Dans la tête de l'adversaire:

Comment les responsables de la sécurité peuvent anticiper les attaques de demain grâce à une Threat Intelligence adaptée à leur contexte

Sponsorisé par

kaspersky

TechTarget

Reprendre l'avantage face aux cyberattaquants suppose, pour les responsables de la sécurité, de détecter les menaces en amont, un enjeu auquel répondent aujourd'hui les techniques modernes de veille des cybermenaces.
La cybersécurité n'est plus une bataille opposant pare-feux et logiciels malveillants. Il s'agit aujourd'hui d'une « course à l'armement » dans laquelle des équipes défensives sous pression affrontent des adversaires bien organisés.

Introduction

Dans ce contexte, laisser l'initiative aux attaquants expose toute organisation à un niveau de risque insoutenable. Fatalité ou pas, nous constatons que l'évolution soutenue de la technologie est favorable aux attaquants qui progressent plus vite que les équipes de défense ne sont en capacité de réagir. D'après l'ENISA (Agence de l'Union européenne pour la cybersécurité), près de 70% des tentatives d'exploitation de failles de sécurité aboutissent aujourd'hui à des intrusions fructueuses, et 68,6% de ces dernières se soldent par des violations de données. Deloitte rapporte que 31% des organisations ont subi au moins six intrusions cyber au cours de l'année passée, pratiquement trois fois plus que l'année précédente. Les services de renseignement internationaux suivent désormais plus d'un millier de campagnes et d'acteurs malveillants actifs dans plus de 85 pays. Le message est clair: les organisations doivent savoir interpréter les signaux à l'échelle de vastes écosystèmes.
Il en résulte que l'anticipation stratégique des menaces est devenue LE facteur clé de différenciation. Les organisations ne se contentent plus de colmater leurs vulnérabilités et de ne réagir qu'après les violations. Au contraire, elles veulent disposer d'informations pour se préparer aux attaques, bien que la plupart de ces organisations recourent encore à des indicateurs statiques et des mesures réactives ne leur permettant pas de comprendre qui les cible, dans quel objectif et avec quels moyens. Disposer de ces éclairages vous permettra de gagner tant en rapidité qu'en efficacité face aux menaces tout en affichant des progrès tangibles sur la protection que requièrent vos activités.

Ce rapport couvre l'évolution de l'information sur la menace à commencer par la donnée brute pour aboutir à des éléments contextuels permettant de révéler les intentions de l'adversaire, son comportement et son écosystème avant que l'attaque ne se produise.

Il montre comment une veille contextuelle, alimentée par l'expertise humaine et l'intelligence artificielle transforme des signaux fragmentés en prévisions sur lesquelles les responsables de la sécurité peuvent s'appuyer, aidant ainsi les organisations à prédire les comportements, à réduire la pression liée à une surabondance d'alertes et à améliorer la prise de décision en matière de prévention, de détection et de réaction. Il fournit également un guide opérationnel, prêt à l'emploi, à l'intention des CISO. Ce guide facilitera l'adoption d'une Threat Intelligence (renseignement sur les cybermenaces, ou cyberintelligence) adaptée au contexte, il fournit des indicateurs de performance clés (KPI) permettant la progression depuis une posture défensive vers une approche centrée sur l'anticipation stratégique.

Qu’entend-on par “contexte” en matière de Threat Intelligence?

Les trois dimensions du contexte

La Threat Intelligence contextuelle repose sur trois logiques complémentaires: comportementale, environnementale et analytique. Combinées, elles transforment des données brutes de télémesure en prévisions qui révèlent les auteurs d’une attaque en cours de préparation, leur mode opératoire et ce qu’ils sont susceptibles de faire ensuite.
Voici une description détaillée de chacune de ces dimensions:

Contexte Comportemental

Le contexte comportemental permet aux équipes de sécurité d’établir des liens entre des événements isolés pour identifier des tendances qui indiquent à quelle phase en est une offensive (repérage, intensification…). Les attaquants peuvent changer de domaine, d’adresse IP ou de hachage de fichiers, mais il est rare qu’ils abandonnent les « empreintes » comportementales qui assurent l’efficacité de leurs opérations. Voici quelques signes fiables indiquant qu’une attaque est en cours de préparation:

- Tactiques, techniques et procédures (TTP)
- Séquences et moments des attaques
- Cycle de vie des infrastructures (configuration » test » déploiement)
- Réutilisation d’outils pour différentes campagnes
- Évolution des capacités au fil du temps

Contexte Environnemental

Considérons ensuite le contexte environnemental qui aide les équipes de sécurité à comprendre quelles menaces externes peuvent s’appliquer à leur profil de risque spécifique. Votre écosystème peut comporter une faille de sécurité, mais le contexte environnemental révèle si les groupes qui ciblent actuellement votre secteur l’ont déjà utilisée. Pour savoir qui est le plus susceptible de vous attaquer, il faut tenir compte de facteurs tels que:

- Le secteur (ex.: énergie, finance, santé)
- La zone géographique et les tensions géopolitiques
- L’infrastructure technologique et l’écosystème de fournisseurs
- La visibilité sur la technologie opérationnelle (OT), les systèmes de contrôle industriel (ICS) et la surface d’exposition
- Les vulnérabilités connues présentant un risque réel pour l’activité

Contexte Analytique

Enfin, le contexte analytique transforme des données fragmentées en un scénario cohérent qui révèle les intentions et priorités des attaquants.
Par exemple, l'IA peut établir des corrélations entre des domaines suspects et une famille de logiciels malveillants. Les analystes peuvent alors réaliser qu'un modèle d'infrastructure donné signale potentiellement l'expansion d'un groupe de cybercriminels dans une nouvelle zone. Le contexte analytique met au jour des plans d'attaque qu'aucun indicateur ne pourrait identifier seul.
Par exemple:

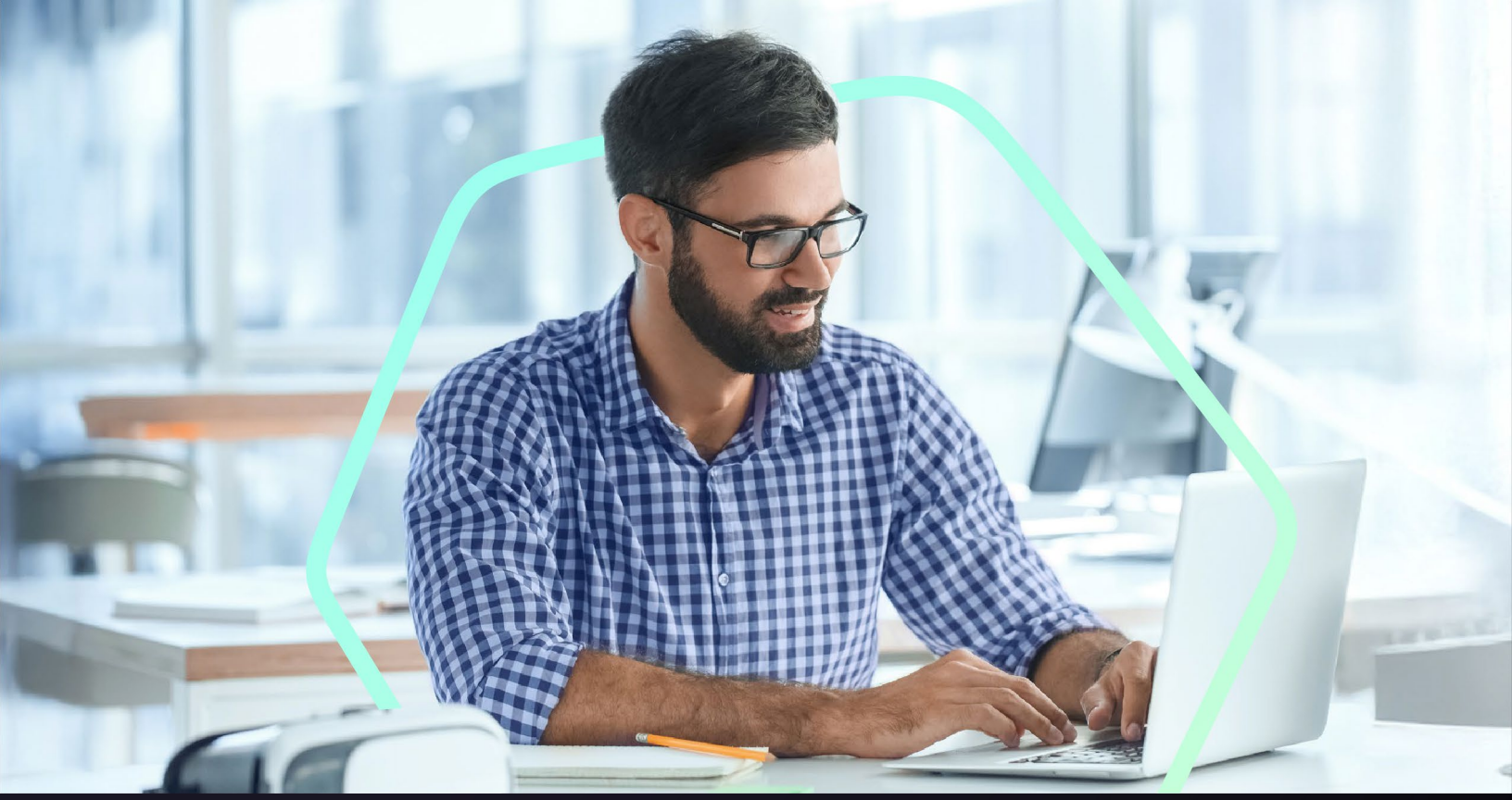
- L'analyse des similitudes entre différentes campagnes
- Le recoupement (clustering) comportemental (ex.: cartographie MITRE ATT&CK)
- Une synthèse par l'IA des attributs des logiciels malveillants, des logiciels affectés, des liens entre les auteurs des menaces
- Des indicateurs révélant les répartitions de responsabilités et les relations au sein de l'écosystème
- La vérification multi-sources

Comment le contexte permet de relier les indicateurs aux intentions des assaillants

Une défense efficace repose sur les données de télémesure provenant de réseaux mondiaux de capteurs, de la surveillance effectuée par les botnets, du recueil d'informations open source et issues du deep web, ainsi que sur les jeux de données historiques à long terme permettant d'inscrire des menaces émergentes dans le cadre d'un contexte fiable. En combinant contextes comportementaux, environnementaux et analytiques, vous obtenez un tableau détaillé de ce que les attaquants prévoient de faire. Par exemple, quand :

- Un indicateur de compromission (IOC) est lié à une campagne ciblée
- Des domaines similaires ont été utilisés par le même acteur
- La configuration de l'infrastructure suggère la préparation d'une attaque
- Une tentative de piratage correspond aux priorités connues d'un attaquant
- Un sondage des systèmes de technologie opérationnelle (OT) représente un repérage ou un signe avant-coureur de problèmes

L'expertise humaine et les analyses pilotées par l'IA s'enrichissent mutuellement pour produire des résultats inatteignables sans cette complémentarité. L'IA traite des millions de données fragmentées à la vitesse d'une machine, recoupant des événements connexes, synthétisant les caractéristiques des logiciels malveillants, établissant des corrélations entre les infrastructures réutilisées et mettant en évidence des anomalies qui prendraient aux analystes des heures, voire des jours, à identifier manuellement. Les chercheurs humains mettent ensuite à contribution leur compréhension approfondie du contexte pour reconnaître les habitudes subtiles des attaquants, les combinaisons rares de TTP, les modèles d'infrastructure et les signaux géopolitiques que les algorithmes ne peuvent pas déduire de manière fiable. Ensemble, l'IA et l'expertise humaine créent un système qui transforme le bruit en prédiction.



Dans la tête de l'adversaire: les tendances à suivre pour les responsables de la sécurité des systèmes d'information

Une fois que les défenseurs savent comment interpréter les données à travers les trois prismes du contexte (comportemental, environnemental et analytique), ils peuvent découvrir la logique profonde qui se cache derrière les opérations des adversaires. Les groupes de cybercriminels modernes ont des cycles de planification, des rôles opérationnels, une gestion des infrastructures et des chaînes d'outils en constante évolution. Repérer ces schémas permet une détection précoce des menaces.

Modèles récurrents qui signalent une phase de préparation ou d'intensification d'une offensive

Préparatifs liés aux infrastructures

Les clusters d'infrastructure associés aux attaques émergentes sont observables plusieurs semaines avant le déploiement de toute charge utile. Ils sont souvent identifiables par de nouveaux enregistrements de domaine, des anomalies de trafic ou des modèles de configuration en miroir. La mise en place de l'infrastructure de l'attaquant peut inclure:

- Des regroupements de domaines nouvellement enregistrés
- Des serveurs utilisés pour déposer les données volées (drop servers) et des systèmes de redirection
- Des configurations d'infrastructure cloud
- Des tests de charges utiles et des leurres

Réutilisation des outils d'une campagne à l'autre

Même si les indicateurs changent, les attaquants se trahissent en réutilisant des outils familiers: loaders, portes dérobées et scripts. Ces empreintes comportementales récurrentes (cartographiées via ATT&CK) se retrouvent d'une opération à l'autre. Malgré l'évolution des IOC, les attaquants réutilisent fréquemment:

- Des logiciels malveillants utilisés pour déployer des charges utiles (loaders)
- Des portes dérobées (backdoors)
- Des outils permettant de créer des tunnels réseau (tunneling)
- Des scripts permettant d'obtenir des privilèges plus élevés

Changements géographiques ou saisonniers

Les menaces connaissent généralement un pic d'activité lors de grands événements internationaux importants à l'échelle mondiale. Ces temps forts peuvent représenter des marqueurs extrêmement clairs, permettant de prévoir qui seront les prochaines cibles et quand auront lieu les attaques. Les acteurs malveillants suivent souvent:

- Les événements géopolitiques
- Les cycles budgétaires et fiscaux
- Les perturbations sur les chaînes d'approvisionnement
- Les instabilités régionales

Corrélation entre technologies opérationnelles (OT) et technologies de l'information (IT) dans les infrastructures critiques

L'ENISA met en évidence une tendance en hausse : les intrusions commencent souvent dans des environnements informatiques où les attaquants s'installent durablement, avant de se tourner vers les systèmes OT pour perturber les opérations. Une exploration précoce de l'OT (interactions inhabituelles avec les protocoles, énumération des actifs, anomalies de configuration mineures, etc.) peut révéler des problèmes plusieurs semaines avant une attaque réelle. La corrélation entre technologies informatiques et opérationnelles (IT/OT) constitue donc l'un des indicateurs d'alerte précoce les plus fiables dans la défense des infrastructures critiques.

Données empiriques sur les modèles prédictifs

Les recherches mondiales sur les cybermenaces illustrent la prévalence concrète de ces modèles dans les campagnes. Le rapport 2025 de l'ENISA sur l'état des menaces montre une convergence claire vers les techniques de repérage et de suivi, en particulier la T1059 (interpréteurs de commandes et de scripts), la T1078 (comptes valides) et la T1083 (découverte de fichiers et de répertoires). Cela confirme le fait que les attaquants conservent les mêmes comportements, alors même que les indicateurs évoluent.

Dans le même temps, l'analyse des menaces montre que le nombre de fichiers malveillants se faisant passer pour des outils d'entreprise est en train d'exploser. Plus de 1 600 échantillons différents ont copié Zoom rien qu'au cours des quatre premiers mois de 2025 (soit environ 41 % de tous les fichiers uniques sur cette période). Selon un autre rapport, plus de 389 millions d'attaques provenant de ressources web ont été bloquées en un seul trimestre. Ces enseignements soulignent la capacité des attaquants à affiner leurs modes opératoires plus rapidement que les systèmes traditionnels fondés sur des indicateurs ne peuvent les suivre. Mais les acteurs malveillants laissent également des traces qui donnent une longueur d'avance aux organisations utilisant des renseignements prédictifs sur les menaces.

Calendrier de détection prédictive (scénario à vecteurs multiples)

Cette chronologie illustre comment la Threat Intelligence contextuelle peut permettre de neutraliser une menace avant qu'elle ne se concrétise en intrusion ou violation.

T-3 semaines: **signaux infrastructurels avant-coureurs**

Un petit groupe de domaines nouvellement enregistrés apparaît, présentant des modèles de certificats et des caractéristiques d'hébergement précédemment associés à un groupe de cyberattaquants connu. Pas encore de charge utile, mais la configuration « semble familière » selon les indicateurs de similarité comportementale.

T-2 semaines: **alertes de similarité comportementale**

Les environnements « bac à sable » (sandbox) automatisés déclenchent l'exécution d'un nouveau loader ne correspondant à aucune signature. Sa séquence API, sa logique de résolution des infrastructures de commande et contrôle (C2) et ses techniques d'évasion ressemblent fortement à des outils utilisés par le même groupe dans le cadre de campagnes précédentes.

T-10 jours: **corrélation multi-sources**

Les analystes établissent une corrélation entre l'infrastructure déployée et le loader suspect. La combinaison du groupe de domaines et du recoupement comportemental indique la préparation d'une nouvelle opération.

T-7 jours: **renforcement proactif**

Les équipes de sécurité intègrent les plages d'infrastructure suspectes dans les pare-feux et enrichissent les règles des systèmes de gestion des informations et des événements de sécurité (SIEM) afin d'augmenter la priorité des alertes liées au mouvement latéral ou à l'abus d'identifiants (T1078, T1087, etc.).

T-2 jours: **tentative de repérage**

L'attaquant sonde le périmètre à partir de l'un des hôtes précédemment signalés à l'aide de modèles de détection de répertoires familiers (ex. : T1083). La tentative est automatiquement bloquée grâce à des mesures préalablement mises en place.

Résultat: **une campagne interrompue avant tout incident**

La campagne est interrompue avant qu'elle ne soit déclenchée, et ce, grâce à la corrélation de diverses données fragmentées (infrastructurelles, comportementales, historiques) afin de permettre une anticipation en amont plutôt que d'attendre l'apparition d'un IOC.

Guide pratique: ce que les responsables de la sécurité des systèmes d'information doivent faire dès maintenant

Voici sept mesures concrètes que peuvent prendre les responsables de la sécurité pour adopter une position défensive adaptée à leur contexte.

1

Cartographiez vos adversaires potentiels, pas seulement leurs indicateurs

Les IOC statiques ne révèlent pas l'identité des groupes qui ciblent votre secteur ni leurs motifs. Une cartographie permet d'en réduire intelligemment le périmètre.

Mesures à prendre:

- Identifiez les groupes malveillants les plus actifs dans votre secteur/zone géographique
- Surveillez leurs outils, leurs TTP et leurs chronologies d'attaque privilégiés
- Partez du principe qu'il s'agit de campagnes structurées en plusieurs étapes

Pourquoi est-ce important?

Le contexte révèle qui est susceptible d'attaquer, permettant d'établir des priorités de manière proactive.

2

Privilégiez la détection comportementale à celle fournie par les indicateurs

Les comportements subsistent même lorsque les indicateurs changent.

Mesures à prendre:

- Concentrez votre travail de recherche sur les TTP récurrents, et non sur les événements isolés
- Utilisez MITRE ATT&CK pour interpréter les objectifs des attaquants

Pourquoi est-ce important?

La détection comportementale dévoile les menaces émergentes avant même que les signatures ou IOC n'émergent.

3

Tirez parti du contexte pour réduire la surabondance d'alertes

L'objectif est de recevoir des alertes moins nombreuses mais plus pertinentes, sans augmenter le volume de données.

Mesures à prendre:

- Utilisez la Threat Intelligence contextuelle pour affiner vos règles et filtrer le bruit de fond parasite
- Intégrez les IOC/TTP pertinents dans les pare-feux et les passerelles afin de renforcer la défense en amont
- Mesurer les améliorations en matière de réduction des faux positifs

Pourquoi est-ce important?

Le contexte priorise exclusivement les alertes importantes pour votre environnement de travail.

4

Intégrez la Threat Intelligence à vos flux de travail existants

La Threat Intelligence apporte une valeur ajoutée lorsqu'elle est intégrée dans les opérations quotidiennes.

Mesures à prendre:

- Enrichissez les événements SIEM au moyen de métadonnées contextuelles
- Utilisez une solution d'orchestration, d'automatisation et de réponse à la sécurité (SOAR) pour automatiser les corrélations et le routage
- Repriorisez les vulnérabilités en fonction de leur probabilité d'exploitation et non uniquement de leur score de notation des vulnérabilités (CVSS)

Pourquoi est-ce important?

La Threat Intelligence contextuelle rend chaque outil (SIEM, SOAR, XDR) plus efficace et plus rapide.

5

Accélérez le travail des analystes grâce à des résumés contextuels

C'est le temps, et non les données, qui représente la ressource la plus précieuse.

Mesures à prendre:

- Normalisez les synthèses enrichies des menaces pour les enquêtes
- Systématisez des « réunions d'information préliminaires » pour toutes les alertes
- Intégrez le délai moyen d'interprétation à la liste des KPI à suivre

Pourquoi est-ce important?

Les synthèses contextuelles générées par l'IA réduisent considérablement le temps d'investigation.

6

Mesurez les progrès à l'aide de KPI opérationnels

Ne vous cantonnez pas à des notions abstraites de retour sur investissement.

KPI à privilégier:

- MTTA: temps moyen nécessaire pour qu'une équipe ou un individu prenne conscience d'un incident ou d'un événement particulier après qu'il se soit produit
- Taux de réduction des faux positifs
- Pourcentage d'alertes résolues avant l'escalade de l'offensive
- Pourcentage de menaces associées à des TTP connus

Pourquoi est-ce important?

Ces indicateurs montrent une progression tangible et mesurable vers davantage de résilience.

7

Utilisez des éclairages issus de plusieurs perspectives

Aucune source unique ne permet d'obtenir une vision globale.

Mesures à prendre:

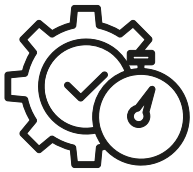
- Combinez au moins deux sources de renseignements indépendantes
- Procédez à une validation croisée avant de donner suite

Pourquoi est-ce important?

Le croisement de diverses sources internationales permet de mettre au jour des relations cachées entre les attaquants. Des corrélations qu'un unique fournisseur de services pourrait échouer à détecter.

Comment mesurer la progression vers une défense proactive

Les organisations doivent mesurer les progrès réalisés en considérant:



L'efficacité

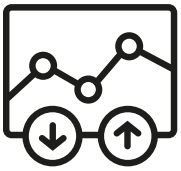
Les équipes proactives réduisent les délais entre la détection, l'interprétation et le passage à l'action. Ces améliorations reflètent l'impact de l'enrichissement contextuel, qui élimine le travail de corrélation manuel et accélère la prise de décision. Au nombre des KPI figurent:

- La réduction du délai moyen de réparation (Mean Time to Repair)
- L'accélération du triage pour les analystes
- L'allègement des coûts d'investigation

La précision

À mesure que la Threat Intelligence contextuelle gagne en maturité, les alertes SIEM se font plus précises, le nombre de vulnérabilités en attente de traitement diminue et davantage d'incidents sont résolus avant qu'ils ne prennent de l'ampleur. La précision augmente car les informations non pertinentes sont filtrées avant d'atteindre les analystes. Au nombre des indicateurs de précision figurent:

- La réduction des faux positifs
- Une priorisation plus précise et plus fiable
- Une attribution plus claire des attaques



L'anticipation

Le marqueur le plus fort de maturité en matière de proactivité est l'augmentation du nombre de détections liées au comportement des attaquants plutôt qu'aux indicateurs ne ressortant qu'aux derniers stades d'une intrusion. Cette donnée reflète le passage d'une réponse réactive aux attaques à la capacité de les désamorcer dès leur phase préparatoire:

- Augmentation des mesures préventives d'atténuation des risques
- Détection plus précoce du déploiement d'infrastructures menaçantes
- Augmentation des alertes liées aux TTP des acteurs plutôt qu'à des IOC individuels

Modèle de montée en maturité en matière de Threat Intelligence contextuelle

Voici un cadre pratique que les responsables de la sécurité des systèmes d'information peuvent utiliser pour évaluer leur progression, de la détection réactive à la défense prédictive.

NIVEAU 1

Réactif (fondé sur les indicateurs)

Approche dominante:

Réagir après la compromission

Base de détection:

IOC statiques, journaux rétrospectifs

Caractéristiques:

- Volume d'alertes élevé, faible priorisation
- Faux positifs fréquents
- Enrichissement manuel chronophage pour les analystes
- OT et IT suivis séparément
- Peu de visibilité sur les modèles ou les intentions des attaquants

Résultats:

- Lenteur du traitement et de la classification
- Signaux d'alerte précoces passés inaperçus
- Perturbations répétées dues à des types d'attaques similaires

NIVEAU 2

Amélioré (corrélé mais toujours fragmenté)

Approche dominante:

Réponse plus rapide, mais toujours réactive

Base de détection:

Corrélations partielles entre des événements liés

Caractéristiques:

- Règles SIEM enrichies manuellement
- Premiers efforts de cartographie ATT&CK
- Reconnaissance occasionnelle des modèles comportementaux
- Premières corrélations entre les alertes OT/IT dans les situations à forte incidence
- Réduction partielle des faux positifs

Résultats:

- Réponse plus rapide qu'au niveau 1
- Persistance de la dépendance aux analystes pour reconstituer le contexte
- Capacité limitée à anticiper les attaques

NIVEAU 3

Contextuel (prenant en compte les comportements)

Approche dominante:

Détection précoce et priorisation éclairée

Base de détection:

Similarités comportementales, groupes de TTP, pertinence environnementale et conjoncturelle

Caractéristiques:

- Cyber-renseignements cartographiés conformément au cadre ATT&CK
- Recoupements des comportements pour identifier les TTP récurrents
- Priorisation sur la base de similarités entre les campagnes
- Analyses OT/IT révélant les premières tentatives de pivots
- Délais d'inspection et d'analyse considérablement réduits grâce à l'enrichissement contextuel

Résultats:

- Activités hautement prioritaires identifiées plus en amont
- Moins d'intensification d'attaques
- Attribution plus claire des attaques et réduction du bruit parasite
- Détection des premiers signes de préparatifs d'une attaque avant l'exploitation de failles

NIVEAU 4

Prédictif (défense axée sur les intentions)

Approche dominante:

Désorganiser les campagnes en cours de préparation

Base de détection:

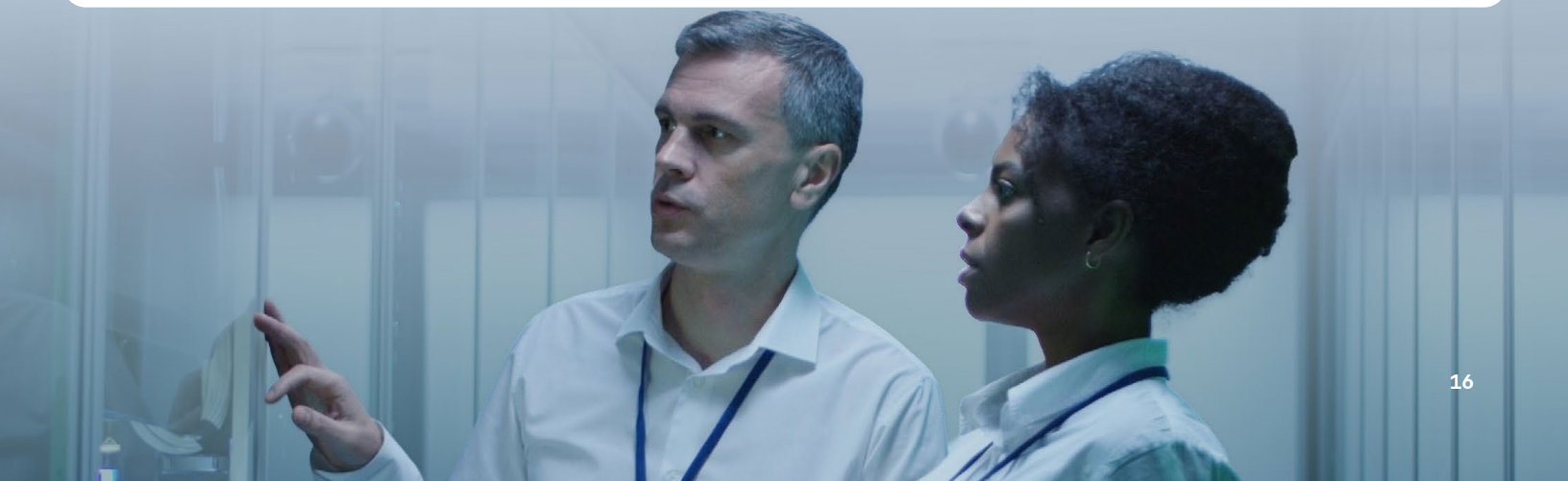
Corrélation multi-sources révélant les intentions et les mécanismes de préparation infrastructurelle

Caractéristiques:

- Enrichissement, grâce à l'IA, des signaux indiquant la réutilisation de logiciels malveillants, de domaines et d'infrastructures
- Interprétation par les analystes des signaux comportementaux et géopolitiques
- Renforcement proactif déployé avant les tentatives d'exploitation de failles
- Vision claire des acteurs, des secteurs et des vulnérabilités les plus importants actuellement
- Corrélations OT/IT détectant les repérages précoces plusieurs semaines avant une attaque

Résultats:

- Campagnes neutralisées avant qu'elles ne soient déclenchées
- Réduction du nombre d'incidents parvenant à la phase d'accès initial
- La sécurité devient proactive plutôt que réactive
- L'organisation renforce considérablement sa confiance en la résilience de sa cybersécurité



L’avenir de la cyberdéfense intelligente à l’ère de l’IA

L’utilisation de l’IA par des acteurs malveillants est en train de profondément métamorphoser le panorama des menaces. Les attaquants utilisent désormais des modèles génératifs pour automatiser les repérages, cartographier les environnements OT, créer des campagnes d’hameçonnage polymorphes à grande échelle et générer des variantes de logiciels malveillants en constante mutation qui échappent aux méthodes de détection traditionnelles. Les données rapportées par Securelist montrent déjà une forte croissance des comportements augmentés par l’IA: séries à rythme rapide de campagnes d’hameçonnage sur mesure pour cibler des organisations spécifiques, loaders et serveurs de dépôt automatiquement modifiés, sans oublier des opérations de bourrage d’identifiants capables d’adapter en continu leur ciblage et leur cadence. Ces techniques permettent aux attaquants de compresser de manière drastique les délais de leurs campagnes, laissant aux défenseurs de moins en moins de temps pour détecter les premiers signaux.

Dans cette nouvelle réalité, l’analyse contextuelle devient le seul atout réellement pérenne. L’analyse des corrélations comportementales et infrastructurelles ainsi que des similarités entre campagnes révèle des modèles récurrents que les indicateurs générés par l’IA sont impuissants à masquer: mécanismes familiers de C2, habitudes de repérage, sondages OT répétés et réutilisation des infrastructures d’une itération à l’autre.

L’avenir de la cyberdéfense s’articule autour de la combinaison de l’enrichissement des signaux permis par l’IA et de l’interprétation humaine afin de comprendre les intentions des attaquants avant qu’ils ne passent à l’action. En développant cette vision prospective dès aujourd’hui, les responsables de la sécurité se placent en situation d’affronter non seulement les menaces immédiates, mais aussi les offensives augmentées par l’IA qui se profilent à l’horizon.

Kaspersky Threat Intelligence

Kaspersky possède des connaissances approfondies, une vaste expérience dans la recherche sur les cybermenaces et une expertise unique dans tous les aspects de la cybersécurité. Cela a fait de Kaspersky un partenaire de confiance des forces de l'ordre et des organisations gouvernementales du monde entier, notamment Interpol et diverses unités CERT. Kaspersky Threat Intelligence fournit une Threat Intelligence tactique, opérationnelle et stratégique actualisée sur les menaces. En savoir plus

DEMANDER DES INFORMATIONS COMPLÉMENTAIRES