UNIVERSITÉ DE LORRAINE | LORRAINE INP
les talents se lèvent à l'Est

Sécurité et Analyse des Risques

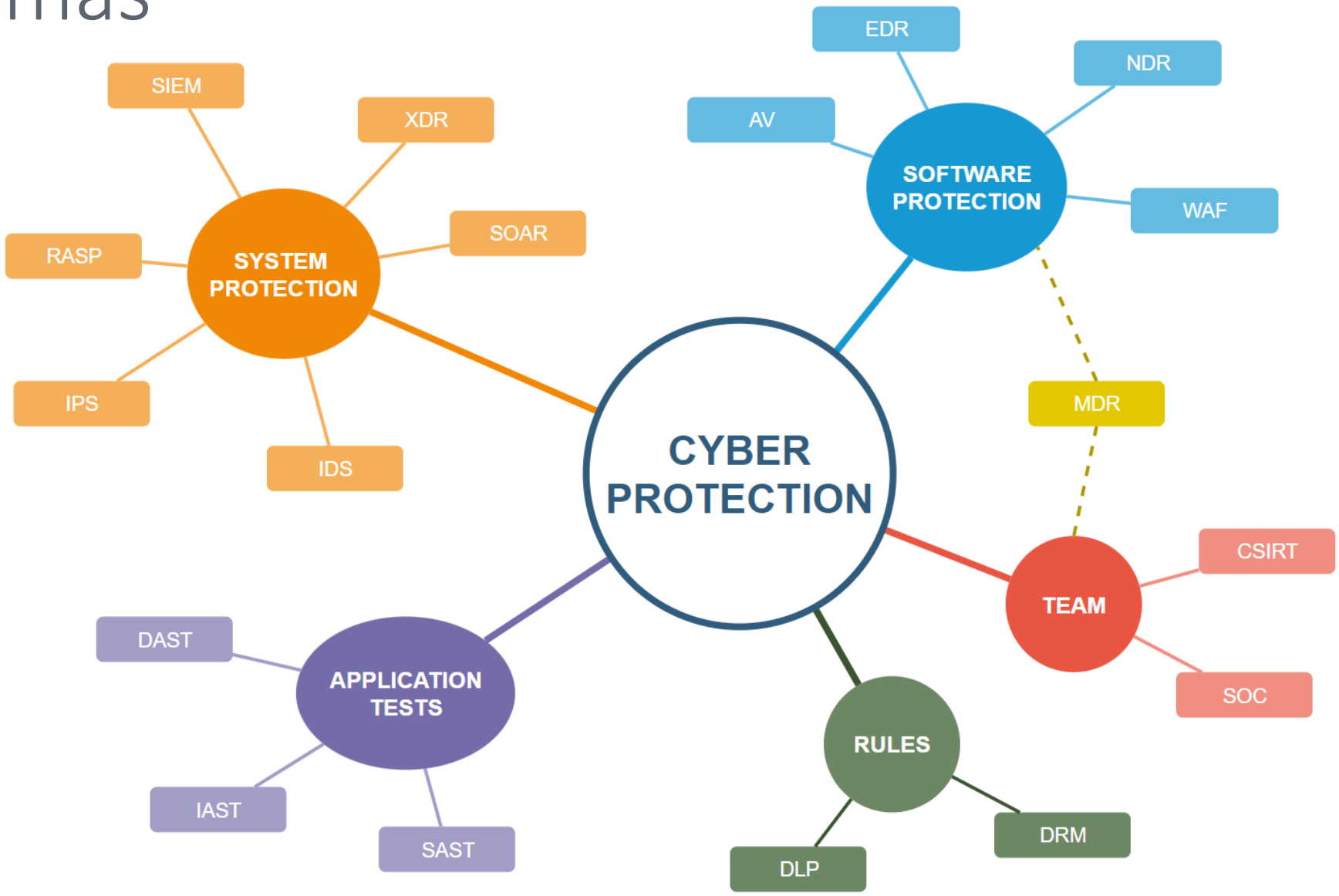
Juliette BLUEM – Guillaume TISSERAND – Arthur TERRIEN

POLYTECH NANCY

Acronymes

- AV : Antivirus
- WAF : web application firewall
- EDR : Endpoint Detection and Response
- SOAR : Security Orchestration, Automation and Response
- DLP : Data Loss Prevention
- DRM : Digital Rights Management
- SOC : Security Operations Center
- DAST : Dynamic Application Security Testing
- IAST : Interactive Application Security Testing
- NDR : Network Detection Response
- MDR : Managment Detection Response
- XDR : Extended Detection Response
- CSIRT : Computer Security Incident Response Team
- IPS : Intrusion Prevention System
- SIEM : Security Information & Event Management
- RASP : Runtime Application Self-Protection
- SAST : Static Application Security Testing
- IDS : Intrusion Detection System

Schémas


CYBER PROTECTION
SYSTEM PROTECTION
SIEM
XDR
SOAR
RASP
IPS
IDS
SOFTWARE PROTECTION
EDR
NDR
AV
WAF
MDR
TEAM
CSIRT
SOC
RULES
DRM
DLP
APPLICATION TESTS
DAST
IAST
SAST

Mise en pratique

- Le **SOC** cherche à mettre en place une politique de **DLP** dans le but de prévenir les pertes d'informations et de **DRM** pour restreindre l'accès à ces dernières en fonction des utilisateurs. Cette politique s'intègre également dans le déploiement de solutions logiciels de protection tel qu'un **AV** ou un **WAF**.
- Dans certaines structures, notamment les sociétés de développement d'antivirus, pour leur propre test de produit réalisent différentes phases de test appelées **DAST**, **IAST**, **SAST** et **RASP**. Les principales différences entre toutes ces méthodes, résident dans leur secteur d'application (logiciel, surveillance de trafic, faille 0-day, action active et passive)

Mise en pratique

- En opposition avec le **SOC** qui effectue de la prévention aux attaques, le **CSIRT** agit après que l'incident se soit passé. Il permet aux sociétés d'être plus résiliente face aux cyberattaques.
- Il n'est pas exclue que le **CSIRT** effectue de la prévention, notamment en mettant en place un **XDR**, **EDR**, **MDR**, **NDR** ou encore un **IPS**, **SOAR** qui lui permettra de surveiller l'infrastructure d'une société après son rétablissement,
- A l'issue du sinistre, le **CSIRT** pourra proposer un plan d'action composé de divers éléments tels que la mise en place d'un **SIEM**, d'un **IPS** ou encore d'un **IDS** pour contrôler des règles pour l'infrastructure

AV – Définition

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatiques1 ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiants ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

WAF – Définition

Un Web Application Firewall (WAF) est un type de pare-feu qui protège le serveur d'applications Web dans le backend contre diverses attaques. Le WAF garantit que la sécurité du serveur Web n'est pas compromise en examinant les paquets de requête HTTP / HTTPS et les modèles de trafic Web.

DLP – Définition

Le terme Data Loss Prevention (DLP) fait référence à un ensemble de techniques qui permettent d'identifier, de contrôler et de protéger l'information grâce à des analyses de contenu approfondies, que l'information soit stockée, en mouvement ou traitée. L'objectif est de limiter la fuite de données sensibles, que cette dernière soit accidentelle ou intentionnelle. D'après le rapport «2013 Cost of Data Breach Study: Global Analysis» réalisé par Ponemon Institute, les fuites de données sont la cause d'actes criminels (exemple : vols de données), d'erreurs humaines et/ou de bugs dans le système.

Les termes « data loss » (perte de données) et « data leak » (fuite de données), qui sont étroitement reliées, sont souvent utilisées de manière interchangeable bien qu'ils aient un sens différent. La perte de données devient une fuite de données dans le cas où le support contenant l'information sensible aurait été perdu puis obtenu par des personnes initialement non autorisées. Une fuite de données est toutefois possible sans que ces dernières aient été perdues.

EDR – Définition

Les logiciels EDR surveillent les terminaux (ordinateurs, serveurs, tablettes, téléphones…) et non le réseau du système d'information.

Pour ce faire, ces logiciels analysent les usages faits des terminaux surveillés, notamment via l'analyse comportementale. Celle-ci permet de reconnaître des comportements déviant d'une norme, après une phase d'apprentissage. Les logiciels d'EDR sont également capables de surveiller l'exploitation de failles de sécurité.

L'avantage d'une solution EDR est de permettre à une entreprise de se protéger à la fois contre les attaques connues (ex : un virus) mais aussi inconnues, en analysant des comportements suspects.

DRM – Définition

La gestion des droits numériques (GDN)1,2 ou la gestion numérique des restrictions3, en anglais « digital rights management » (DRM), ou encore les mesures techniques de protection (MTP)4, ont pour objectif de contrôler l'utilisation qui est faite des œuvres numériques.

Ces dispositifs peuvent s'appliquer à tous types de supports numériques physiques (disques, DVD, Blu-ray, logiciels…) ou de transmission (télédiffusion, services Internet…) grâce à un système d'accès conditionnel.

Ces dispositifs techniques ou logiciels peuvent viser à :

- restreindre la lecture du support à une zone géographique prévue (par exemple les zones des DVD) ;
- restreindre la lecture du support à du matériel spécifique (par exemple les versions smartphone ou tablette) ;
- restreindre la lecture du support à un constructeur ou vendeur (afin de bloquer la concurrence) ;
- restreindre ou empêcher la copie privée du support (transfert vers un appareil externe) ;
- restreindre ou verrouiller certaines fonctions de lecture du support (désactivation de l'avance rapide sur certains passages d'un DVD). Très utile pour obliger l'exposition aux annonces publicitaires ;

- identifier et tatouer numériquement toute œuvre et tout équipement de lecture ou enregistrement (pour faciliter le pistage des copies non autorisées, mais surtout empêcher la personnalisation et donc le contrôle d'une technologie, par exemple empêcher l'installation d'un autre système d'exploitation sur un ordinateur).

Les mesures techniques exploitent un chiffrement de l'œuvre, combiné à un accès conditionnel. L'éditeur ou le distributeur qui exploite ce contrôle d'accès ne confie la clé de contrôle d'accès du produit, qu'en échange d'une preuve d'achat ou de souscription pour y accéder (abonnement à une chaîne payante, VOD, téléchargement, etc.). L'accès à la lecture (et/ou sa copie) du document ainsi protégé n'est alors autorisée que pour l'équipement ou l'identification logicielle certifiée par le fournisseur.

Les notions concernant les mesures techniques de protection existent dans le droit (DMCA aux États-Unis, EUCD en Europe, le DADVSI en France), faisant l'objet d'un accord international. La loi reconnaît l'accès conditionnel comme une mesure de protection et punit les usagers qui les contournent ou en publient les secrets.

Ces mesures technologiques provoquent cependant le débat car elles peuvent restreindre la lecture des œuvres au seul équipement certifié par le diffuseur (les dispositifs concurrents pouvant être incompatibles entre eux). Devenues des normes (pourtant commerciales et industrielles) adoptées sur le plan international par les diffuseurs, elles se révèlent parfois délicates à adapter aux spécificités du droit local, telles que par exemple la copie privée, le dépôt légal, le droit de courte citation, etc. En associant de façon obligatoire tel éditeur de produit avec tel éditeur de contenus, elles sont aussi accusées d'engendrer des situations de monopoles et de non concurrence. Autrement dit, et malgré ce que leur nom pourrait laisser entendre, les DRM sont une contrainte technique et non légale.

SOAR – Définition

Le SOAR fait référence à trois capacités logicielles clés qu'utilisent les équipes de sécurité : la gestion des cas et des workflows, l'automatisation des tâches et la centralisation de l'accès, de l'interrogation et du partage des informations sur les menaces.

Le SOAR est généralement mis en œuvre en coordination avec le centre opérationnel de sécurité d'une entreprise. Les plateformes SOAR peuvent surveiller les flux d'informations sur les menaces et déclencher des réponses automatisées afin de limiter les problèmes de sécurité.

SOC – Définition

Le SOC, pour Security Operation Center, est, comme son nom l'indique, le centre des opérations de sécurité. Plus précisément, un SOC se concentre sur la surveillance des menaces et la qualification des incidents.

Pour y parvenir, les analystes utilisent un outil, le SIEM (Security Information Management System). Le SIEM intègre des logiciels utilisés pour surveiller les infrastructures des entreprises. Les analystes y configurent un ensemble de règles de corrélation selon la politique de sécurité préconisée afin de détecter d'éventuelles menaces.

DAST – Définition

Un DAST est un processus de test non fonctionnel permettant d'évaluer une application à l'aide de certaines techniques. Le résultat final de ce processus de test couvre les faiblesses et les vulnérabilités de sécurité présentes dans une application. Ce processus de test peut être réalisé de manière manuelle ou à l'aide d'outils automatisés. L'évaluation manuelle d'une application implique une intervention humaine plus importante pour identifier les failles de sécurité qui pourraient échapper à un outil automatisé. En général, les erreurs de logique métier, les vérifications de conditions de course et certaines vulnérabilités de type "zero day" ne peuvent être identifiées qu'à l'aide d'évaluations manuelles.

D'autre part, un outil DAST est un programme qui communique avec une application web par le biais du frontal web afin d'identifier les vulnérabilités de sécurité potentielles de l'application web et les faiblesses architecturales. Il effectue un test en boîte noire. Contrairement aux outils de test de sécurité des applications statiques, les outils DAST n'ont pas accès au code source et détectent donc les vulnérabilités en effectuant réellement des attaques. Les outils DAST permettent des analyses sophistiquées, détectant les vulnérabilités avec un minimum d'interactions avec l'utilisateur une fois configurés avec le nom de l'hôte, les paramètres d'exploration et les informations d'authentification. Ces outils tenteront de détecter les vulnérabilités dans les chaînes de requête, les en-têtes, les fragments, les verbes (GET/POST/PUT) et l'injection DOM.

MDR – Définition

L’acronyme MDR regroupe les solutions managées (gérées par un fournisseur de cybersécurité) de détection et de réponse aux incidents. Elles sont opérées par un SOC, interne ou externalisé, et permettent d’adresser de bout en bout les menaces cyber.

Grâce à l’automatisation, notamment via l’usage d’un outil d’orchestration (SOAR), un analyste peut procéder à une remédiation lorsqu’une menace est détectée et confirmée. Il est également parfaitement possible, selon le niveau de maturité en cybersécurité d’une entité, d’appliquer automatiquement la remédiation.

Ces solutions permettent une accélération du traitement des alertes.

NDR – Définition

Le NDR apporte une visibilité étendue aux équipes du SOC, à l'échelle du réseau, pour détecter le comportement d'attaquants possiblement cachés, ciblant les infrastructures physiques, virtuelles et cloud. Il apporte de la complémentarité aux outils EDR et SIEM.

L'approche du NDR offre une vue d'ensemble et se concentre sur les interactions entre les différents nœuds du réseau.

Le fait d'obtenir un contexte de détection plus large peut révéler toute l'étendue d'une attaque et permettre des actions de réponse plus rapides et mieux ciblées.

IAST – Définitions

La technologie interactive (IAST) utilise un agent déployé sur le serveur Web de l'application testée pour surveiller le trafic envoyé lors de l'exécution et signale les vulnérabilités découvertes. Contrairement aux examens DAST, une session de surveillance IAST ne génère pas son propre trafic, mais surveille les tests de votre système, l'exploration manuelle ou le trafic envoyé lors d'un examen DAST ou SAST. Vous bénéficiez donc d'une identification continue des problèmes d'exécution sans avoir besoin d'envoyer des demandes de tests dédiées à l'application en cas de problèmes de surveillance.

Alors qu'un examen DAST voit l'application comme une "boîte noire", l'agent IAST voit à "l'intérieur" de la boîte, ce qui lui permet de découvrir plus de détails sur les vulnérabilités, tels que : l'emplacement de la vulnérabilité dans le code, l'URL, ainsi que l'entité vulnérable spécifique (telle que le paramètre, l'en-tête ou le cookie), alors que l'examen SAST fournit uniquement l'emplacement, et que l'examen DAST fournit uniquement l'URL et l'entité.

Lorsque vous installez l'agent IAST sur votre serveur Web et lancez une session de surveillance IAST, l'agent surveille le trafic (demandes, pile d'appels, variables, etc.) envoyé à l'application, et signale à AppScan Enterprise les vulnérabilités découvertes. Contrairement aux examens SAST et DAST, une session IAST peut être exécutée indéfiniment.

Vous pouvez définir l'agent IAST qui communique avec AppScan Enterprise via l'interface utilisateur ou via l'API REST. Pour plus d'informations sur l'API REST IAST, reportez-vous à la documentation sur l'API REST.

XDR – Définition

Les solutions XDR permettent de démocratiser les outils de détection. En SaaS, elles permettent de regrouper des données provenant de différentes sources et de les relier entre elles afin de se protéger et de répondre au mieux lors de cyberattaques. Le XDR ne protège pas seulement les endpoints, mais aussi les e-mails, serveurs, cloud. En augmentant les capacités de détection, le XDR permet une réaction rapide aux menaces, en amont de la kill chain, limitant nettement les dégâts. Le XDR surveille en continu et de manière proactive, pour alerter rapidement en cas de suspicion d'attaque

- EDR : apporte plus de précision, mais moins de couverture du réseau.
- NDR : couvre le réseau mais ne surveille pas les endpoints.
- XDR : abroge les frontières des périmètres de détection, apporte de l'automatisation pour accélérer les investigations et détecter les attaques sophistiquées.

CSIRT – Définition

CSIRT veut dire Computer Security Incident Response Team. C’est une entité qui gère la réponse aux incidents.

Les équipes du CSIRT travaillent en anticipation : ils enrichissent nos différents outils de connaissance de la menace (Threat Intelligence). Ils interviennent également en cas d’urgence afin d’accompagner des entreprises dans la gestion de crises cyber.

IPS – Définitions

Un système de prévention des intrusions (IPS) est une forme de sécurité de réseau qui sert à détecter et prévenir les menaces identifiées. Les systèmes de prévention des intrusions surveillent en permanence votre réseau, recherchant les éventuels actes de malveillance et capturent des informations à leur sujet. L'IPS signale ces événements aux administrateurs du système et prend des mesures préventives, telles que la fermeture des points d'accès et la reconfiguration des firewalls pour empêcher de futures attaques. Les solutions IPS peuvent également être utilisées pour identifier les problèmes liés aux politiques de sécurité de l'entreprise, afin de dissuader les employés et les invités du réseau d'enfreindre les règles incluses dans ces politiques.

SIEM – Définition

Un réseau d'entreprise typique ayant une multitude de points d'accès, il est essentiel que vous disposiez d'un moyen de surveiller les signes d'effraction potentielle, d'incidents et de menaces imminentes. Les menaces réseau actuelles sont de plus en plus sophistiquées et capables d'infiltrer toutes les solutions de sécurité, même les plus robustes.

Pour y parvenir, les analystes utilisent un outil, le SIEM (Security Information Management System). Le SIEM intègre des logiciels utilisés pour surveiller les infrastructures des entreprises. Les analystes y configurent un ensemble de règles de corrélation selon la politique de sécurité préconisée afin de détecter d'éventuelles menaces.

RASP – Définition

Le « Runtime Application Self-Protection » est une technologie de sécurité qui s'intègre aux applications. Elle a la capacité de détecter et prévenir les attaques en temps réel en contrôlant l'exécution des applications.

Cette technologie a été développée pour garder une longueur d'avance sur la pléthore de menaces liées aux applications, qui évolue sans cesse. Une fois intégré à une application, RASP remplit deux missions :

Diagnostic environnemental : Elle collecte et consigne les attaques et évènements pour enrichir les bases de données SOC et SIEM, permettant aux entreprises d'avoir une connaissance pointue de leur environnement de menaces et ainsi de mettre en place les actions préventives et curatives adéquates.

Autoprotection : La technologie RASP intercepte en permanence les signaux envoyés vers l'application pour vérifier leur sécurité et uniquement autoriser ceux qui sont sûrs. Elle procure une protection automatisée contre les menaces connues et inconnues en apportant une réponse adaptée aux comportements suspects en temps réel.

SAST – Définition

- Le « Static application security testing » doit permettre aux programmeurs de déceler les failles courantes avant la compilation d'une version. Une équipe de développement peut employer plusieurs outils SAST pour prendre en charge différents langages ou frameworks.

IDS – Définition

Les systèmes de détection d'intrusion sont des outils ayant pour objectifs de détecter des activités malicieuses sur la cible qu'ils surveillent. Une alerte sera déclenchée dès lors qu'un comportement malicieux est détecté. Les systèmes de détection d'intrusion sont utilisés en plus des solutions traditionnelles telles que les pare-feux, pour détecter différents types d'utilisations malicieuses de leur cible qui ne peuvent être détectés par ces dernières. Pour cela, de nombreux paramètres doivent être pris en compte selon ce que l'on cherche à surveiller. En effet, le système de détection d'intrusion ne se placera pas au même endroit dans l'architecture réseau. Celui-ci peut être placé en coupure du réseau, ou sur un hôte. De plus, la temporalité de l'analyse est un paramètre important, celui-ci peut produire son analyse en temps réel ou à posteriori.

Les systèmes de détection d'intrusion vont se baser sur l'écriture de règles de filtrage écrites par les utilisateurs pour effectuer leurs analyses. Par exemple, pour le système de détection d'intrusion Snort, les règles de filtrages seront composées des éléments suivants :

- l'action (alert, log, pass, activate, dynamic) déterminant le comportement à adopter en cas de détection d'intrusion ;
- le protocole à filtrer ;
- les adresses IP source et destination ;
- les numéros de ports ;
- la direction du trafic (->, <- ou <>), s'il est entrant, sortant ou bidirectionnel ;
- les options (motifs dans le paquet, drapeaux, taille, etc.).

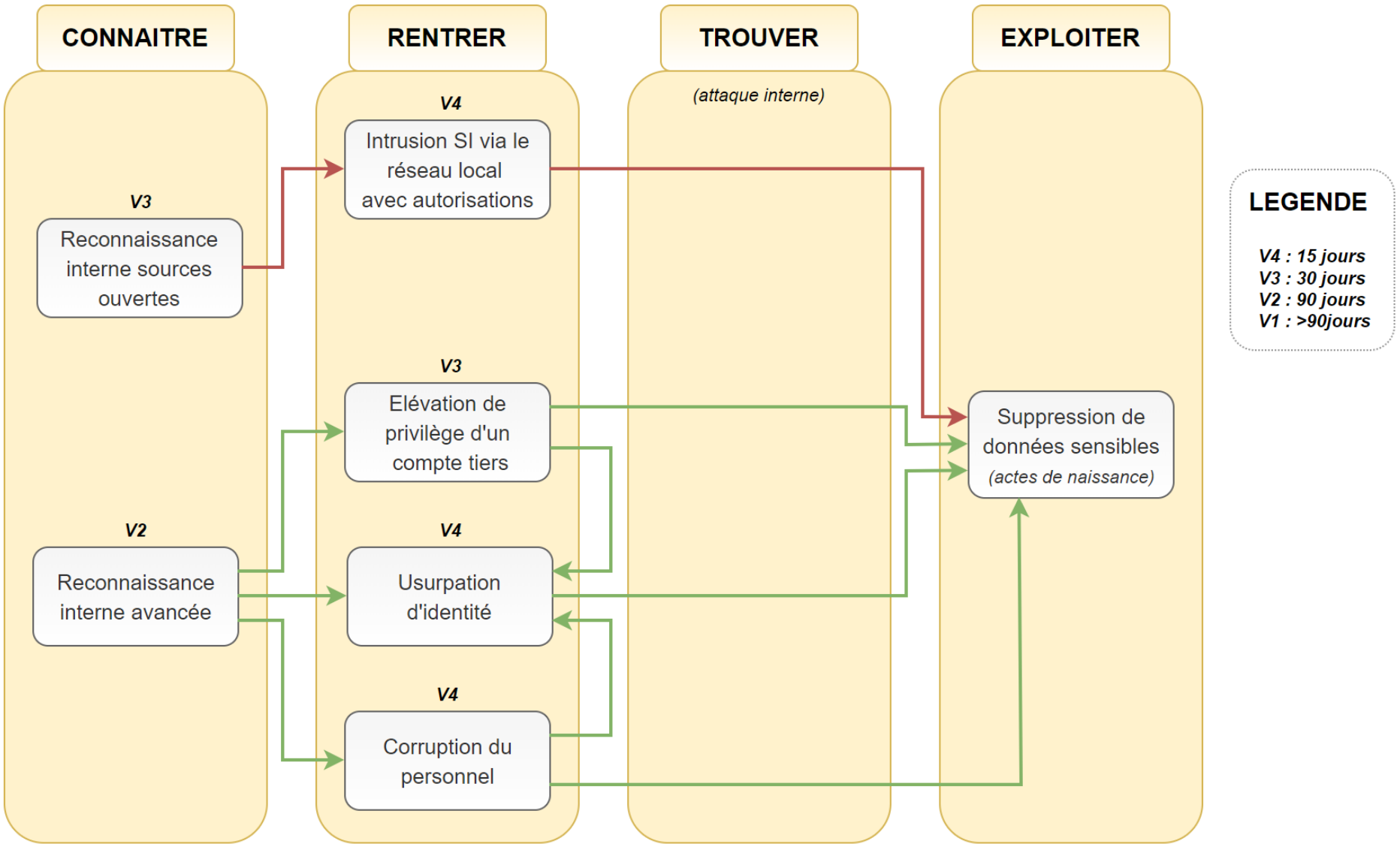
UNIVERSITÉ DE LORRAINE | LORRAINE INP
les talents se lèvent à l'Est

Atelier 4 – Méthode EBIOS

Cas d'usage : la mairie d'Angers

POLYTECH NANCY

SCENARIOS OPERATIONNELS



Justification des vraisemblances - CONNAITRE

Reconnaissance Interne en Source Ouverte V3

- Bien support
  - Réseau Local, Ordinateur de l'apprenti
- Vulnérabilité
  - Potentielle désactivation des mesures de sécurité mises en place
- Mesures de sécurité existantes
  - Aucune, l'apprenti peut désactiver toutes les mesures
    - Anti-virus, pare-feu, politique de mot de passe et mot de passe, contrôle d'accès au bâtiment, filtrage d'adresse

V3 : Son apprentissage est la plus grande de source d'information qui lui permettra de mettre à bien ses différentes actions

Justification des vraisemblances - CONNAITRE

Reconnaissance Interne avancée V2

- Bien support
  - Ingénierie sociale, enquête OSINT
- Vulnérabilité
  - Crédulité des personnels de la mairie et possible exploitation des informations personnels collectées
- Mesures de sécurité existantes
  - Les personnels sont régulièrement sensibilisés aux risques cyber mais ne sont pas former aux relations humaines

V3 : Dès son arrivé il commence son travail de social engineering en s'intéressant à chaque employé et il ira même jusqu'à sympathiser avec l'un des personnels

Justification des vraisemblances - RENTRER

Intrusion via le réseau local de l'établissement V4

- Biens support impactés
  - Réseau local administré par l'administrateur et son apprenti
  - PC de l'apprenti et de ses collègues
- Vulnérabilité
  - L'apprenti possède un compte administrateur lui permettant d'accéder à toutes les données du réseau
- Mesures de sécurité existantes
  - Mot de passe administrateur sur la base de données
  - Potentiellement aucune

V4 : l'apprenti a monté et administré le réseau avec son tuteur, il aura même fait exprès de laisser des portes dérobées dans le but de voler des informations avant de les supprimer. Cela ne lui prendra pas beaucoup de temps à s'introduire.

Justification des vraisemblances - RENTRER

Elévation de privilège V3

- Biens supports
  - PC de l’apprenti et du personnel
- Vulnérabilités
  - Le tuteur de l’apprenti, sans verrouiller son ordinateur, va régulièrement prendre un café et discute à peu près 10 minutes avec ses collègues devant la machine à café
- Mesure de sécurité existantes
  - Aucune, le tuteur n’applique pas ses propres consignes de sensibilisation : « faites ce que je dis, pas ce que je fais »

V3 : Il ne faudra pas plus de 30 jours pour réussir à accéder secrètement à l’ordinateur de son tuteur. Cela permettra à l'apprenti de réaliser une élévation de privilège d’un compte tiers plus accessible pour pouvoir effectuer ses actions et qui ne laissera normalement pas de trace pour retrouver l'origine de l'attaque excepté son tuteur.

Justification des vraisemblances - RENTRER

Usurpation d’identité

- Bien support impacté
  - PC
- Vulnérabilité
  - Avec un peu d'observation, je peux prendre la place d'un de mes collègues en son absence (exemple sa pause)
- Mesures de sécurité existantes
  - verrouillage de session

V4 : L’apprenti aura eu toute la phase de reconnaissance interne pour observer les habitudes de ses collègues. Il ne lui faudra pas plus de 15jours pour les utiliser. En effet son maitre d’apprentissage est un grand fumeur. L’apprenti utilisera cette carte pour se faire passer pour lui lors d’une de ses longues et nombreuses pauses.

Justification des vraisemblances - RENTRER

Corruption de personnel

- Bien support impacté
  - Personnel
- Vulnérabilités
  - Réussir à faire supprimer des données sensibles directement par quelqu'un d'autre.
  - Réussir à soutirer des authentifiant/identifiants afin de réaliser une élévation de privilèges.
- Mesures de sécurité existantes
  - Sensibilisation aux mesures de social engineering extérieures à l’entreprise.

V4 : L'apprenti charmera rapidement la secrétaire, moins de 15 jours, afin d'avoir son entière confiance et pouvoir lui emprunter son poste informatique en toute transparence afin de supprimer depuis son poste des fichiers sensibles.

UNIVERSITÉ DE LORRAINE | LORRAINE INP
les talents se lèvent à l'Est

Ateliers 5 – Méthode EBIOS

Cas d'usage : la mairie d'Angers

POLYTECH NANCY

Risques

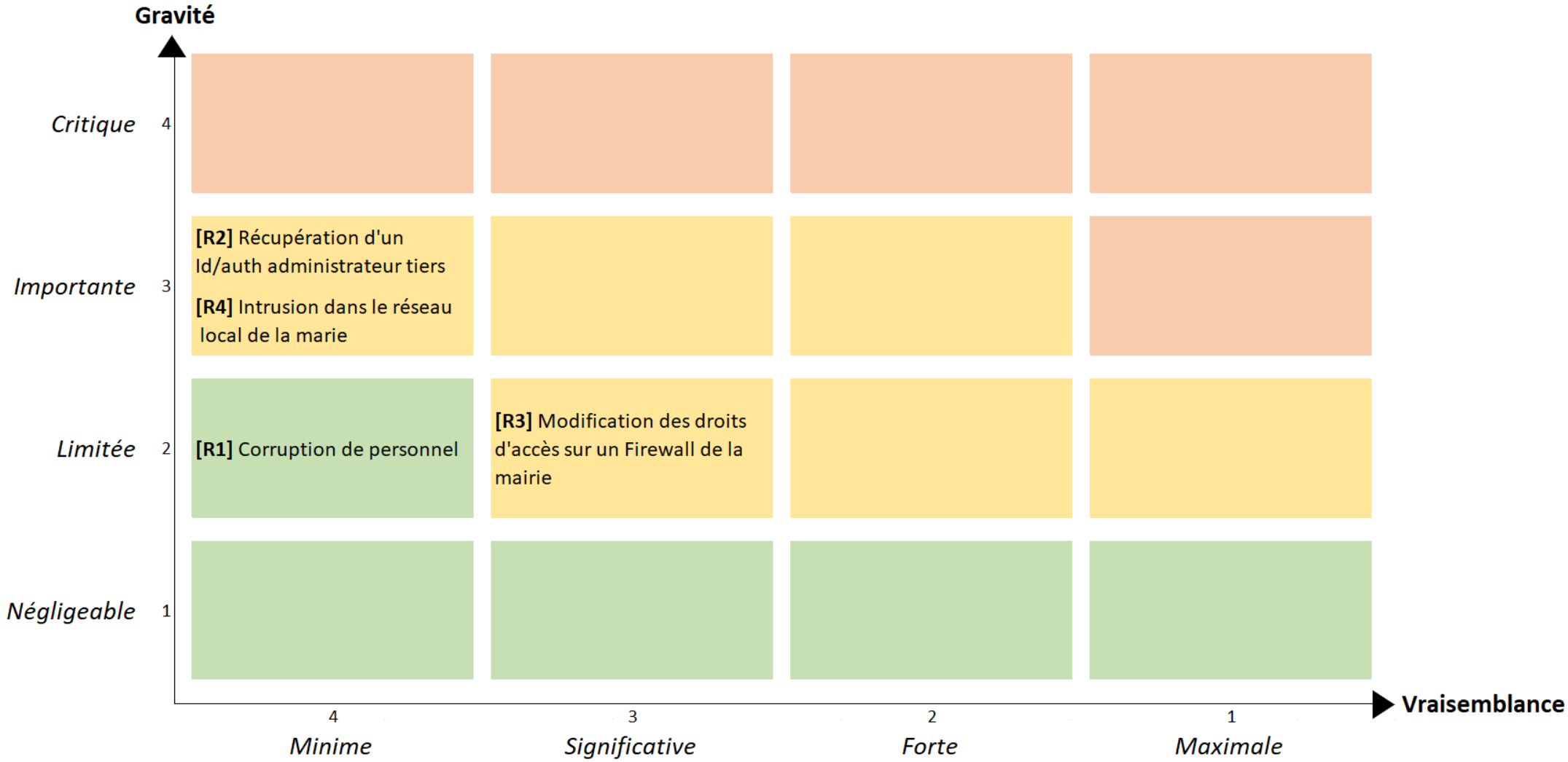
R1 : Corruption de personnel

R2 : Récupération d’un identifiant/authentifiant administrateur tiers

R3 : Modification des droits d’accès sur un firewall de la mairie

R4 : Intrusion dans le réseau local de la mairie

Cartographie des risques



Guillaume

- R1 → Transférer (Service RH)
- R2 → Traiter
- R3 → Traiter
- R4 → Réduire

Mesure de Sécu.	Risque associé	Type de mesure	Responsable	Echéance	Objectif	Indicateur	Statut
Demande de formation RH	R1	Gouvernance	Service RH	2 mois	Détecter et Signaler les tentatives de corruption	Taux de réussite	A lancer
Mise en place d'un gestionnaire de mot de passe	R2	Protection	RSSI	1 mois	Le mot de passe maître sera en l'unique connaissance du RSSI	Taux de mot de passe enregistré dans le gestionnaire	A lancer
Mise en place d'un accès sécurisé aux équipements VPN et Mot de passe admin	R3	Protection	RSSI	2 mois	Accès restreint au RSSI, action tiers sous justification écrite et contrôlé	Effectif à la mise en place	A lancer
Changement de tous les mots de passe	R1, R2 et R3	Gouvernance	RSSI	2 semaines	Mise en place d'une politique de mot de passe forte	Mot de passe de 100 bits minimum	A lancer
Mise en place d'un centre de surveillance type Nagios	R2, R3 et R4	Défense	RSSI	1 mois	Réception des log de l'Infra. Syst.	Taux d'équipement enregistré dans la solution	A lancer
Mise en place d'un accès restreint aux équipements réseaux	R4		RSSI	2 mois	Mise en place de mot de passe aux équipements	Taux d'équipement sécurisé	A lancer
Protection renforcé des données sensibles	R1, R2, R3 et R4	Protection	RSSI	2 mois	Chiffrer les documents et droits de suppression	Taux de document chiffré	A lancer

Arthur – PLAN D'ACTION

MESURE DE SECURITE	SCENARIOS DE RISQUES ASSOCIES	RESPONSABLE	COÛT / COMPLEXITE	INDICATEUR	OBJECTIF	ECHEANCE	STATUT	
GOUVERNANCE								
Sensibilisation renforcée à la corruption par un prestataire spécialisé	R1	RSSI / DRH / Prestataire	+	Taux de participation	Réduire les corruptions de personnel par une formation permettant de détecter et d'alerter les comportements de corruption	1 mois	à lancer	➢ Transférer
Politique de changement de mot de passe mensuel	R1 - R2 - R3	RSSI	+	Taux de changement de mot de passe	Augmenter la fréquence de changement de mot de passe du personnel	2 mois	à lancer	➢ Réduire
PROTECTION								
Mise en place d'un système de validation de connexion via l'envoie d'un SMS à l'administrateur	R2	RSSI	++	Taux de notification SMS émise	Alerter l'administrateur d'une connexion en cours afin de la valider si il en est bien l'émetteur	4 mois	à lancer	➢ Traiter
Mise en place d'un gestionnaire de mot de passe	R2	RSSI	+	Taux de mot de passe stocké	Stocke le mot de passe administrateur de manière sécurisé et créer des mots de passe avec un pattern plus complexe	2 mois	à lancer	➢ Réduire
Protection renforcée des données sur le SI	R1 - R2 - R3 - R4	DSI	+++	Taux de fichiers protégés	Protéger les données sensibles via un système de chiffrement ou de cloisonnement	9 mois	à lancer	➢ Traiter
Renforcement de la sécurité du système informatique selon les recommandations ANSSI	R3	DSI / RSSI	+++	Taux d'équipements sécurisé informatiquement	Renforcer la protection des équipements via l'augmentation de la sécurité des équipements informatiques avec l'utilisation de différents protocoles de sécurité	12 mois	à lancer	➢ Réduire
Renforcement du contrôle d'accès physique aux équipements réseaux/informatiques	R3 - R4	RSSI	++	Taux d'équipements sécurisé humainement	Renforcer le contrôle d'accès aux équipement via la création d'une équipe de sécurité au sein de la mairie	12 mois	à lancer	➢ Transférer
DEFENSE								
Surveillance renforcée des flux entrants et sortants - analyse des journaux d'événements à l'aide d'un outil	R4	DSI	++	Taux d'alerte de l'outil	Alerte le responsable de comportement particulier sur le réseau local de la mairie	6 mois	à lancer	➢ Transférer

Juliette

Mesure de Sécu.	Risque associé	Qui ?	Quand ?	Objectif	Indicateur	Statut	Option
Mettre en place des évènements de sensibilisation aux risque INTERNE de social engineering	R1	Le service informatique en collaboration avec le service RH	Début des évènements dans le trimestre. Garder un rythme d'évènements régulier par la suite.	Faire comprendre aux employés que même les collègues peuvent vouloir nuire à l'entreprise	Taux de participation aux évènements	À Lancer	Réduction
Définir une validité quotidienne pour les couples identifiant/authentifiant des administrateurs.	R2	Le service informatique	Dès que possible	En cas de récupération d'accès administrateur, la personne malveillante n'aura qu'une très courte fenêtre de tire.		À Lancer	Transfert
Recevoir une notification dès qu'un administrateur se connecte	R2	Le service informatique	Cette semaine, cette action n'est pas compliquée à mettre en place.	Pouvoir réagir immédiatement (avant qu'il y ai des dégâts) en cas d'usurpation d'identifiant.	Notification	À Lancer	Traitement
Accorder des droits particuliers et adaptés aux utilisateurs	R3	Le service informatique	Dans le mois	En cas d'usurpation, la personne malveillante sera limitée dans ses actions.	Table des droits	À lancer	Reduction
Obliger chaque personne étrangère à l'entreprise (et elle seule) à présenter une pièce d'identité à un agent de contrôle.	R4	Le service RH	Dans le mois	Dissuader des personnes malveillantes de se faire passer pour des techniciens et accéder à des locaux confidentiels	Documents historique des passages	À Lancer	Transfert
Mettre en place une limite d'accès à certains équipements	R4	Le service informatique	Dans le trimestre	Empêcher les personnes non-autorisées à rentrer dans des espaces confidentiels	Logs des salles	À Lancer	Reduction