Branchenlösungen

Wie autonome Prävention auf spezifische Branchen angewendet wird – Gesundheitswesen, Fertigung und OT, Finanzdienstleistungen, Behörden, Bildungswesen, Seeschifffahrt und Managed Service Provider.

- Wie schützt Cyber Crucible Fertigungs-, OT- und ICS-Umgebungen?
- Wie schützt Cyber Crucible Finanzdienstleistungsunternehmen?
- Wie unterstützt Cyber Crucible Regierungs- und Hochsicherheitsumgebungen?
- Kann Cyber Crucible Schiffe und abgelegene oder unterbrochene Betriebsabläufe schützen?
- Warum arbeiten MSPs und Reseller mit Cyber Crucible zusammen?
- Wir wurden kürzlich kompromittiert. Kann Cyber Crucible in einer möglicherweise bereits kompromittierten Umgebung bereitgestellt werden?

Wie schützt Cyber Crucible Fertigungs-, OT- und ICS-Umgebungen?

Kurzantwort: Die Lösung läuft vollständig auf dem Endpunkt ohne Cloud-Abhängigkeit und schützt so operative Technologien und industrielle Steuerungssysteme, die offline, luftisoliert (air-gapped) oder nur zeitweise verbunden sind — und sie unterbricht ausschließlich den bösartigen Prozess, sodass die Produktion weiterläuft.

Warum herkömmliche Tools hier an ihre Grenzen stoßen

OT- und ICS-Umgebungen können weder einen Cloud-Umweg noch eine vollständige Netzwerksperrung tolerieren. Viele sind bewusst getrennt vom Netz. Sicherheitsmodelle, die von ständiger Konnektivität und einem entfernten SOC ausgehen, greifen hier schlicht nicht.

Was sich ändert

- **100 % offlinefähig** — vollständiger Schutz ohne erforderliches Signal, bereit für den Air-Gap-Einsatz.
- **Keine Systemsperrungen** — bösartige Prozesse werden im Arbeitsspeicher unterbrochen, während die Produktion weiterläuft.
- **Ein Agent für die gesamte Umgebung** — derselbe schlanke Agent schützt SPS-Steuerungen auf dem Werksboden, Fahrzeuge in einem Logistiknetzwerk und Schiffe auf See, ganz ohne Analysten im Prozess und ohne Annahmen zur Konnektivität.

Wie schützt Cyber Crucible Finanzdienstleistungsunternehmen?

Kurze Antwort: Es stoppt Infostealer und den Diebstahl von Sitzungs-Tokens auf Kernel-Ebene, bevor die Exfiltration beginnt, und analysiert alles lokal, sodass Schlüssel und Tokens niemals in eine Cloud eines Drittanbieters hochgeladen werden müssen.

Die Bedrohung, mit der Finanzunternehmen tatsächlich konfrontiert sind

Hyperautomatisierte „Smash-and-Grab“-Angriffe zielen auf Sitzungs-Tokens und API-Schlüssel ab. Sie bewegen sich innerhalb von Sekunden von der Infiltration bis zur Selbstlöschung — schneller, als eine Cloud-Warnung das Gebäude verlassen kann. Ein gestohlenes Sitzungs-Token umgeht oft Passwörter und MFA vollständig und verschafft einem Angreifer jederzeit einen scheinbar legitimen Weg zurück in das System.

Der dokumentierte Fall

Ein großes Finanzdienstleistungsunternehmen betrieb drei branchenführende EDR-Lösungen und einen ausgelagerten Top-50-MSSP. Cyber Crucible wurde eingesetzt, um den blinden Fleck zu finden. Innerhalb von 60 Tagen hatte es autonom fast 10.000 bösartige Prozesse abgefangen — 98 % davon auf der hochprivilegierten Microsoft-SQL-Server-Farm des Unternehmens — ohne jegliche Warnung durch die bestehenden Altsysteme.

Die Ursache ließ sich auf eine wahrscheinlich kompromittierte Anmeldeinformation für die Fernüberwachung zurückführen. Monate später berichtete die Branche über eine weltweite Ransomware-Welle, die SQL-Server durch Backdoors weltweit kompromittierte. Der Finanzsektor erlitt schwerwiegende Sicherheitsverletzungen. Dieser Kunde wurde nie zum Opfer.

Wie unterstützt Cyber Crucible Regierungs- und Hochsicherheitsumgebungen?

Kurzantwort: Durch vollständige Datensouveränität — vollständig lokale Installation in physisch gesicherten Racks, luftgetrennter (Air-Gapped) Betrieb und Multi-Tenant-Architektur — ohne Public Cloud, ohne SOC eines Drittanbieters und ohne Datenaustausch.

Souveränität durch Architektur

Für Organisationen, die absolute Kontrolle benötigen, muss nichts die Umgebung verlassen. Es gibt keine Drittanbieter-Plattformen im Ablauf, keinen externen Zugriff und keine vom Anbieter gehostete Analyse Ihrer Daten.

Dies ist von Bedeutung, da viele Anbieter sensible Identitätsdaten — private Schlüssel, Sitzungstoken — an ihre gehosteten SOC-Teams hochladen. Diese zentralisierte Speicherung stellt einen Single Point of Failure und ein hochwertiges Ziel für staatlich unterstützte Angreifer dar und kann durch rechtlichen Zwang ohne Ihr Wissen erreicht werden.

Standardmäßig unauffällig

Bedrohungen werden auf Kernel-Ebene lautlos neutralisiert. Nur Sie wissen, dass ein Angriff versucht wurde, und wenn keine Daten berührt wurden, gibt es typischerweise keine externen Warnungen oder erforderliche Offenlegungen.

Multi-Tenant

Die Architektur unterstützt Multi-Tenant-Bereitstellungen, was sich für die Verwaltung mehrerer Abteilungen oder Behörden von einer einzigen sicheren lokalen Instanz aus eignet.

Kann Cyber Crucible Schiffe und abgelegene oder unterbrochene Betriebsabläufe schützen?

Kurze Antwort: Ja, und das wurde bereits unter Beweis gestellt. Bei einem maritimen Einsatz arbeitete Cyber Crucible über mehrtägige Fahrten hinweg autonom, ohne dass IT-Personal an Bord war, und passte sich an Satellitenverbindungen mit geringer Bandbreite sowie lange Phasen ohne Verbindung an – dabei wurde alles geschützt, von Passagierterminals bis hin zu unternehmenskritischen maritimen Steuerungssystemen.

Was der Einsatz gezeigt hat

- **Autonome Reaktion** ohne anwesendes IT-Team über mehrere Tage hinweg.
- **Satellitenfähiger Betrieb** über unregelmäßige, bandbreitenschwache und wetterbedingt unterbrochene Verbindungen.
- **Forensische Aufbewahrung** — umfangreiche Protokolle blieben trotz Verbindungsabbruch für die Analyse nach der Fahrt erhalten.
- **Widerstandsfähigkeit unter Angriff** — das System hielt stand, als Angreifer versuchten, es abzuschalten oder seine Leistung zu beeinträchtigen.

Der ungewöhnliche Teil

Die Protokolle zeigten Aktivitäten, die auf die Beteiligung eines Nationalstaats hindeuteten, wobei das Vorgehen selektiv war: Betroffen waren ausschließlich Schiffe, die in internationalen Gewässern unterwegs waren, während inländische Ausflugsschiffe unangetastet blieben.

Als konventionelle Eindringversuche scheiterten, eskalierten die Angreifer — sie kaperten Windows-Anmeldedaten und griffen anschließend auf BIOS-Ebene zu, um Systeme bereits vor dem Booten zu sperren. Selbst als Systeme angehalten wurden, bevor das Betriebssystem laden konnte, hielt der Einsatz weiterhin stand, wo herkömmliche Sicherheitslösungen bereits versagt hatten.

Warum arbeiten MSPs und Reseller mit Cyber Crucible zusammen?

Kurze Antwort: Weil autonome Prävention es einem Partner ermöglicht, die Marge, die Kundenbeziehung und das SLA selbst zu kontrollieren – anstatt ein vom Anbieter gehostetes SOC weiterzuverkaufen und die Schuld zu tragen, wenn dieses SOC einen Angriff mit Maschinengeschwindigkeit übersieht.

Die Falle beim Weiterverkauf von Detection

Die Branche hat Partner dazu gedrängt, vom Anbieter gehostete MDR- und SOC-Dienste weiterzuverkaufen. Wenn die menschengesteuerte Überwachung zwangsläufig einen automatisierten Angriff übersieht, verpasst der Anbieter den Vorfall – und der Kunde entlässt nicht den Anbieter. Er entlässt den Partner.

Was sich operativ ändert

- Bedrohungen werden sofort neutralisiert, bevor Analysten überhaupt eine Warnmeldung erhalten.
- Das Alarmvolumen sinkt drastisch gegenüber den 100+ Warnmeldungen pro Endpunkt und Tag, die zu Alarmmüdigkeit führen.
- Kein Feintuning von YARA-Regeln und keine manuelle Bedrohungssuche.
- Partner erschließen sich den Umsatzstrom selbst, anstatt sich mit Anbieterprovisionen zu begnügen.

Und in Bezug auf das Risiko

Ein Partner, dessen Sicherheitsangebot Angriffe verhindert, anstatt sie lediglich zu dokumentieren, führt mit seinen Kunden ein grundlegend anderes Gespräch über Ergebnisse und Verantwortlichkeit.

Wir wurden kürzlich kompromittiert. Kann Cyber Crucible in einer möglicherweise bereits kompromittierten Umgebung bereitgestellt werden?

Kurze Antwort: Ja. Cyber Crucible bewertet, was Programme gerade tun, anstatt nach bekannten schädlichen Dateien zu suchen, und beginnt daher bereits bei der Bereitstellung, bösartiges Verhalten zu stoppen — auch das eines Angreifers, der bereits Fuß gefasst hat.

Warum eine vorherige Kompromittierung keine Rolle spielt

Da die Prävention auf der verhaltensbasierten Absicht auf Kernel-Ebene beruht, muss ein bereits vorhandener Angreifer dennoch *handeln* — auf Identitätsdaten zugreifen, sich in Prozesse einschleusen, mit der Verschlüsselung beginnen oder Daten verschieben. Genau diese Aktionen lösen die Unterbrechung aus.

Auf diese Weise brachte die Bereitstellung im Finanzdienstleistungssektor eine aktive, andauernde Eindringung ans Licht, auf die der bestehende Sicherheits-Stack nie reagiert hatte. Cyber Crucible wurde nicht zur Untersuchung einer bekannten Sicherheitsverletzung eingesetzt, sondern um einen blinden Fleck aufzudecken — und fand dabei fast 10.000 bereits laufende bösartige Prozesse.

Was zu erwarten ist

Die Bereitstellung in einer kompromittierten Umgebung führt häufig zu sofortiger, umfangreicher Interceptionsaktivität. Das ist das Werkzeug, das wie beabsichtigt funktioniert, und es ist oft der erste eindeutige Beweis, den eine Organisation dafür erhält, dass bereits etwas im Gange war.