Solutions par secteur d'activité

Comment la prévention autonome s'applique à des secteurs spécifiques - santé, industrie manufacturière et OT, services financiers, gouvernement, éducation, secteur maritime et fournisseurs de services gérés.

- Comment Cyber Crucible protège-t-il les environnements de fabrication, OT et ICS ?
- Comment Cyber Crucible protège-t-il les entreprises de services financiers ?
- Comment Cyber Crucible prend-il en charge les environnements gouvernementaux et à haute sécurité ?
- Cyber Crucible peut-il protéger les navires et les opérations à distance ou déconnectées ?
- Pourquoi les MSP et les revendeurs s'associent-ils à Cyber Crucible ?
- Nous avons récemment subi une violation. Cyber Crucible peut-il être déployé dans un environnement potentiellement déjà compromis ?

Comment Cyber Crucible protège-t-il les environnements de fabrication, OT et ICS ?

Réponse courte : La solution s'exécute entièrement sur le poste (endpoint), sans aucune dépendance au cloud, ce qui lui permet de protéger les technologies opérationnelles et les systèmes de contrôle industriel qui sont hors ligne, isolés (air-gapped) ou connectés de manière intermittente — et elle ne suspend que le processus malveillant, de sorte que la production continue.

Pourquoi les outils conventionnels peinent ici

Les environnements OT et ICS ne peuvent tolérer ni un aller-retour vers le cloud ni un verrouillage complet du réseau. Beaucoup sont volontairement déconnectés. Les modèles de sécurité qui supposent une connectivité constante et un SOC distant ne s'appliquent tout simplement pas.

Ce qui change

- **Fonctionnement 100 % hors ligne** — protection complète sans signal requis, prête pour les environnements isolés (air-gap).
- **Aucun verrouillage** — les processus malveillants sont suspendus en mémoire pendant que la production se poursuit.
- **Un seul agent pour l'ensemble de l'environnement** — le même agent léger protège les automates (PLC) sur le site de production, les véhicules d'un réseau logistique et les navires en mer, sans intervention d'analyste et sans hypothèse de connectivité.

Comment Cyber Crucible protège-t-il les entreprises de services financiers ?

Réponse courte : Il stoppe les infostealers et le vol de jetons de session au niveau du noyau, avant même que l'exfiltration ne commence, et il analyse tout localement afin que les clés et les jetons n'aient jamais à être téléchargés vers un cloud tiers.

La menace à laquelle les entreprises financières sont réellement confrontées

Des attaques hyper-automatisées de type « smash and grab » ciblent les jetons de session et les clés API. Elles passent de l'infiltration à l'auto-suppression en quelques secondes — plus vite qu'une alerte cloud ne peut quitter les locaux. Un jeton de session volé contourne souvent entièrement les mots de passe et la MFA, offrant à un attaquant un moyen d'accès apparemment légitime à tout moment.

Le cas documenté

Une importante entreprise de services financiers exploitait trois solutions EDR parmi les meilleures du secteur ainsi qu'un MSSP externalisé faisant partie du Top 50. Cyber Crucible a été déployé pour identifier l'angle mort. En 60 jours, il avait intercepté de manière autonome près de 10 000 processus malveillants — 98 % d'entre eux sur la ferme de serveurs Microsoft SQL hautement privilégiés de l'entreprise — sans aucune alerte de la part de la pile de sécurité existante.

La cause racine a été retracée jusqu'à un identifiant de surveillance à distance probablement compromis. Des mois plus tard, le secteur a signalé une vague mondiale de ransomware installant des portes dérobées sur des serveurs SQL à travers le monde. Le secteur financier a subi de graves violations. Ce client n'en a jamais été victime.

Comment Cyber Crucible prend-il en charge les environnements gouvernementaux et à haute sécurité ?

Réponse courte : Grâce à une souveraineté totale des données — installation entièrement sur site dans des racks physiquement sécurisés, fonctionnement en air gap et architecture multi-tenant — sans cloud public, sans SOC tiers et sans partage de données.

Souveraineté par architecture

Pour les organisations exigeant un contrôle absolu, aucune donnée n'a besoin de quitter l'environnement. Il n'y a aucune plateforme tierce dans le circuit, aucun accès externe, et aucune analyse de vos données hébergée par le fournisseur.

Cela compte, car de nombreux fournisseurs téléchargent des données d'identité sensibles — clés privées, jetons de session — vers leurs équipes SOC hébergées. Ce stockage centralisé constitue un point de défaillance unique et une cible de grande valeur pour les attaquants soutenus par des États, et il peut être atteint par contrainte légale à votre insu.

Discret par défaut

Les menaces sont neutralisées silencieusement au niveau du noyau. Vous seul savez qu'une attaque a été tentée, et si aucune donnée n'a été touchée, il n'y a généralement aucune alerte externe ni aucune divulgation requise.

Multi-tenant

L'architecture prend en charge les déploiements multi-tenant, ce qui convient à la gestion de plusieurs départements ou agences depuis une seule instance sécurisée sur site.

Cyber Crucible peut-il protéger les navires et les opérations à distance ou déconnectées ?

Réponse courte : Oui, et cela a déjà été démontré. Lors d'un déploiement maritime, Cyber Crucible a fonctionné de manière autonome pendant des traversées de plusieurs jours sans aucun personnel informatique à bord, s'adaptant à des liaisons satellite à faible bande passante et à de longues périodes de déconnexion, tout en protégeant aussi bien les terminaux passagers que les systèmes de contrôle maritime critiques.

Ce que le déploiement a démontré

- **Réponse autonome** sans équipe informatique présente pendant plusieurs jours d'affilée.
- **Fonctionnement adapté au satellite** sur des liaisons instables, à faible bande passante et sujettes aux interruptions météorologiques.
- **Conservation des données à des fins d'analyse judiciaire** — des journaux détaillés préservés malgré la déconnexion, pour une analyse post-traversée.
- **Résilience face aux attaques** — le système a tenu bon lorsque des adversaires ont tenté de le désactiver ou de dégrader ses performances.

L'élément inhabituel

Les journaux ont révélé une activité compatible avec l'implication d'un État-nation, et le ciblage était sélectif : seuls les navires opérant en eaux internationales étaient touchés, tandis que les navires d'excursion nationaux restaient épargnés.

Lorsque les tentatives d'intrusion classiques ont échoué, les adversaires sont montés en puissance — détournant les identifiants de connexion Windows, puis accédant aux paramètres au niveau du BIOS pour verrouiller les systèmes avant le démarrage. Même avec des systèmes bloqués avant que le système d'exploitation ne puisse se charger, le déploiement a continué de tenir la ligne là où les piles de sécurité traditionnelles avaient déjà échoué.

Pourquoi les MSP et les revendeurs s'associent-ils à Cyber Crucible ?

Réponse courte : Parce que la prévention autonome permet à un partenaire de conserver la marge, la relation client et le SLA — au lieu de revendre un SOC hébergé par un éditeur et d'endosser la responsabilité lorsque ce SOC manque une attaque à vitesse machine.

Le piège de la revente de la détection

Le secteur a poussé les partenaires à revendre des services MDR et SOC hébergés par des éditeurs. Lorsque la surveillance pilotée par des humains manque inévitablement une attaque automatisée, c'est l'éditeur qui manque la brèche — mais ce n'est pas lui que le client renvoie. C'est le partenaire.

Ce qui change sur le plan opérationnel

- Les menaces sont neutralisées instantanément, avant même que les analystes ne reçoivent une alerte.
- Le volume d'alertes chute considérablement par rapport aux plus de 100 alertes par terminal et par jour à l'origine de la fatigue liée aux alertes.
- Aucun réglage de règles YARA ni chasse aux menaces manuelle.
- Les partenaires captent le flux de revenus au lieu de se contenter de commissions d'éditeur.

Et du côté du risque

Un partenaire dont l'offre de sécurité empêche les attaques plutôt que de simplement les documenter engage une conversation fondamentalement différente avec ses clients sur les résultats et la responsabilité.

Nous avons récemment subi une violation. Cyber Crucible peut-il être déployé dans un environnement potentiellement déjà compromis ?

Réponse courte : Oui. Cyber Crucible évalue ce que les programmes font en temps réel plutôt que de rechercher des fichiers connus comme malveillants ; il commence donc à bloquer les comportements malveillants dès son déploiement — y compris ceux d'un attaquant déjà présent dans l'environnement.

Pourquoi une compromission préalable ne l'aveugle pas

Comme la prévention repose sur l'intention comportementale au niveau du noyau, un attaquant déjà présent doit tout de même *agir* — accéder aux données d'identité, s'injecter dans des processus, commencer un chiffrement ou exfiltrer des données. Ce sont précisément ces actions qui déclenchent l'interception.

C'est ainsi que le déploiement dans le secteur des services financiers a révélé une intrusion active et en cours que la pile de sécurité existante n'avait jamais détectée. Cyber Crucible n'a pas été déployé pour enquêter sur une violation connue ; il a été déployé pour rechercher un angle mort, et il a découvert près de 10 000 processus malveillants déjà en cours.

À quoi s'attendre

Le déploiement dans un environnement compromis produit souvent une activité d'interception immédiate et de grande ampleur. C'est l'outil qui fonctionne comme prévu, et il s'agit fréquemment de la première preuve tangible pour une organisation qu'une activité malveillante était déjà en cours.