Fiche produit

Exposure Analysis and Response (ExAR) pour Akamai Guardicore Segmentation

Les environnements d'entreprise évoluent en permanence et, au fil des changements, les périmètres de sécurité statiques finissent inévitablement par ne plus refléter la réalité opérationnelle. Les attaquants exploitent ces failles structurelles. Ils utilisent désormais l'intelligence artificielle pour réduire le délai traditionnel entre la découverte d'une vulnérabilité et son exploitation, le faisant passer de plusieurs semaines à environ 20 heures. Les correctifs appliqués à un rythme humain et les périmètres de sécurité statiques ne sont plus en mesure de suivre les activités de reconnaissance automatisées, les exploitations assistées par l'IA et les mouvements latéraux automatisés.

Les capacités **Exposure Analysis and Response (ExAR)** d'Akamai Guardicore Segmentation transforment la microsegmentation en couche de sécurité dynamique et active, au lieu d'un contrôle réseau statique.

Grâce à l'intégration de la détection des menaces et de la visibilité sur l'exposition aux risques à notre méthodologie, la plateforme offre une cartographie continue de la surface d'attaque, une détection comportementale automatisée et une réponse à la vitesse des machines.

Cette approche en boucle fermée permet à votre équipe de sécurité de valider en continu l'efficacité des règles, d'identifier immédiatement les chaînes d'attaque actives, de mettre en quarantaine les actifs vulnérables à la vitesse des machines et de déjouer automatiquement les attaques avant qu'elles ne compromettent votre activité.

Principal défi : l'asymétrie des chemins de communication connectés

La plupart des équipes de sécurité doivent gérer des signaux individuels et déconnectés les uns des autres, tandis que les attaquants se concentrent sur la recherche et l'exploitation des chemins menant à vos données. Les couches de défense classiques ne parviennent pas à isoler les risques réels pour plusieurs raisons :

- **Les silos de visibilité rompent le contexte.** Les solutions de gestion de l'exposition, de détection et de réponse, ainsi que les solutions de segmentation traditionnelles, fonctionnent souvent de manière isolée et ne communiquent pas entre elles. Pour obtenir une vision complète du rayon d'impact d'une attaque, il faut corréler les détections au niveau du réseau, de l'hôte et de l'identité avec la portée réelle offerte par la segmentation.
- **La gravité ne reflète pas nécessairement l'exploitabilité.** Grâce à l'IA, les attaquants peuvent cibler des vulnérabilités pourtant considérées comme peu critiques pour causer des dommages majeurs. Les approches de gestion des vulnérabilités fondées sur leur niveau de gravité ou leur exploitabilité théorique ne permettent pas de mettre en évidence les vulnérabilités qui demeurent exposées en raison des failles de segmentation. Les solutions de segmentation traditionnelles ne disposent pas de capacités natives de détection des vulnérabilités, ce qui permet aux attaquants de tirer avantage des faiblesses présentes au sein des règles.

Avantages pour votre entreprise

Prioriser les risques réels
Évaluez l'exposition à l'aide d'un calcul multidimensionnel des risques basé sur l'exploitabilité réelle et le contexte métier. Isolez instantanément la fraction des chemins d'accès réseau qui représente la menace la plus élevée pour vos actifs les plus critiques.

Déjouer les attaques à la vitesse des machines
Neutralisez les activités malintentionnées post-exploitation, les mouvements latéraux malveillants et les outils d'IA non autorisés grâce à des défenses actives et natives. Mettez en œuvre des mesures de protection, telles que la mise en quarantaine immédiate des actifs vulnérables directement à la couche applicative, sans latence opérationnelle.

Détecter les activités malveillantes
Remplacez le triage d'alertes passives par des incidents fiables et entièrement corrélés, regroupant les informations des hôtes, des processus, des identités et du réseau au sein d'une chaîne d'attaque incontestable.

Maintenir une stratégie efficace
Passez de tests de configuration ponctuels à une boucle continue et automatisée de rétroaction. Vérifiez en permanence que les règles Zero Trust appliquées contiennent les menaces et empêchent les mouvements latéraux de manière efficace.

Akamai Security

- **Les règles statiques deviennent obsolètes.** Les exceptions de règles, la prolifération des ressources cloud, la compromission des identités et les actifs non gérés affectent en permanence la réalité des architectures Zero Trust. Sans validation continue et automatisée, la segmentation n'apporte qu'une illusion théorique de protection.

À l'ère des menaces accélérées par l'IA, s'en remettre à des audits manuels et à des règles statiques expose les entreprises à des risques élevés. Avec ExAR, Akamai Guardicore Segmentation intègre une validation continue de la réalité à votre stratégie de confinement. Cette nouvelle approche vise à faire passer vos équipes d'un mode de lutte permanente contre les incidents à une maîtrise proactive et durable de votre véritable surface d'attaque interne.

Boucle de segmentation qui tient compte de l'exposition

ExAR fournit une protection de bout en bout à travers un cycle continu en trois étapes et en boucle fermée :

1. Compréhension et analyse

ExAR modélise le chemin d'attaque exact qu'un adversaire pourrait emprunter dans votre environnement. En combinant la découverte continue des actifs observés sur le réseau, la télémétrie des hôtes, le contexte des identités et les vulnérabilités logicielles connues, la plateforme calcule le risque réel auquel votre entreprise serait exposée si le chemin d'attaque concerné n'était pas traité.

2. Détection des activités

L'**outil intégré d'investigation des menaces basé sur l'IA** va au-delà des risques théoriques et des règles statiques.
Il détecte automatiquement les activités suspectes et corrèle la télémétrie provenant de plusieurs domaines afin d'identifier les comportements réels d'un attaquant.

- **Informations sur les menaces et indicateurs de compromission :** s'appuie sur les informations mondiales d'Akamai et les indicateurs de compromission (IOC) pour identifier les menaces.
- **Détection avancée des menaces :** détections comportementales natives alignées sur le cadre MITRE pour identifier les activités malveillantes furtives.
- **Analyse des attaques interdomaines :** corrèle les événements de sécurité à travers les frontières réseau, les référentiels d'identités et les points de terminaison.
- **Détection des mouvements latéraux :** identifie les mouvements internes suspects avant l'exfiltration des données.

ExAR fournit ces capacités avancées sans agent supplémentaire, sans surcharge de ressources ni pics d'utilisation du CPU sur vos serveurs de production.

3. Défense active

Lorsqu'une violation des frontières ou une technique de compromission post-exploitation est confirmée, ExAR offre aux équipes de sécurité des plans de réponse rapide et des outils automatisés d'atténuation des risques. Les défenses peuvent être adaptées immédiatement grâce à un blocage dynamique en bordure de l'Internet via un pare-feu DNS natif, au déploiement de pots de miel pour détourner et épuiser les outils d'attaque automatisés, à l'ajustement des règles de segmentation pour fermer les chemins d'accès vulnérables, et à l'isolation des actifs vulnérables au moyen de contrôles réseau.

Là où la solution s'intègre le mieux

Akamai Guardicore Segmentation avec EXAR est idéal pour les cas d'usage suivants :

Entreprises confrontées à des attaques accélérées par l'IA
Les entreprises qui reconnaissent que l'application de correctifs au rythme des humains et les pare-feux de blocage des ports hérités ne suffisent pas face à des fenêtres d'attaque de moins de 24 heures.

Équipes SecOps souffrant d'une surcharge d'alertes
Les équipes de sécurité qui doivent s'adapter à la réalité d'aujourd'hui en priorisant les risques et les menaces selon leur exploitabilité réelle afin de protéger les actifs les plus critiques.

Responsables de la sécurité souhaitant moderniser leur stratégie de segmentation
Les entreprises qui recherchent une segmentation capable de résister aux menaces futures en prenant en compte la prolifération des capacités offensives renforcées par l'IA dès le premier jour.

Infrastructures hybrides sensibles
Les environnements fortement réglementés (services financiers, santé ou production manufacturière) qui doivent avoir la certitude que les modifications de sécurité n'interrompront pas la disponibilité des systèmes de production.

Programmes Zero Trust en phase de maturité
Les entreprises qui souhaitent ajouter une couche continue de validation afin de s'assurer que les frontières de leur réseau restent efficaces à mesure que les applications et les configurations de conteneurs évoluent.

Offres optimisées basées sur les actifs

Aujourd'hui, face à des attaques accélérées par l'IA et à des menaces capables d'adapter leurs tactiques en temps réel, déployer une segmentation sans cartographie continue de l'exposition crée une faille de sécurité inacceptable.

Pour garantir l'efficacité de vos frontières de sécurité lorsque les mécanismes de prévention échouent, chaque déploiement d'Akamai Guardicore Segmentation peut intégrer un package ExAR complet couvrant l'ensemble de l'infrastructure de l'entreprise dès le premier jour.

Tableau des fonctionnalités

Capacité	Plus	Premier
Incidents corrélés fiables (TTP MITRE, données d'analyse approfondies)	✓	✓
Détection télémétrique interdomaine (hôte, réseau, identité)	✓	✓
Tableau de bord interactif d'exposition (analyse complète de la stratégie)	✓	✓
Outil d'investigation des menaces basé sur l'IA agentique (détection et raisonnement autonomes)	✓	✓
Actions recommandées (mesures de réponse adaptées au contexte)	✓	✓
Visibilité approfondie au niveau de l'hôte (télémétrie de requêtes intégrée)	✓	✓
Intégration des informations sur les menaces d'Akamai (flux de renseignements mondiaux)	✓	✓
Recherche des menaces menée par des analystes humains 24 h/24, 7 j/7 (enquêtes réalisées par des experts)	⊘	✓
Coordination de l'assistance en direct (accompagnement en temps réel lors des incidents)	⊘	✓
Protection par pare-feu DNS en bordure de l'Internet (défense en profondeur)	Module complémentaire disponible	✓
Leurres de type pots de miel dynamiques (neutralisation à la vitesse des machines)	Module complémentaire disponible	✓

Résultats concrets observés sur le terrain

Étude de cas n° 1 : arrêt d'un abus de privilèges et d'activités de reconnaissance furtives

- **Environnement :** fabricant multinational de produits électroniques
- **Incident :** un attaquant a compromis un compte interne à privilèges, a acheminé du trafic SSH via des ports inhabituels pour contourner les mécanismes de détection et a téléchargé un exécutable personnalisé de découverte du réseau.
- **Apport d'ExAR :** la télémétrie approfondie d'ExAR a identifié le téléchargement furtif d'un exécutable suspect malgré une activité réseau normale. Son moteur d'analyse interdomaine a attribué l'activité de reconnaissance réseau à l'exécutable et à l'utilisateur concernés. ExAR a alors généré un incident de gravité élevée et recommandé explicitement des règles de segmentation visant à fermer le chemin d'attaque ciblé.

Étude de cas n° 2 : atténuation d'une compromission d'Active Directory

- **Environnement :** important organisme d'assurance maladie
- **Incident :** des attaquants ont utilisé l'infrastructure Cobalt Strike pour déployer rapidement 10 services Windows aléatoires. Ces services ont récupéré les identifiants, énuméré les configurations de répertoire et collecté des fichiers de bases de données Azure AD.
- **Apport d'ExAR :** les structures d'alerte traditionnelles ont généré une série d'événements mineurs et déconnectés les uns des autres. ExAR a instantanément regroupé les 10 actions post-exploitation en une chaîne d'attaque cohérente, validé l'existence d'une menace active et recommandé des limites de microsegmentation spécifiques pour empêcher l'attaquant d'atteindre son objectif.

Gardez une longueur d'avance sur les menaces accélérées par l'IA. Demandez une démonstration dès aujourd'hui.

© 2026 Akamai Technologies | Assistance |
| Publication : 08/26