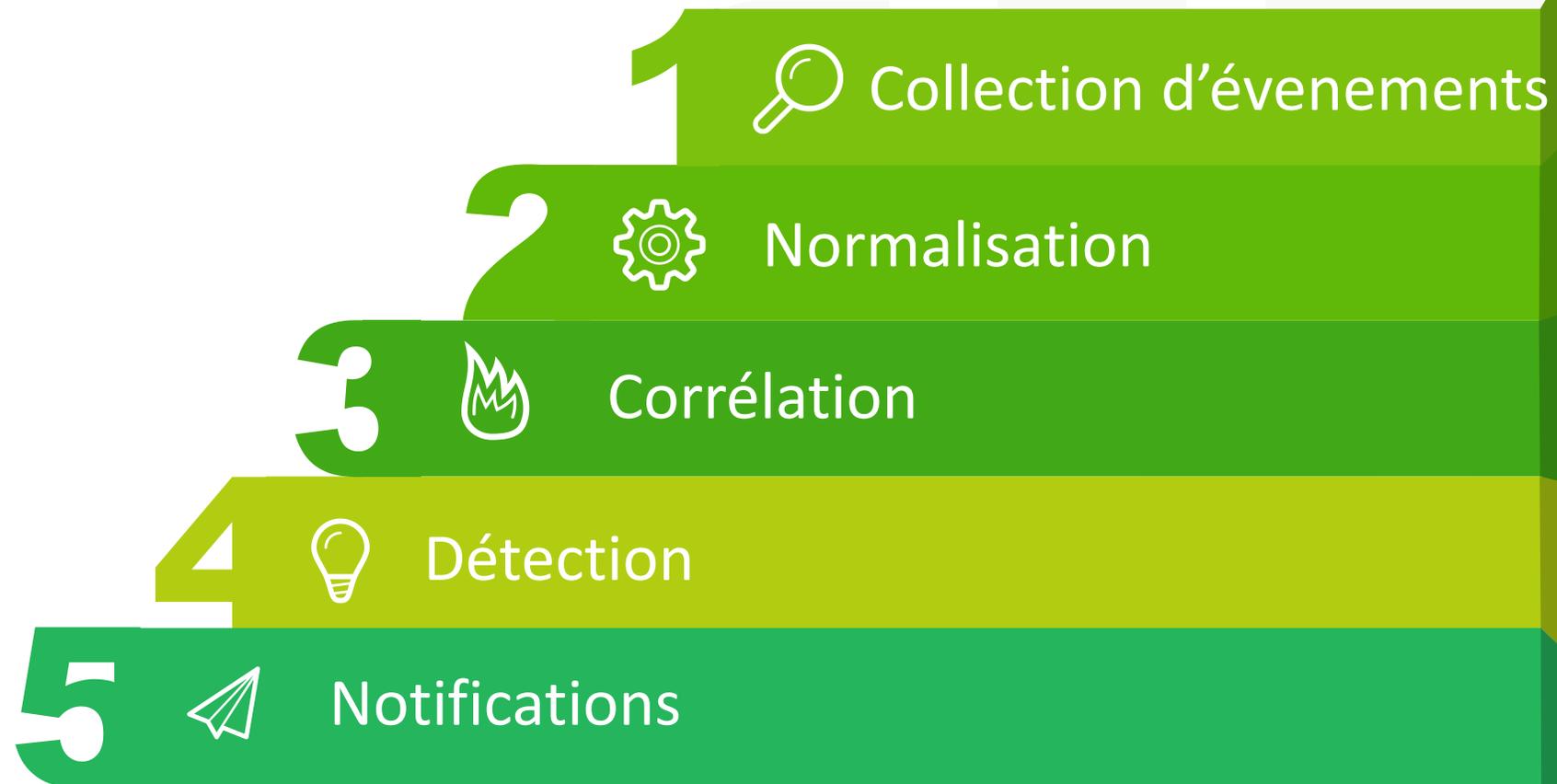
Notre plateforme de services à destination des CERT / CSIRT



7 Modules Clés

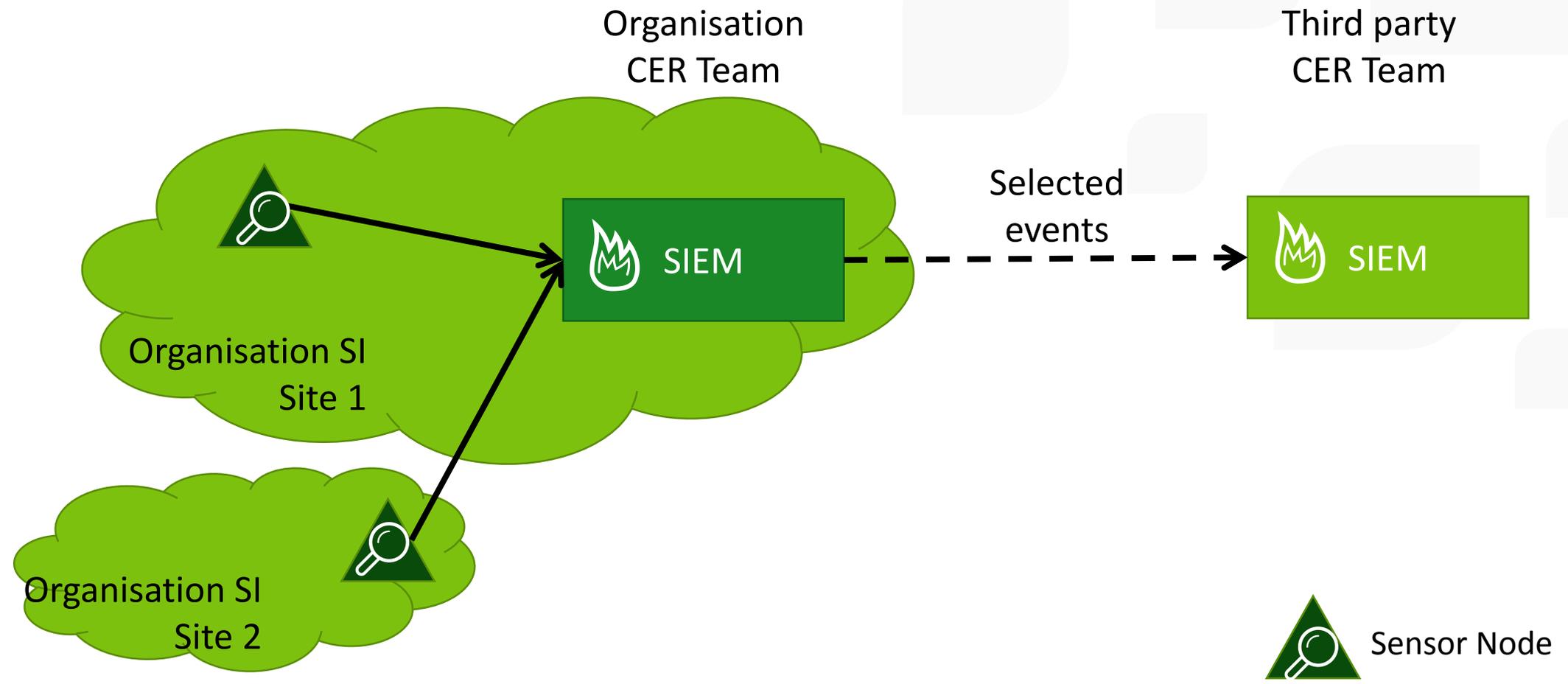
1. **Module Configuration**
2. **Module Dashboard**
3. **Module Evènements et Incidents**
4. **Module Détection de vulnérabilités**
5. **Module Alertes sur les vulnérabilités**
6. **Module Newsletters**
7. **Module Support**

Etapes clefs d'une solution SIEM



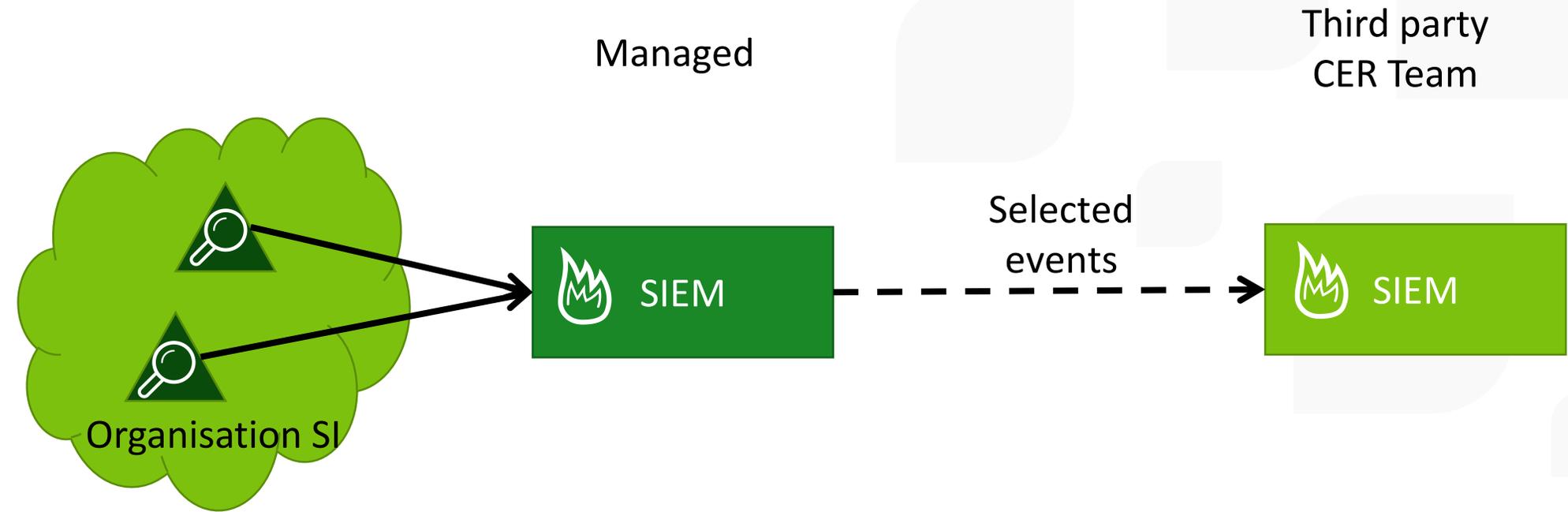
Modèles de déploiement

ON SITE / ON PREM – Multi site enabled



Modèles de déploiement

Managed SIEM



 Sensor Node

Architecture de la solution SIEM

APP WEB



Sonata Project



mongoDB



Col / Corr.



logstash



elasticsearch

Sensors



OpenVAS
Open Vulnerability Assessment System



arachni
web application security scanner framework



NMAP



Extra Sensor



4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

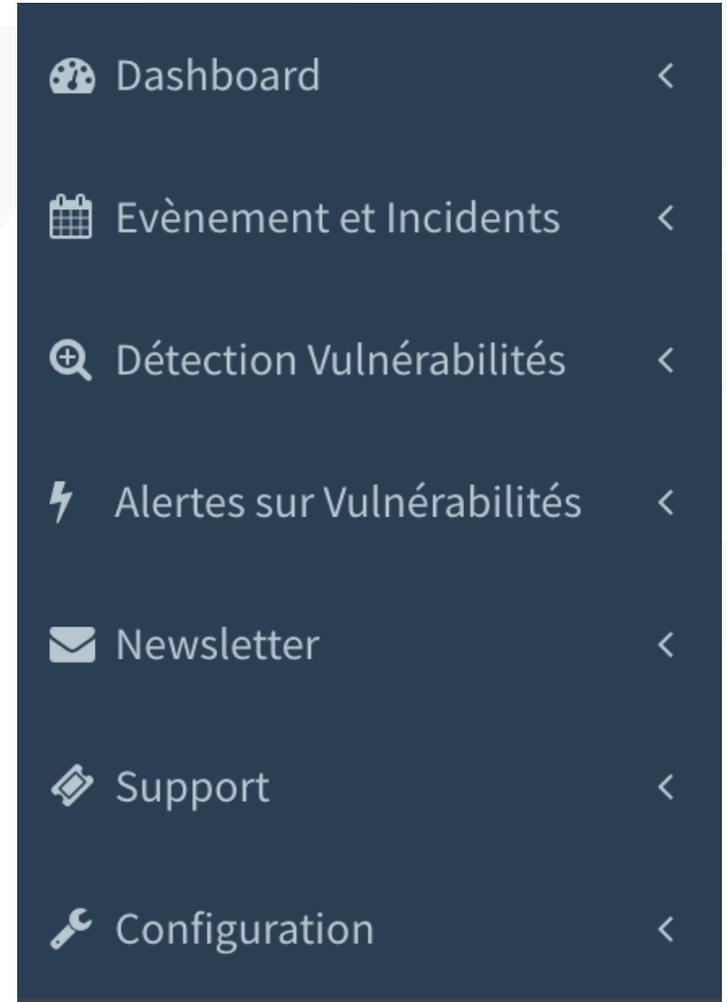
Support 07

04 Détection de vulnérabilités



Organisation

- Solution organisée en forme de modules.
- Chaque module correspond à une entrée du menu principal.



Module Configuration

- Définition du périmètre
 - Identifier les Actifs et services associés
 - Leur affecter des TAG
- Gestion des Roles
 - Ensemble de privilèges fins (créer newsletter / valider newsletter)
- Gestion des Utilisateurs

1. Module Configuration : Description

Rechercher

- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités
- Newsletter
- Support

- Configuration**
 - Récap
 - Utilisateurs
 - Groupes
 - Escalades
 - Actifs
 - Corrélation
 - Collecteurs
 - Notifications
 - Elastic

Filtres Ajouter

<input type="checkbox"/>	Nom d'utilisateur	Adresse email	Groupes	Activé	Verrouillé	Créé le	Opérations
<input type="checkbox"/>	root	khalil.chtara@alpha-engineering.net	super_admins	oui	non	1 mars 2017 03:07:12	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	admin@ansi	ansi@ansi.tn	super_admins	oui	non	28 févr. 2017 18:43:01	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	wassim	wassim.youssef@alpha-engineering.net	group1 , group2	oui	non	1 mars 2017 10:10:05	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest1	usertest1@alpha.net	group3	non	oui	23 mars 2017 11:23:35	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest2	usertest1@alpha-engineering.net	group4 , group5	non	oui	23 mars 2017 14:28:14	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest3	usertest3@gmail.com	group2 , group5	oui	non	23 mars 2017 14:30:16	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest4	usertest4@gmail.com	group3	oui	non	23 mars 2017 14:32:40	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest5	usertest5@alpha-engineering.net	group3	oui	non	23 mars 2017 14:33:19	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest6	usertest6@alpha.net	group3	non	non	23 mars 2017 14:40:58	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	usertest7	usertest7@alpha.net	group1	non	oui	24 mars 2017 17:12:26	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	khalil	admin6@alpha.net	group3	oui	non	14 juin 2017 12:38:54	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>
<input type="checkbox"/>	jasma	asma@alpha.net	group3	oui	non	16 juin 2017 02:16:18	<input type="button" value="i"/> <input type="button" value="pencil"/> <input type="button" value="trash"/>

Tous les éléments (12)

- 1 / 1 - 12 résultats - Par page 32

Le module « configuration » comporte

- Gestion des utilisateurs et des groupes
- Gestion des actifs
- Durée d'archivage des logs
- Politique d'escalade
- Logique de corrélation
- Collecteurs

1. Module Configuration : Groupes

Rechercher

- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités
- Newsletter
- Support
- Configuration**
 - » Récap
 - » Utilisateurs
 - » **Groupes**
 - » Escalades
 - » Actifs
 - » Corrélation
 - » Collecteurs
 - » Notifications
 - » Elastic

<input type="checkbox"/>	Nom	Rôles	Opérations
<input type="checkbox"/>	group1	<ul style="list-style-type: none">• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_EDIT• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_LIST• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_CREATE• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_VIEW• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_DELETE• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_EXPORT• ROLE_ADMIN_DETECTION_VULNERABILITIES_SCANS_ALL• ROLE_USER	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/>
<input type="checkbox"/>	group2	<ul style="list-style-type: none">• ROLE_ADMIN_ADRESSE_EDIT• ROLE_ADMIN_ADRESSE_LIST• ROLE_ADMIN_ADRESSE_CREATE• ROLE_ADMIN_ADRESSE_VIEW• ROLE_ADMIN_ADRESSE_DELETE• ROLE_ADMIN_ADRESSE_ALL• ROLE_USER	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/>
<input type="checkbox"/>	group3	<ul style="list-style-type: none">• ROLE_ADMIN_CONFIGURATION_ACTIFS_DETECTION_AUTOMATIQUE_EDIT• ROLE_ADMIN_CONFIGURATION_ACTIFS_DETECTION_AUTOMATIQUE_LIST• ROLE_ADMIN_CONFIGURATION_ACTIFS_DETECTION_AUTOMATIQUE_CREATE• ROLE_ADMIN_CONFIGURATION_ACTIFS_DETECTION_AUTOMATIQUE_VIEW• ROLE_ADMIN_CONFIGURATION_ACTIFS_DETECTION_AUTOMATIQUE_DELETE• ROLE_ADMIN_CONFIGURATION_ACTIFS_DETECTION_AUTOMATIQUE_ALL• ROLE_USER	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/>

- Un groupe permet de rassembler un ensemble de privilèges fins et d'associer ce groupe à un utilisateur (menu utilisateur)

- Les privilèges sont en forme de nom technique significatifs

Prefix_Module_Permission

1. Module Configuration : Actifs

Rechercher

Dashboard <

Evènement et Incidents <

Détection Vulnérabilités <

Alertes sur Vulnérabilités <

Newsletter <

Support <

Configuration <

- » Récap
- » Utilisateurs
- » Groupes
- » Escalades
- » **Actifs**
- » Corrélation
- » Collecteurs
- » Notifications
- » Elastic

ANSI SIEM @ Alpha Engineering

Gestion des Actifs

Détection automatique

Importation d'inventaire

Filtres

Ajouter

	Id	Nom	Adresse Mac	Adresse Ip	Date de découverte	Date du dernier scan	Opérations
<input type="checkbox"/>	142	khalil	00:30:67:EB:A6:7A	192.168.160.16	12 juin 2017 16:06:57	21 juin 2017 15:32:46	    
<input type="checkbox"/>	144		00:30:67:E3:38:DB	192.168.160.333	12 juin 2017 16:07:02	15 juin 2017 17:20:59	    
<input type="checkbox"/>	145		44:8A:5B:A4:17:A9	192.168.160.41	12 juin 2017 16:07:02	21 juin 2017 15:32:46	    
<input type="checkbox"/>	146		D8:5D:4C:C6:73:C8	192.168.160.45	12 juin 2017 16:07:02	21 juin 2017 15:32:46	    
<input type="checkbox"/>	147		90:F6:52:83:34:10	192.168.160.48	12 juin 2017 16:07:02	21 juin 2017 15:32:46	    
<input type="checkbox"/>	148		60:6D:C7:66:1E:DB	192.168.160.49	12 juin 2017 16:07:02	21 juin 2017 15:32:46	    
<input type="checkbox"/>	149		98:01:A7:D6:48:AD	192.168.160.50	12 juin 2017 16:07:03	14 juin 2017 12:54:51	    
<input type="checkbox"/>	150		3C:A0:67:1C:EB:5D	192.168.160.51	12 juin 2017 16:07:03	21 juin 2017 15:32:47	    
<input type="checkbox"/>	151		3C:A0:67:20:0D:43	192.168.160.59	12 juin 2017 16:07:03	21 juin 2017 15:32:47	    
<input type="checkbox"/>	152		44:8A:5B:A3:F4:70	192.168.160.67	12 juin 2017 16:07:03	21 juin 2017 15:32:47	    
<input type="checkbox"/>	153		60:6D:C7:66:88:6F	192.168.160.68	12 juin 2017 16:07:03	14 juin 2017 12:54:53	    
<input type="checkbox"/>	154		60:6D:C7:66:4D:5D	192.168.160.70	12 juin 2017 16:07:03	21 juin 2017 15:32:47	    
<input type="checkbox"/>	155		44:8A:5B:A4:17:B6	192.168.160.71	12 juin 2017 16:07:03	21 juin 2017 15:32:47	    
<input type="checkbox"/>	156		D8:5D:4C:C6:6F:2B	192.168.160.87	12 juin 2017 16:07:03	15 juin 2017 17:21:03	    
<input type="checkbox"/>	157		44:8A:5B:A4:17:A8	192.168.160.97	12 juin 2017 16:07:03	21 juin 2017 15:32:48	    
<input type="checkbox"/>	158		00:0C:29:70:EF:02	192.168.160.152	12 juin 2017 16:07:03	21 juin 2017 16:04:42	    

- Les actifs sont identifiés suite à un scan du réseau ou a un ajout manuel
- On peut associer un nom (tag) à un actif
- On peut importer un inventaire d'actifs
- Fonctions de filtrage avancés pour la recherche d'actifs

23

1. Module Configuration : Notifications

- Rechercher
- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités
- Newsletter
- Support
- Configuration**
 - Récap
 - Utilisateurs
 - Groupes
 - Escalades
 - Actifs
 - Corrélation
 - Collecteurs
 - Notifications
 - Elastic

<input type="checkbox"/>	Module	Message		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est arrêté.		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est redémarré et il est en cours d'exécution.		
<input type="checkbox"/>	Configuration	Le scan profond3 est arrêté et il reste en pause.		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est démarré et en cours de découvrir le cible		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est redémarré et il est en cours d'exécution.		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est arrêté.		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est redémarré et il est en cours d'exécution.		
<input type="checkbox"/>	Configuration	Le scan profond3 est arrêté et il reste en pause.		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est redémarré et il est en cours d'exécution.		
<input type="checkbox"/>	Configuration	Le scan profond3 est arrêté et il reste en pause.		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est démarré et en cours de découvrir le cible		
<input type="checkbox"/>	Configuration	Le scan << profond3 >> est redémarré et il est en cours d'exécution.		
<input type="checkbox"/>	Configuration	Le scan << profond2 >> est arrêté.		
<input type="checkbox"/>	Configuration	Le scan << profond2 >> est démarré et en cours de découvrir le cible		
<input type="checkbox"/>	Configuration	Le scan << profond2 >> est arrêté.		
<input type="checkbox"/>	Configuration	Le scan << profond2 >> est redémarré et en cours de découvrir le cible		
<input type="checkbox"/>	Configuration	Le scan profond2 est arrêté et il reste en pause.		
<input type="checkbox"/>	Configuration	Le scan << profond2 >> est redémarré et en cours de découvrir le cible		
<input type="checkbox"/>	Configuration	Le scan profond2 est arrêté et il reste en pause.		

Vous avez 1440 notifications

- Le scan << profond3 >> est arrêté. : 2017-06-22 13:02:51
- Le scan << profond3 >> est redémarré et il est en cours d'exécution. : 2017-06-22 13:02:43

Voir tout

- Permet de lister les différentes notifications affichées à l'utilisateur

4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07



2. Module Dashboard : Description



2. Module Dashboard : Modification de la disposition

Rechercher

- Dashboard <
- » Tableau de board
- » Modifier la disposition
- Evènement et Incidents <
- Détection Vulnérabilités <
- Alertes sur Vulnérabilités <
- Newsletter <
- Support <
- Configuration <

ANSI SIEM @ Alpha Engineering

La liste des vulnérabilité détecté	Enabled
Les ports les plus touchés par les vulnérabilités	Enabled
Niveau Alerte	Enabled
Tickets ouverts	Enabled
Envoi des Newsletters	Enabled

La liste des actifs avec le plus de vulnérabilités	Enabled
Top 5 Evenements	Enabled
Top des destinataires des Newsletters	Enabled
Pourcentage de degré des vulnérabilités détectées	Enabled
Nombre des newsletters envoyées par mois	Enabled

Le module « Dashbord » affiche un tableau de bord global et permet à l'utilisateur de personnaliser l'ordre et les dashboards affichés

✓ Sauvegarder

4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07



3. Module Evènement et Incidents : Présentation

Rechercher

Dashboard <

Evènement et Incidents <

- Alertes
- Evènements
- Incidents
- Rapport

Détection Vulnérabilités <

Alertes sur Vulnérabilités <

Newsletter <

Support <

Configuration <

ANSI SIEM @ Alpha Engineering

Filtres ▾ Ajouter

<input type="checkbox"/>	ID ▾	Date de définition	Méthode	Détails	Niveau de risque	Source	Destination	Opérations
<input type="checkbox"/>	1	14 juin 2017 18:49:33	fdgfdg	sfgvdv	2	48.115.151.51	159.59.59.59	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	2	22 juin 2017 17:19:30	szszs	zszszs	22	112.255.58.44	58.54.87.48	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	3	22 juin 2017 17:19:46	yuik	fdgvdbvsxsxsx	222	222.98.95.89	59.59.59.59	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Tous les éléments (3) Supprimer ▾

- 1 / 1 - 3 résultats - Par page 32 ▾

Le module « Evènements et Incidents » contient les sous modules :

- **Alertes** : Gérer et visualiser l'ensemble des alertes déclenchées relativement au périmètre supervisé par la plateforme.
- **Evènements** : Gérer et visualiser l'ensemble des évènements déclenchés.
- **Incidents** : Gérer et visualiser l'ensemble des incidents déclenchés.
- **Rapport** : Créer des rapports sur les alertes, évènements et incidents.

3. Module Evènement et Incidents : Présentation

- Rechercher
 - Dashboard
 - Evènement et Incidents**
 - Alertes
 - Evènements
 - Incidents
 - Rapport
 - Détection Vulnérabilités
 - Alertes sur Vulnérabilités
 - Newsletter
 - Support
 - Configuration
- ANSI SIEM @ Alpha Engineering

Filtres Ajouter

<input type="checkbox"/>	ID	Date de définition	Méthode	Détails	Niveau de risque	Source	Destination	Opérations
<input type="checkbox"/>	1	14 juin 2017 18:49:33	fdgfdg	sfgvdv	2	48.115.151.51	159.59.59.59	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	2	22 juin 2017 17:19:30	szszs	zszszs	22	112.255.58.44	58.54.87.48	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	3	22 juin 2017 17:19:46	yuik	fdgvdbvsxsxsx	222	222.98.95.89	59.59.59.59	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Tous les éléments (3) Supprimer OK

Export - 1 / 1 - 3 résultats - Par page 32

Ouverture possible de tickets par rapport à des Evt / Alertes

Le ticket peut être a destination du CERT local / CERT tier (paramètre de configuration)

Permet d'envoyer donc des informations précises à un autre tier

3. Module Evènement et Incidents : Présentation

- Rechercher
 - Dashboard
 - Evènement et Incidents**
 - Alertes
 - Evènements
 - Incidents
 - Rapport
 - Détection Vulnérabilités
 - Alertes sur Vulnérabilités
 - Newsletter
 - Support
 - Configuration
- ANSI SIEM @ Alpha Engineering

Filtres Ajouter

<input type="checkbox"/>	ID	Date de définition	Méthode	Détails	Niveau de risque	Source	Destination	Opérations
<input type="checkbox"/>	1	14 juin 2017 18:49:33	fdgfdg	sfgvdv	2	48.115.151.51	159.59.59.59	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	2	22 juin 2017 17:19:30	szszs	zszszszs	22	112.255.58.44	58.54.87.48	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	3	22 juin 2017 17:19:46	yuik	fdgvdbvsxsxsx	222	222.98.95.89	59.59.59.59	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Tous les éléments (3) Supprimer OK

Export - 1 / 1 - 3 résultats - Par page 32

Configuration et gestion des règles de corrélation

4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07



<input type="checkbox"/>	Id	Nom de Scan	Date de démarrage	Fin de Scan	Temps de Scan	Actifs	Vulnérabilités	Statut	Opérations
<input type="checkbox"/>	7	scan-test	15 juin 2017 16:19:05	15 juin 2017 16:41:15	00:22:10	2	8	Terminé	    
<input type="checkbox"/>	9	openvas	15 juin 2017 16:26:04					En cours	     

Tous les éléments (2) Supprimer

Export - 1 / 1 - 2 résultats - Par page 32

Le module « Détection des vulnérabilités » est composé par les sous modules :

- **Planificateur de scan des vulnérabilités** : Eviter impact sur le système en cours d'audit
- **Rapports** : La génération de rapports se base sur :
 - * Les informations déjà collectées au niveau du module
 - * Des bloc, à inclure au choix, contenant des sous ensemble de ces informations (tableaux / graphiques)
 - * Il est possible de personnaliser le rapport en fonction du choix des blocs d'informations à inclure.

4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07



Rechercher

- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités**
- » Gestion des Vulnérabilités
- » Liste des CVEs
- » Rapport
- Newsletter
- Support
- Configuration

Filtres Ajouter

<input type="checkbox"/>	Famille de Menace	Sévérité	Risque	CVE-ID	CPE-ID	Date de définition	Opérations
<input type="checkbox"/>	SMBv1 Unspecified Remote Code Execution (Shadow Brokers)	10	High	NOCVE	--	28 févr. 2017 15:31:26	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	DCE Services Enumeration Reporting	5	Medium	NOCVE	--	28 févr. 2017 15:31:23	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	TCP timestamps	3	Low	NOCVE	--	28 févr. 2017 15:30:19	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	ICMP Timestamp Detection	0	Log	CVE-1999-0524	--	28 févr. 2017 15:30:19	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	OS Detection Consolidation and Reporting	0	Log	NOCVE	--	28 févr. 2017 15:30:49	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	Traceroute	0	Log	NOCVE	--	28 févr. 2017 15:32:55	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	CPE Inventory	0	Log	NOCVE	--	28 févr. 2017 15:32:55	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	DCE Services Enumeration	0	Log	NOCVE	--	28 févr. 2017 15:30:27	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SMB/CIFS Server Detection	0	Log	NOCVE	--	28 févr. 2017 15:30:28	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SMB Native LanMan	0	Log	NOCVE	--	28 févr. 2017 15:30:28	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SMB/CIFS Server Enumeration	0	Log	NOCVE	--	28 févr. 2017 15:30:28	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SMB Remote Vulnerability Detection	0	Log	NOCVE	--	28 févr. 2017 15:31:22	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SMB Test with 'smbexec'	0	Log	NOCVE	--	28 févr. 2017 15:31:38	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SSH Protocol Versions Supported	0	Log	NOCVE	--	15 juin 2017 14:27:43	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	SSH Server type and version	0	Log	NOCVE	--	15 juin 2017 14:25:53	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>
<input type="checkbox"/>	Services	0	Log	NOCVE	--	15 juin 2017 14:25:41	<input type="info"/> <input type="edit"/> <input type="delete"/> <input type="refresh"/>

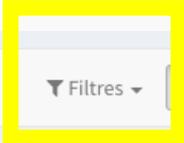
Le module « Alerte sur les vulnérabilités » est composé par les sous modules :

- **Gestion des Vulnérabilités** : Gérer les vulnérabilités détectées depuis les scans
- **Liste des CVEs** : Lister les vulnérabilités (mise à jour automatique de la liste CVE et identification des actifs concernés)
- **Rapports**

5. Module Alertes sur les vulnérabilités : Liste CVE

- Rechercher
- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités**
 - Gestion des Vulnérabilités
 - Liste des CVEs
 - Rapport
- Newsletter
- Support
- Configuration

	id	cvss	Summary	Published	Modified
<input type="checkbox"/>	CVE-1999-0001	5	ip_input.c in BSD-derived TCP/IP implementations allows remote attackers to cause a denial of service (crash or hang) via crafted packets.	1999-Dec-30 01:00:00	2010-Dec-16 01:00:00
<input type="checkbox"/>	CVE-1999-0002	10	Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.	1998-Oct-12 02:00:00	2009-Jan-26 01:00:00
<input type="checkbox"/>	CVE-1999-0003	10	Execute commands as root via buffer overflow in Tooltalk database server (rpc.ttdbserverd).	1998-Apr-01 02:00:00	2008-Sep-09 10:33:31
<input type="checkbox"/>	CVE-1999-0004	5	Denial of Service vulnerability in BIND 8 Releases via maliciously formatted DNS messages.	1998-Apr-08 02:00:00	2008-Sep-09 10:33:31
<input type="checkbox"/>	CVE-1999-0005	10	Buffer overflow in POP servers based on BSD/Qualcomm's qpopper allows remote attackers to gain root access using a long PASS command.	1998-Jul-20 02:00:00	2008-Sep-09 10:33:31
<input type="checkbox"/>	CVE-1999-0006	10	Buffer overflow in NIS+, in Sun's rpc.nisd program.	1998-Jun-26 02:00:00	2008-Sep-09 10:33:31
<input type="checkbox"/>	CVE-1999-0007	5	Information from SSL-encrypted sessions via PKCS #1.	1998-Jun-26 02:00:00	2008-Sep-09 10:33:31
<input type="checkbox"/>	CVE-1999-0008	10	Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.	1998-Oct-12 02:00:00	2009-Jan-26 01:00:00
<input type="checkbox"/>	CVE-1999-0009	10	Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.	1998-Apr-08 02:00:00	2008-Sep-09 10:33:31
<input type="checkbox"/>	CVE-1999-0010	5	Denial of Service vulnerability in BIND 8 Releases via maliciously formatted DNS messages.	1998-Apr-08 02:00:00	2008-Sep-09 10:33:31



La solution permet de rechercher dans une copie locale, maintenue à jour, des listes de vulnérabilités

Des filtres avancés permettent de rechercher dans la liste des vulnérabilités

4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07



6. Module Newsletter : Présentation

- Rechercher
- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités
- Newsletter**
- Newsletters
- Destinataires
- Templates
- Support
- Configuration

	Id	Nom	Date de création	Dernier envoi à	Utilisateurs	Groupes	Activé	Opérations
<input type="checkbox"/>	2	Newsletter ICMP Timestamp Detection	13 avr. 2017 18:08:08	17 avr. 2017 18:58:29	test1 test1	Alpha Meca , Alpha Tel	non	    
<input type="checkbox"/>	3	Newsletter ICMP Timestamp	13 avr. 2017 18:10:07	17 avr. 2017 19:03:54	test2 test2	Alpha Meca	non	    
<input type="checkbox"/>	8	Newsletter XSS Informations	17 avr. 2017 14:50:34	17 avr. 2017 20:07:02	khalil chtara , aziz sfaxi , khalil gmail		non	    
<input type="checkbox"/>	9	Newsletter traceroute	17 avr. 2017 16:54:26	17 avr. 2017 20:44:46		AlphaIT	non	    
<input type="checkbox"/>	10	Newsletter CPE	17 avr. 2017 16:56:26	20 avr. 2017 20:10:58	khalil chtara	AlphaIT	non	    
<input type="checkbox"/>	11	Dernières vulnérabilités	22 juin 2017 17:16:05		khalil chtara		non	    
<input type="checkbox"/>	12	Dernières Alertes	22 juin 2017 17:16:05		khalil chtara		non	    

Tous les éléments (7) Supprimer

Export - 1/1 - 7 résultats - Par page 32

Permettre l'envoi de newsletter de sensibilisation à des destinataires organisés en groupes

L'envoi se base sur des templates pré-préparées

Ajout de newsletter contenant le résultat de scan suite a la recommandation du comité de pilotage

Etapes de exploitation du module

1

Création
d'un modèle
(Template)

Peut contenir
jusqu'à 10 clefs
(Key) permettant
de personnaliser
le contenu de la
newsletter

2

Création
newsletter
basée sur une
Template

Donner une valeur
aux clefs préparées
dans le template

3

Sélection des
destinataires /
groupes de
destinataires

Rubrique spécifique
pour la gestion des
destinataires

4

Envoi /
Envoi planifié

Si la newsletter
est active
(validée)

Rechercher



Dashboard <

Evènement et Incidents <

Détection Vulnérabilités <

Alertes sur Vulnérabilités <

 Newsletter <

- >> Newsletters
- >> Destinataires
- >> Templates

Support <

Configuration <

ANSI SIEM @ Alpha Engineering

Templates

Filtres

Ajouter

<input type="checkbox"/>	Id	Nom	Description	Date de création	Dernière modification	Opérations
<input type="checkbox"/>	2	Template ICMP Timestamp	Ce Template décrit la vulnérabilité ICMP Timestamp	11 avr. 2017 05:17:14	20 avr. 2017 11:48:20	
<input type="checkbox"/>	5	Template Scan	Ce template représente la liste des vulnerabilites	11 avr. 2017 05:17:14	20 avr. 2017 11:48:33	
<input type="checkbox"/>	6	Template T...	Ce template décrit la vulnérabilité de toute	11 avr. 2017 05:17:14	20 avr. 2017 11:48:36	
<input type="checkbox"/>	7	Templac...	Ce template contient des informations sur la vulnérabilité	11 avr. 2017 05:17:14	20 avr. 2017 11:48:39	
<input type="checkbox"/>	8	Standard Template	Exemple d'un template standard	25 avr. 2017 19:07:44	25 avr. 2017 19:07:44	
<input type="checkbox"/>	Tous les éléments (5)					Export - 1 / 1 - 5 résultats - Par page 32

Liste des template de newsletter

Notion de newsletter active / non active

Pas de double envoi pour une newsletter (ne pas spammer le destinataire)

4

Visite guidée

01 Configuration

02 Tableau de Bord

03 Evènement et Incidents

04 Détection de vulnérabilités

Alertes sur Vulnérabilités 05

Newsletter 06

Support 07



Rechercher

- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités
- Newsletter
- Support**
 - » Tickets
 - » Catégories
- Configuration

ANSI SIEM @ Alpha Engineering

Filtres Ajouter

<input type="checkbox"/>	Id	Sujet	Créer par	Assigné à	Assigné au groupe	Créé à	Catégorie	Statut	Priorité	Opérations
<input type="checkbox"/>	1	Demande de clarification	root	admin@ansi		15 juin 2017 22:32:11	Helpdesk	Nouveau	Haute	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/> <input type="button" value="↶"/>
<input type="checkbox"/>	2	Incident inconnu !	root	admin@ansi		15 juin 2017 22:34:29	Software	Nouveau	Très basse	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/> <input type="button" value="↶"/>
<input type="checkbox"/>	3	Problème non identifié	root		group3	16 juin 2017 02:14:14	Software	Nouveau	Moyenne	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/> <input type="button" value="↶"/>
<input type="checkbox"/>	4	Identification du port	root		group1	16 juin 2017 02:25:01	Helpdesk	Nouveau	Haute	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/> <input type="button" value="↶"/>
<input type="checkbox"/>	5	Pas de problème !!	root		group3	16 juin 2017 02:25:34	Personnel	Fermer	Très haute	<input type="button" value="i"/> <input type="button" value="✎"/> <input type="button" value="🗑"/> <input type="button" value="↶"/>

Tous les éléments (5) - 1 / 1 - 5 résultats - Par page 32

Le module « Support » est composé par les sous modules :

- **Gestion des Tickets**

Créer des tickets en sélectionnant des vulnérabilités / alertes
Gestion des commentaires sur les tickets

- **Gestion des catégories**

En accords avec les actifs / métier

7. Module Support : Présentation

Rechercher

- Dashboard
- Evènement et Incidents
- Détection Vulnérabilités
- Alertes sur Vulnérabilités
- Newsletter
- Support**
 - Tickets
 - Catégories
- Configuration

Filtres Ajouter

<input type="checkbox"/>	Id	Sujet	Créer par	Assigné à	Assigné au groupe	Créé à	Catégorie	Statut	Priorité	Opérations
<input type="checkbox"/>	1	Demande de clarification	root	admin@ansi		15 juin 2017 22:32:11	Helpdesk	Nouveau	Haute	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	2	Incident inconnu !	root	admin@ansi		15 juin 2017 22:34:29	Software	Nouveau	Très basse	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	3	Problème non identifié	root		group3	16 juin 2017 02:14:14	Software	Nouveau	Moyenne	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	4	Identification du port	root		group1	16 juin 2017 02:25:01	Helpdesk	Nouveau	Haute	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	5	Pas de problème !!	root		group3	16 juin 2017 02:25:34	Personnel	Fermer	Très haute	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Tous les éléments (5) Supprimer

Export - 1 / 1 - 5 résultats - Par page 32

Pour chaque alerte détectée, l'utilisateur peut ouvrir un ticket afin de communiquer l'information vers les groupes de support sur cette alerte.



TEAM WORK | WORK HARD

La clé de toute réussite

1

À propos de nous

2

Métier et sécurité

3

Solution SIEM

4

Visite guidée

5

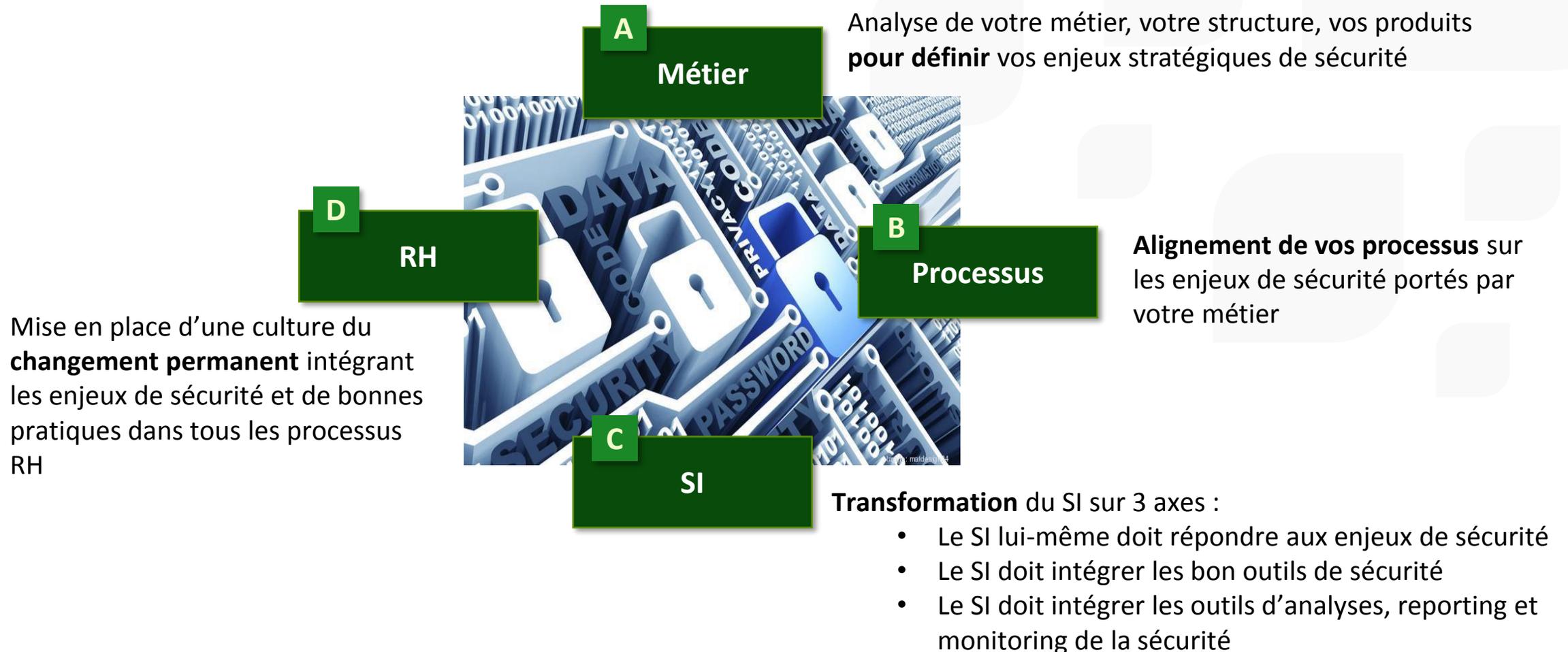
Démo

6

Next Step



■ Vision : des missions d'analyse des stratégies de sécurité qui passe par un cercle vertueux du changement



Architecture de la solution SIEM

Int. Artificielle

Approches IA et ML pour faire face aux nouvelles menaces



Accompagnement Métier

Adaptation des outils aux besoins spécifiques du métier

Streaming

Traitement des infos à la volée



ROSI

Indicateurs sur le retour d'investissement de sécurité

Big Data

Supporter un grand volume d'événements



Processus métiers spécifiques aux CERT

Collaboration entre CERT

Sensors



 *Say hello to*

enginov



- **enginov** une organisation innovante basée sur des communautés interconnectées:

