GATEWATCHER

Dominique MEURISSE
VP Sales Int'l

Devant la recrudescence des Attaques ciblées et des ransomwares :

- Quels sont les bénéfices attendus de la détection du réseau (NDR) ?
- Quelle complémentarité DETECTION-PREVENTION ?

SECURITY FORUM

Van der Valk Hotel Nivelles-Sud
– 4 octobre 2022

Cyber attaques :
Situation en Belgique

La Belgique, championne européenne des cyberattaques

Les chiffres parlent d'eux-mêmes…

Avec le taux le plus élevé en Europe d'organisations victimes de cyberattaques, la Belgique demeure la cible favorite des cybercriminels : **71% organisations touchées en Belgique** contre 68% aux Pays-Bas, 67% en France et 61% en Allemagne. (*source Trends Tendances, 16/05/2019).*

ASCO

A titre d'exemple, une **cyberattaque de type rançongiciel** a visé en juin 2019 ASCO, situé à Zaventem. Le constructeur d'équipements en aéronautique a été contraint de mettre ses 1000 employés au chômage technique pour une durée d'un mois. Par ailleurs, les usines de la firme situées aux Etats Unis, au Canada et en Allemagne ont également été forcées de stopper leur production industrielle.

Cyber attaque à l'encontre de la Chancellerie Belge
23 Sep 2022

L'informatique de la Chancellerie du Premier ministre belge ciblée par une attaque informatique.

Belgique : le gouvernement et l'armée victimes de cyberattaques chinoises 07/22

Dans une déclaration récente, le gouvernement belge a déclaré avoir détecté trois acteurs chinois à l'origine de plusieurs cyberattaques sur les institutions publiques et les forces de défense du pays. Selon la Belgique, les trois gangs concernés sont APT 27 (UNSC 2814), APT 30 (Gallium) [illegible]PT 31 (Softcell).

Cyber attaques

Malveillantes

Arrestation/recrutement

Edward Snowden est désormais russe

Le lanceur d'alerte, qui est réfugié en Russie depuis 2013, a bénéficié d'un décret signé par Vladimir Poutine.

Sébastien Raoult

Etatiques

Cible : Organisation fédéral US
Dommage collatéraux : 18.000 Clients

Panne d'Internet : coupure de câbles de fibre optique

Une enquête a été ouverte, mercredi 27 avril 2022, après que des câbles du réseau national de fibre optique ont été sectionnés, entraînant des coupures d'accès à Internet dans plusieurs grandes villes de France. Une panne d'ampleur est-elle probable ? Internet est-il vulnérable ?

Du *CyberChaos* au *CyberPrematie* !!

Guerre en Ukraine : une bataille de communication

Arrestation
Recrutement

THE UNITED STATES DEPARTMENT of JUSTICE

FOR IMMEDIATE RELEASE
Wednesday, September 14, 2022
Three Iranian Nationals Charged With Engaging In Computer Intrusions And Ransomware-Style Extortion Against U.S. Critical Infrastructure Providers

Sébastien Raoult

un étudiant en informatique vosgien, est incarcéré depuis le 2 juin à la prison de Tiflet 2, près de Rabat, après avoir été interpellé le 31 mai à l'aéroport de Rabat-Salé. Il faisait alors l'objet d'une notice rouge émise par Interpol à la demande de la justice américaine, dans le cadre d'une affaire de cyberpiraterie
Il risque 116 ans de prison aux États-Unis

INTERPOL

Two prolific ransomware operators suspected of carrying out a string of attacks, demanding ransoms of up to EUR 70 million, have been arrested in Ukraine.
The arrests were made on 28 September as a result of global law enforcement cooperation involving the French National Gendarmerie, the Ukrainian National Police and the United States Federal Bureau of Investigation (FBI), INTERPOL and Europol.

Tea Pot

GTA 6 : la police arrête le hacker présumé, c'est un ado de 17 ans 23/09/2022

Un adolescent a été arrêté hier soir dans le sud de l'Angleterre dans le cadre de l'enquête sur le piratage des serveurs de Rockstar Games. Le jeune homme serait un membre du groupe de hackers Lapsus$, qui fait décidemment beaucoup parler de lui en ce moment.... => UBER

Tea Pot

Teapotuberhacer
Or
$Lapsus ?

MOTIVATIONS ?

MFA sur le VPN :

- Achat de credential sur le Darkweb
- employé valide sa connexion sur son application
- Attaque: demander en boucle à l'utilisateur de s'authentifier avec un second facteur,
- L'utilisateur valide le second facteur et divulgue ses identifiants.

L'attaquant :

- Accède et scanner le réseau local
- Découvre un script qui contenait les identifiants d'un compte administrateur.

Avec l'élévation de ses privilèges, il a ensuite compromis:

- La solution d'IAM, et de PAM
- Le programme de bug bounty (il a donc eu accès à tous les bugs rapportés à Uber)
- Google Suite
- l'EDR Sentinel One
- l'instance Slack
- plusieurs outils internes d'Uber

PARADOXE FRANCAIS

- Rechercher l'**assistance technique d'experts**; de communiquer au maximum sur l'attaque et les futurs risques à avenir au sein de l'entreprise ;
- de restaurer les systèmes touchés **depuis des sources saines**
- de **déposer** plainte
- **surtout, de ne pas payer la rançon demandée.**

VS

Rançongiciels : l'Etat prêt à valider l'indemnisation des rançons par les assurances.
Le gouvernement entend clarifier le cadre légal des assurances contre les risques cyber en légalisant une mesure qui autorisera les compagnies à indemniser les victimes, sous réserve d'un dépôt de plainte.
07 septembre 2022

LPM => impose l'utilisation de Sondes de detection Certifiées

La loi n°son article 34, des dispositions relatives au renforcement des capacités de détection des attaques informatiques, aujourd'hui indispensables pour élever le niveau de sécurité de la Nation. Le décret d'application publié au journal officiel aujourd'hui vient en préciser les modalités de mise en application, avec une entrée en vigueur au 1er janvier 2019.
Pour répondre à l'accroissement du niveau général de la menace, le renforcement de la capacité nationale de détection, de caractérisation et de prévention des attaques informatiques apparaît comme prioritaire.

Confortant le modèle français en matière de cyberdéfense, l'article 34 de la loi n°2018-607 relative à la programmation militaire pour les années 2019 – 2025 , et son décret d'application viennent aujourd'hui renforcer les missions de l'ANSSI en améliorant ses capacités de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés.

TF1

Cyberattaque au CHU de Corbeil-Essonnes : des données volées publiées par les hackers

Cyberattaques :

Détection - Protection / Action - Réaction

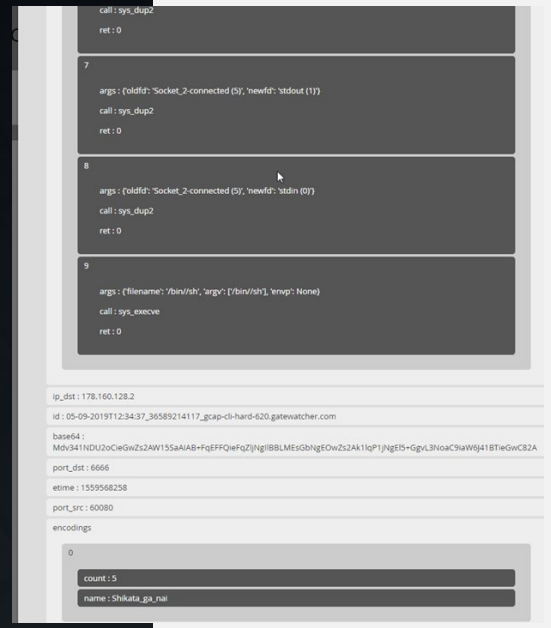
Diminuer le temps de détection d'une attaque c'est maximiser la disponibilité du Revenu et éviter de payer des rançons
=> ROI

Historique : temps réel
=> détection limité
(4.500 régles NGFW)

Ex 1 : shellcode :

base64 :
Mdv341NDU2oCieGwZs2AW15SaAIAB+FqEFFQieFqZljNgIlBBLMEsGbNgEOwZs2Ak1lqP1jNgEl5+GgvL3NoaC9iaW6J41BTieGwC82A

NDR : *ShellCode décodé et mis en clair*



Ex 2 : DGA

Syntaxe des requettes DGA utilisées

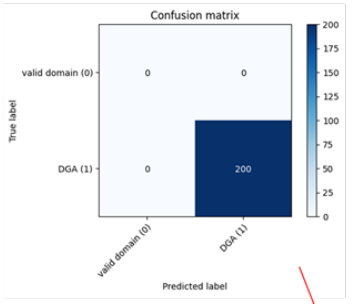
<encoded_guid> + <byte> +<encoded_hostname>

```
7cbtailjomqle1pjvr2d32i2voe60ce2.appsync-api.us-east-1.avsvmcloud.com
```

Encoded guid (15 chars)	**byte**	Encoded hostname
7cbtailjomqle1p	**j**	**vr2d32i2voe60ce2**

Once we learned of the existence of SUNBURST, we retrained the model with the new TLDs (72 hours later).

	domain	truth_label	predict_proba	predict_label
863	fvid9kfs8iph7gbt9uf29l49711e.appsync-api.us-ea...	1	0.999792	1
576	agfcf1umrv7s0ahp00mudofi75f4tjvh.appsync-api.u...	1	0.999792	1
201	3jn61ob016fliibe6d6n0t6j0oeu.appsync-api.us-ea...	1	0.999792	1
76	18shu72lull6bclce2q0b12eu1.appsync-api.eu-west...	1	0.999805	1
367	6i6gkuq4rrqj9n8h6d6n0e6j0ieu.appsync-api.us-ea...	1	0.999792	1
...	...	...	...	...
509	97v4u78ma1kdecak6d6n0c6j0ieu.appsync-api.us-ea...	1	0.999792	1
1043	jcvi7o1j7k24b0hywh60tun0gwusouv0.appsync-api.u...	1	0.999792	1
1122	l743rbuf8scv0161v52296bbfg5qal49.appsync-api.u...	1	0.999792	1
1611	tml0euav96phrjb800mudofi75f4tjvh.appsync-api.u...	1	0.999792	1
1558	sjs8jtah96r4mbf6u30o2st.appsync-api.us-east-2....	1	0.999803	1

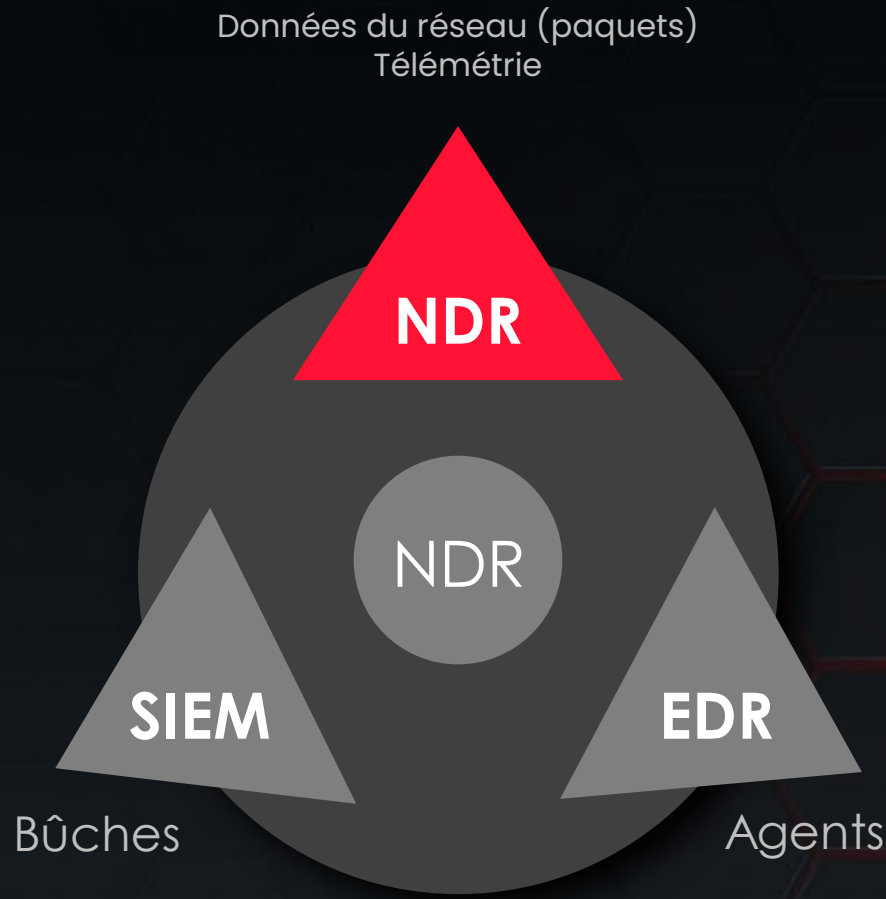


100% DGA domain names detected.

DÉFINITION D'UN NDR
NDR, EDR, ET SIEM/UEBA

Définition du Gartner

Network Detection and Response (NDR) utilise une combinaison d'apprentissage automatique (ML), d'analyse avancée et de détection basée sur des règles pour détecter les activités anormales et suspectes sur les réseaux d'entreprise.



- Augmenter la visibilité
- Solution adaptée à la détection des APT
- Facilite les enquêtes grâce aux métadonnées collectées
- Réponse rapide aux incidents
- "Le réseau ne ment jamais"

- Conformité
- Approche holistique (rapports, tableaux de bord)
- Données Normalisée
- Convergence IT/OT/IoT

- La prévention seule ne suffit plus
- Solution adaptée à la mobilité
- Permettre et simplifier l'enquête
- Réponse rapide aux incidents

Qui sommes nous ?

QUI EST GATEWATCHER ?

Créé en
2015

40% effectifs
R&D

Un réseau de plus de
50 partenaires

99%
renouvellement clients

Un acteur mondial avec
des bureaux
dans le monde entier

France, Royaume-Uni & Irlande
Allemagne, Benelux, Nordics
Afrique du Nord, Moyen-Orient,
Singapore

+600
infrastructures protégées

+20 milliards
d'événements gérés par jour

100 Millions
fichiers analysés par jour

ENGAGEMENT POUR DELIVRER

PRINCIPALES REFERENCES

BNP PARIBAS La banque d'un monde qui change
EURONEXT
TOTAL
SAFRAN
GROUPE BPCE
BANQUE DE FRANCE
SUEZ
VEOLIA
LCH The Markets' Partner
SANOFI
framatome
AIRBUS
AMSN PRINCIPAUTÉ DE MONACO
NAVAL GROUP
orano
stet
SOCIETE GENERALE
European Investment Bank
MINISTÈRE DES ARMÉES
MINISTÈRE DE L'INTÉRIEUR
orange
CA
EDF
SNCF

ENGAGEMENT PARTENAIRES

INTEGRATEURS & MSSP : Atos, sogeti Part of Capgemini, Orange Cyberdefense

ALLIANCES TECHNOLOGIQUES : proofpoint, splunk>, NOZOMI NETWORKS, Gigamon

DÉTECTION

DÉTECTION RENFORCÉE

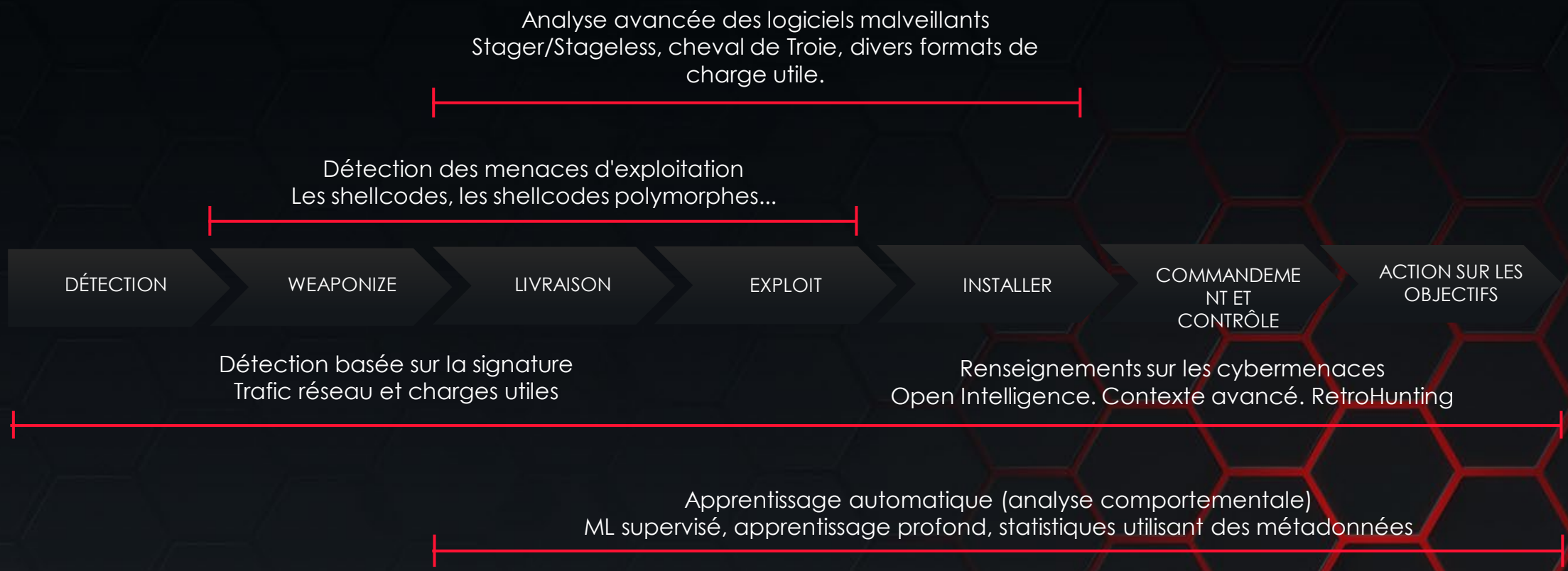
Perspectives humaines alimentées par l'IA

Détection statique et dynamique des menaces	Règles statiques Anti-malware Sandboxing et analyse
Enrichissement et analyse	Métadonnées Suivi des paquets Rétro-analyse
Détection zero-day	Shellcode avancé Payload polymorphe
Intelligence artificielle (Machine Learning)	Powershell obfusqué DGA (C&C inconnu) Ransomware Analystes augmentés

Combinaison de connaissances et d'analyse comportementale sont les deux piliers d'une solution de détection efficace.

S'adapter à l'évolution du paysage des menaces

Les rôles de nos moteurs de détection dans la chaîne de mise à mort



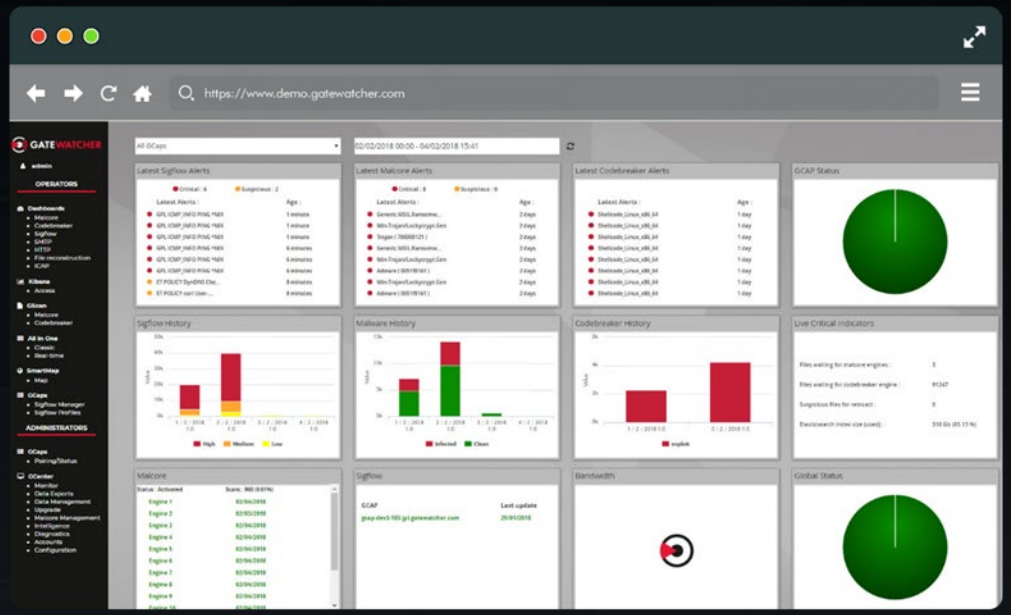
S'adapter à l'évolution du paysage des menaces

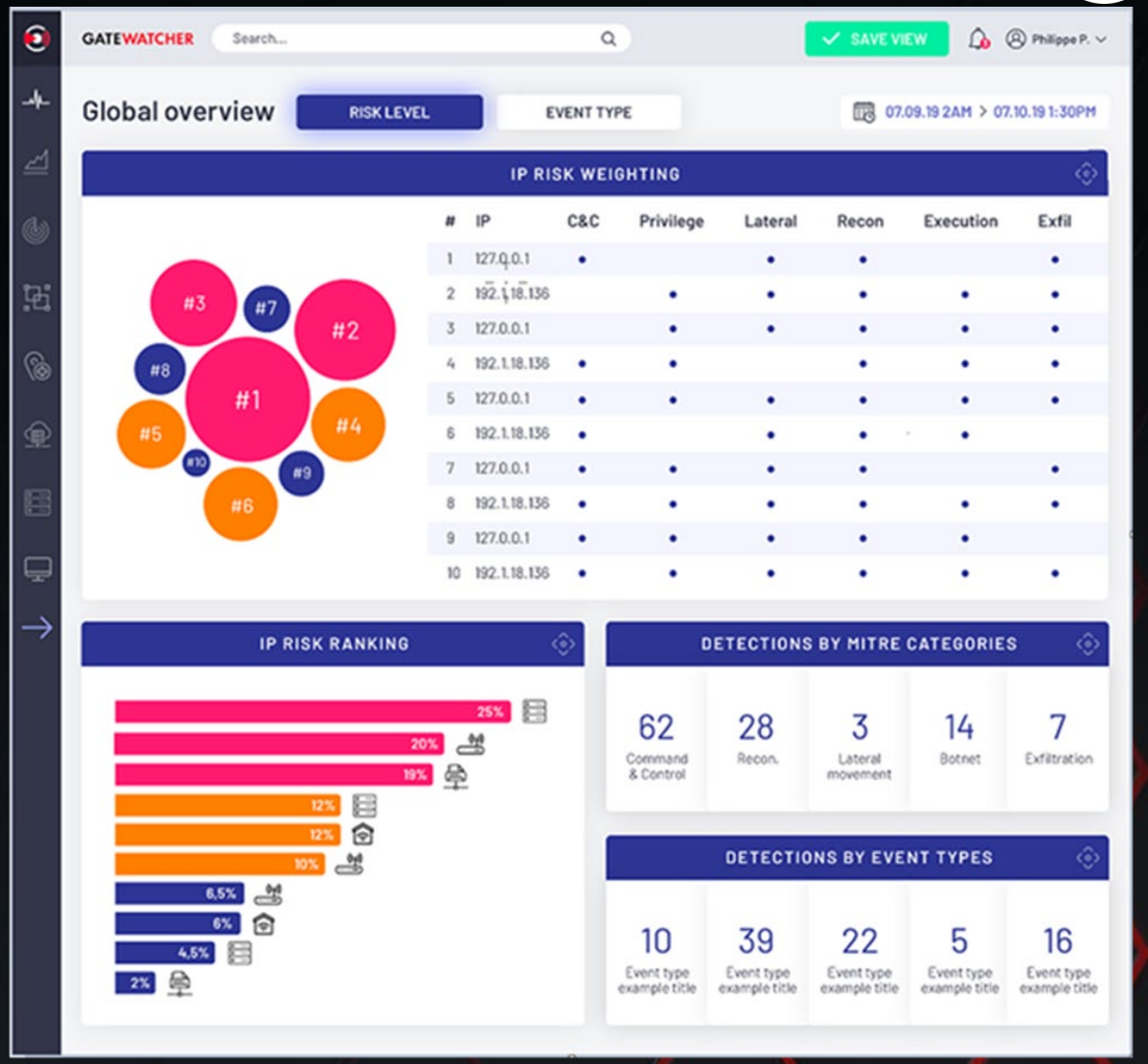
Une utilisation contrôlée de l'IA

ML, DL, Graph ML

OBJECTIFS	TYPE AI	PROTOCOLES	COMMENTAIRES
Détection de la DGA	Supervisé	DNS	Les algorithmes détectent les noms de domaine générés de manière aléatoire (https://attack.mitre.org/techniques/T1568/002/).
Détection des ransomwares	Semi-supervisé	SMB	Les algorithmes détectent les anomalies dans les opérations sur les fichiers (lecture/écriture) via le protocole SMB.
Détection du phishing	Hybride	SMTP	Approche hybride (apprentissage profond combiné à une approche supervisée), qui permet de détecter les URL malveillantes dans les courriers électroniques.
Détection des ransomwares	Apprentissage profond	Fichiers	Mise en œuvre de réseaux neuronaux LSTM pour combiner les hachages flous avec d'autres caractéristiques afin de détecter les similitudes et de catégoriser les fichiers.
Détection d'authentification malveillante	Hybride	Kerberos	Graphique et algorithmes supervisés combinés pour détecter les attaques malveillantes dans les protocoles Kerberos. Une approche basée sur l'UEBA.
Réduction des faux positifs	Semi-supervisé	Alertes	Réduction des faux positifs grâce à la technique du clustering.
Analyste augmenté	Supervisé	Sortie d'alertes/triage	Superviser les algorithmes pour fournir des conseils ou des recommandations aux analystes.

REPORTING



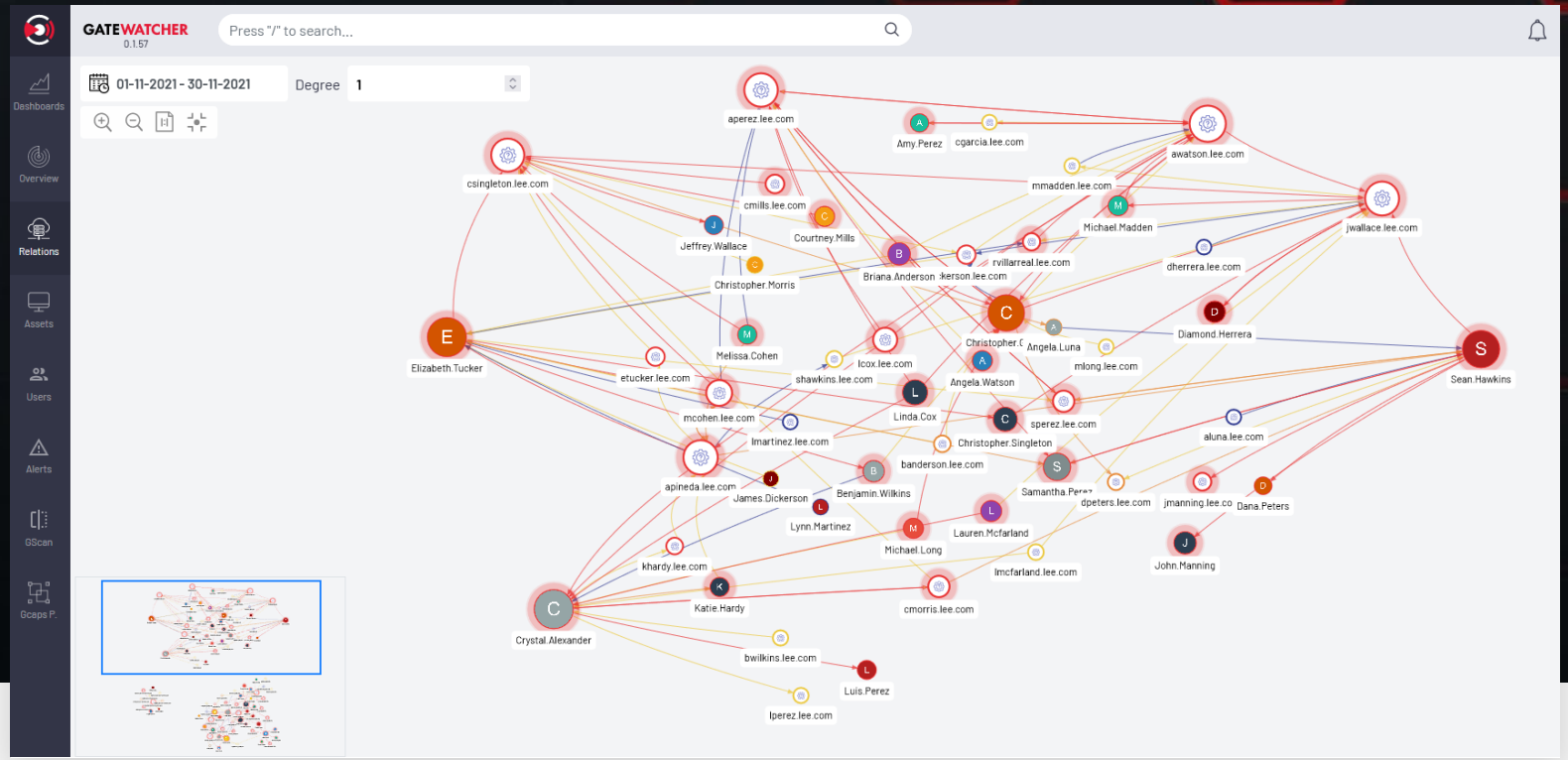


INVESTIGATION

HUNTING & FORENSIC

Behavorial
and mapping analysis

Dynamic Mapping of users & assets



Added-Value for Cyber Response Teams

- Immediate view of networks to identify gaps & attack surface
- Provides risk scoring and detailed insights into networks including asset behavior, roles, protocols, and data

Benefits

- Generates macro views as well as dynamic information on assets and connections over time
- Increases awareness with automated and passive asset inventory

REPONSE

FAVORISER LA PRISE DE DÉCISION

Intégration SOCs et environnements informatiques

Open APIs	Rest API Swagger API SIEM, SOAR, EDR
Intégration XDR	OpenXDR SIEM
Orchestration	Scripting Événements déclenchés API d'administration

Aider les équipes SOCs à prendre de meilleures mesures
pour l'élimination des menaces, quelle que soit l'infrastructure existante.

Tea Pot

- ShellCode
- CC & DGA
- Lateral Move
- NMAP
- UBA
- Cartography

Achat sur Darkweb d'une adresse UBER

employé valide sa connexion sur son application

Attaque :demander en boucle à l'utilisateur de s'authentifier avec un second facteur,

L'utilisateur valide le second facteur et divulgue ses identifiants.

L'attaquant :

- Accède et scanner le réseau local
- découvre un script qui contenait les identifiants d'un compte administrateur.

Avec l'élévation de ses privilèges,

il a ensuite compromis:

- la solution d'IAM, et de PAM
- le programme de bug bounty (il a donc eu accès à tous les bugs rapportés à Uber)
- Google Suite
- l'EDR Sentinel One
- l'instance Slack
- plusieurs outils internes d'Uber

COMMUNIQUER SANS COMPROMETTRE L'INTEGRITE DU SOC
QUEL ÉCOSYSTÈME ?

SIEM/XDR

Corréler nos métadonnées et nos alertes avec d'autres solutions pour créer des scénarios d'attaque et de défense.

FIREWALL

Flux de communication bidirectionnel pour bloquer le plus rapidement possible les menaces les plus obfusquées, en cas de doute.

EDR

Assurer la visibilité du réseau et des systèmes en fournissant automatiquement des données contextuelles enrichies.

ORCHESTRATION

Pour optimiser la phase de tri et exécuter les playbooks.

MICRO-SEGM.

Pour analyser les flux d'applications.

VISIBILITÉ

Les technologies de soutien telles que les agrégateurs ou les solutions de décryptage des flux.

PROTÉGER VOTRE ENTREPRISE
ANTICIPER VOS PROCHAINES MENACES

Vos avantages

Réduction du MTTD

Visibilité complète

Détection des attaques complexes

Détection des attaques de type "Zero Day".

Contexte de l'attaque (Patient 0)

Optimisation du SOC

Réduction du MTTR

Automatisation et l'orchestration

Des ressources réduites

Amélioration de votre cyber-stratégie

Couverture de la menace

Renforcement des solutions existantes

Nos expertises

DÉTECTION

DÉTECTION RENFORCÉE

Perspectives humaines alimentées par l'IA

ENQUÊTE

INVESTIGATION ET ENQUETE

Analyse comportementale et cartographique

RÉPONSE

FAVORISER LA PRISE DE DÉCISION

Intégration SOCs & environnements informatiques

INTELLIGENCE

UNE DÉTECTION PLUS INTELLIGENTE

Analyse de flux enrichis

MERCI