# Architektur & Technologie

Wie Cyber Crucible unter der Haube funktioniert – Genetic AI, Betrieb auf Kernel-Ebene, Rogue Process Prevention, Betriebssystemunabhängigkeit und warum Entscheidungen auf dem Endpunkt getroffen werden.

# Warum reagieren Sie mit dem Anhalten von Programmen?

Kriminelle haben gelernt, dass das ausschließliche Operieren im Arbeitsspeicher – unter Einsatz von Techniken wie Prozessinjektion – eine Reihe von Vorteilen bietet:

1. Übernahme der Identität eines Benutzers für dieses Programm.
2. Umgehung von Identitätsmanagement-Prüfungen.
3. Umgehung von anwendungsbasierten Firewall-Regeln und Whitelists.
4. Umgehung von Data-Loss-Prevention-Tools auf Servern.
5. Löschung nahezu aller im Arbeitsspeicher befindlichen Beweise, wenn der Prozess beendet wird.
6. Löschung nahezu aller im Arbeitsspeicher befindlichen Beweise nach einem Neustart des Computers.

Durch das Anhalten der vom Angreifer kontrollierten Programme werden die Beweise quasi eingefroren.

Auch der Angreifer wird dadurch eingefroren.

Die Beweise stehen forensischen Tools im Rahmen eines Untersuchungsprozesses zur Verfügung.

Ist die Organisation zu diesem Zeitpunkt nicht in der Lage, forensische Analysen durchzuführen, versetzt ein einfacher Neustart durch den Angreifer das System wieder in einen unbedenklichen Zustand. Ein erzwungenes Beenden des angehaltenen Programms und dessen Neustart hat in der Regel ebenfalls den gewünschten Effekt.

# Verhindert Cyber Crucible jede Prozessinjektion?

Nein!

Es gibt eine Vielzahl von Aktivitäten auf Systemen, die eine Prozessinjektion darstellen, aber nicht zwangsläufig bösartig sind.

Cyber Crucible macht all diese Prozessinjektionsaktivitäten für die Bedrohungssuche und Ursachenanalyse sichtbar, stoppt die Aktivität jedoch nicht, es sei denn, es beginnen Datenexfiltrations-Aktivitäten wie Datendiebstahl oder Ransomware-Verschlüsselung.

Nachfolgend ein Beispiel für eine Prozessinjektion, die von der Endpoint-Security-Software PC Matic namens PCPitStop durchgeführt wird. Es handelt sich wahrscheinlich um ein Verhalten, das sie zur Überprüfung laufender Prozesse ausführen.

5373968.png?width=680
Dank der kernelbasierten Verhaltensanalyse von Cyber Crucible haben Sie vollständige Sichtbarkeit auf alle Aktivitäten, unabhängig von der Berechtigungsstufe der Software (einschließlich hochprivilegierter Microsoft- oder Antivirus-Anbieter-Software).

Falls eine automatisierte Reaktion durchgeführt wird, können diese Seite sowie die Seite „Prozesserstellungen“ durchsucht werden, um schnelle Untersuchungsergebnisse zu liefern.

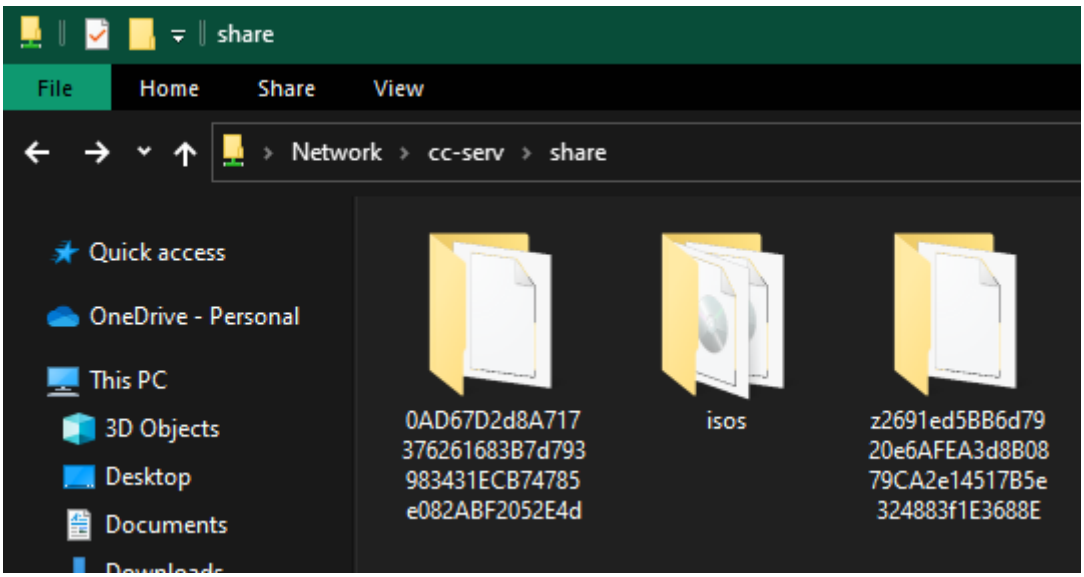
Zusätzlich kann die REST-API von Threat-Hunting-Teams genutzt werden, um nach Indikatoren für mögliches bösartiges In-Memory-Tradecraft zu suchen.

# Was sind diese merkwürdig aussehenden, zufälligen Dateien, die ich sehe?

Unsere Data Extortion Prevention-Software empfängt Verhaltensindikatoren von mehreren Engines, bevor sie in Sekundenbruchteilen entscheidet, ob ein Angriff vorliegt. Eine dieser Engines, die Dateiüberwachungs-Engine, verwendet spezielle Dateien an verschiedenen Speicherorten.

Diese Dateien, die Sie manchmal sehen und manchmal nicht, stammen von Cyber Crucible. Je nachdem, wie eine Anwendung Dateien auflistet, werden sie Ihnen möglicherweise angezeigt. Zum Beispiel wird ein Programm, das den Datei-Explorer verwendet, um Dateien zum Speichern oder Öffnen aufzulisten, Ihnen diese nun anzeigen.

Wir nennen diese Dateien „Kanarienvögel“, angelehnt an den Ausdruck „Kanarienvogel im Kohlebergwerk“ (wiki).



# Was ist das Besondere an Cyber Crucible Canary-Dateien?

In Canary-Dateien sind spezielle Daten versteckt, für den Fall, dass sie jemals von einem Angreifer gestohlen werden. Cyber Crucible kann die Datei bis zum ursprünglichen Besitzer zurückverfolgen.

Die Dateinamen sind größtenteils zufällig (sogenannt pseudo-zufällig) und so gestaltet, dass Angreifer sie nicht identifizieren und umgehen können. Die Namen werden mit einer speziellen mathematischen Formel von Cyber Crucible erzeugt, die es unserer Software ermöglicht, eine Datei als Canary zu erkennen, selbst wenn sich die Namen von Rechner zu Rechner oder von Datei zu Datei unterscheiden.

Die Fähigkeit der Cyber Crucible Software, diese Dateien zu erkennen, bedeutet auch, dass pro Server nur eine einzige Canary-Datei erforderlich ist, selbst wenn Tausende von Arbeitsstationen den Server nutzen.

# Wo befinden sich Canary-Dateien?

Canary-Dateien befinden sich an verschiedenen Stellen in Ihrem Dateisystem.

Immer wenn auf Ihrem System eine neue Dateiquelle auftaucht, von jedem beliebigen Benutzer, überprüft Cyber Crucible automatisch, ob dort bereits Canary-Dateien platziert wurden. Dies gilt auch für Wechseldatenträger wie USB-Sticks, Netzwerk-Dateiquellen und cloudbasierte Dateispeicher.

# Wie nutzt Cyber Crucible Speicheranalysen?

Die Kernel-Analysen von Cyber Crucible verfolgen den Zustand des Arbeitsspeichers eines Programms während seines gesamten Lebenszyklus, vom Programmstart bis zum Programmende. Zudem wird der Zustand der Interaktionen im Arbeitsspeicher mit anderen Programmen erfasst.

Die Verhaltensüberwachung prüft auf unsichere Zustände im Arbeitsspeicher des Programms. Dies kann auf einen Exploit, einen Softwarefehler oder bekannte speicherbasierte (sogenannte „dateilose“) Angriffe hinweisen.

Diese Überwachung erfolgt live an den Programmen auf äußerst effiziente Weise, um sicherzustellen, dass der Systembetrieb und die Abläufe des Kunden durch die Analyse von Cyber Crucible nicht beeinträchtigt werden.

Sobald ein mögliches Angreiferverhalten zum Zweck von Identitäts- oder Datendiebstahl oder Erpressung erkannt wird, fließt diese Verhaltensverfolgung und -analyse des Arbeitsspeichers gemeinsam mit anderen erfassten Telemetriedaten in die Entscheidung ein, ob ein Programm beendet werden sollte.

# Wie unterscheidet sich CCs verhaltensbasierte Speicheranalyse vom Memory Scanning?

# Was ist Memory Scanning?

Memory Scanning ist die Praxis, einen Speicherblock zu nehmen, ihn normalerweise zur Analyse an einen anderen Ort im System zu kopieren und ihn dann zu scannen.

## Fotografie vs. Live-Aktion

Dies ist kein Live-Scanning des Programms während es agiert, sondern eine Momentaufnahme des Programms zu einem bestimmten Zeitpunkt. Man kann es sich wie eine Fotografie im Vergleich zu einem Live-Stream vorstellen. Der Zustand des Programms kann sich von einem Moment zum nächsten drastisch ändern, weshalb dies am ehesten für forensische Zwecke in einer kontrollierten Umgebung nützlich ist. In einer nicht kontrollierten Umgebung, wie einer Kundenumgebung, ist es weniger nützlich. Je ausgelasteter die Maschine ist oder je mehr ein Programm tut, desto schwieriger ist es, ein genaues Bild vom aktuellen Zustand eines Programms zu erhalten.

Cyber Crucible setzte zu Beginn stark auf Memory Scanning und versuchte, möglichst viele „Aufnahmen“ der Speicherzustände von Programmen zu machen. Als wir schneller wurden, stießen wir auf mehrere Engpässe hinsichtlich der Geschwindigkeit, mit der Speicher-Momentaufnahmen erstellt werden konnten, sowohl bei einzelnen als auch bei mehreren Programmen gleichzeitig.

## Bedenken hinsichtlich CPU- oder GPU-Ressourcenverbrauch

Dieses Memory Scanning kann äußerst ressourcenintensiv sein und bei großen Programmen einige Zeit in Anspruch nehmen. Als Cyber Crucible noch Memory Scanning einsetzte, anstatt intelligenter verhaltensbasierter Speicherüberwachung, war ein gesamter CPU-Kern für das Scannen reserviert.

Intel verfügt über eine innovative Technologie namens Intel TDT AMS, die auf bestimmten Intel-basierten Architekturen mit integrierter Intel-GPU verfügbar ist.

Sie scannt den Speicher eines Programms beim ersten Start und nutzt dabei die GPU, um die CPU nicht zu belasten. Zudem ist die GPU für die Art des durchgeführten Scannens leistungsfähiger (dazu später mehr).

# Scan-Methodik

Memory Scanning wird durchgeführt, um nach bestimmten Codes oder „Strings“ zu suchen. Dabei handelt es sich oft um dieselben Datenfragmente, nach denen Antivirus-/EDR-Tools in potenziell bösartigen Dateien suchen.

Memory Scanning ist speziell begrenzter als einige der komplexen Suchvorgänge, die gegen eine Datei durchgeführt werden können.

Daher sucht das Scanning standardmäßig nach bereits bekannten Elementen, wie älterer Malware, ist dabei jedoch in seinen Möglichkeiten eingeschränkt.

Cyber Crucible scannte früher Speichersegmente nach kryptografischem Material, dies erwies sich jedoch für moderne Umgebungen als zu limitiert, und wir entwickelten eine andere Methode, um Verhaltensweisen mittels kernelbasierter Logik zu beobachten.

# Verhaltensbasierte vs. Scan-Methodiken

Cyber Crucible ist aus mehreren Gründen von einer scan-basierten zu einer verhaltensbasierten Methodik übergegangen.

## Nachteile des Scannings

Der erste Grund ist, dass ein Live-Bild über alle Programme hinweg genutzt werden musste. Momentaufnahmen ermöglichten es kaum, auch nur eine begrenzte Analyse abzuschließen, bevor bereits die nächste benötigt wurde. Zu viel Programmaktivität wurde übersehen, fast so, als würde

eine Videokamera mit zu niedriger Bildrate arbeiten. Dies wurde durch die Notwendigkeit, alle Programme gleichzeitig zu überwachen, noch verstärkt. Server oder stark ausgelastete Arbeitsstationen – wohl die Computer, die am meisten Überwachung benötigten und am wichtigsten waren – erhielten letztlich den geringsten Anteil an Überwachung. Unabhängig vom Unternehmen oder Produkt waren die technologischen Grenzen offensichtlich und nicht praktikabel.

Der zweite Grund ist, dass Scanning, abgesehen vom Ressourcenverbrauch, standardmäßig die Suche nach **etwas Bekanntem** erfordert. Memory Scanning muss also signaturbasiert sein. Zudem muss das Signatur-Scanning eine begrenzte Teilmenge des umfangreicheren Signatur-Scannings sein, das bei dateibasiertem Antivirus-Scanning zu finden ist. Angreifer umgehen dateibasierte Signaturabwehrmaßnahmen bereits seit Jahren; die Wahrscheinlichkeit, dass Angreifer durch ein weniger leistungsfähiges signaturbasiertes System entdeckt werden, ist sehr gering.

# Vorteile der verhaltensbasierten Analyse

Die verhaltensbasierte Speicherüberwachung von Cyber Crucible erfordert keine Signaturen und nutzt Kernel-Speicherzugriff, um die Verhaltensweisen aller Programme gleichzeitig zu verfolgen. Lassen Sie uns das im Detail betrachten.

Erstens bedeutet verhaltensbasierte Überwachung, dass neue Malware oder Malware, die von Angreifern verändert wurde, um neu zu erscheinen, leicht in Echtzeit erkannt werden kann. Signaturbasiertes Scanning, ob von Speicher oder Dateien, beruht darauf, dass dieses spezifische Stück Malware bereits zuvor gesehen wurde. Angreifer umgehen signaturbasierte Abwehrmaßnahmen seit Jahren, trotz einer vollständigen Palette an Scan-Techniken gegen Dateien. Die für den Speicher verfügbaren Scan-Techniken stellen davon nur eine Teilmenge dar und sind noch weniger effektiv.

Zweitens ist die neuartige verhaltensbasierte Speicherüberwachung von Cyber Crucible in der Lage, über die gesamte Laufzeit der Programme hinweg in Echtzeit über alle Programme gleichzeitig zu bleiben. Memory Scanning leidet unter schwerwiegenden Ressourcenengpässen, die sich verschlimmern, je mehr Programme ausgeführt werden. Angreifer führen normalerweise Dutzende von Malware-Samples gleichzeitig aus und überlasten dadurch die Memory-Scanning-Analyse durch die Geschwindigkeit und Anzahl der gleichzeitig zu untersuchenden Programme – unabhängig davon, ob es sich um Zero-Day- oder alte Malware handelt.

# Was passiert, wenn CC Speicherangriffe erkennt

Zunächst ist es sehr wichtig zu beachten, dass Speicheränderungen aus verschiedenen Gründen auftreten können:

1. In-Memory-Angriffe
2. Interaktion zwischen Programmen
3. Softwarefehler
4. Exploits

Eine Prozessinjektion oder Speicheränderungstechnik, die verwendet wird, auch zwischen Programmen, ist also nicht zwangsläufig eine bösartige Aktion.

Wenn ein Programm, das ein wahrscheinlich bösartiges Speicherereignis erlitten hat (also #1 oder #4 oben), in eine automatisierte Reaktion von Cyber Crucible einbezogen wird, erfolgt eine automatisierte Erfassungsaktivität.

Der Teil des Speichers, der in einem Programm verändert wurde, sowie der Zustand „davor“ wird in einem strukturierten Cyber Crucible-Format namens .ccdiff gespeichert.

Dieser injizierte oder veränderte Speicherbereich wird gespeichert und steht im Cyber Crucible Webportal zum Download zur Verfügung.

# Warum wird dies nicht automatisch zur Analyse an Virustotal (etc.) übermittelt?

Unter bestimmten Umständen enthält der bei einem Angriff verwendete bösartige Code Variablen, die für einen Angriff spezifisch sind, insbesondere für ein Opfer.

Die Übermittlung dieses bösartigen Codes an eine öffentliche Analyseplattform wie Virustotal würde eine unerwünschte, opferidentifizierende Informationsoffenlegung gegenüber der Sicherheitscommunity darstellen.

# Warum wäre die Übermittlung dieser Binärdaten an Virustotal (etc.) hilfreich?

Signaturbasierte Antivirus- und EDR-Tools suchen nach Zeichenfolgen oder Code-Bytes, die bei früheren Angriffen beobachtet wurden. Selbst wenn diese Malware noch nie zuvor gesehen wurde, kann sie nach einiger Zeit der Sicherheitscommunity bekannt werden. Diese Scan-Tools benötigen den Code in der Regel nicht in einem korrekt formatierten Binärformat, um eine Zuordnung zu einer bekannten Malware zu erkennen.

# Was ist Genetic AI, und wie unterscheidet sie sich von einem LLM?

**Kurze Antwort:** Genetic AI ist die eigens entwickelte Security-KI von Cyber Crucible. Sie modelliert, wie sich Programme verhalten – im Arbeitsspeicher, über Prozesse hinweg und gegenüber Dateien – und erkennt bösartige Abweichungen in Echtzeit. Sie ist kein Large Language Model; LLMs analysieren Textmuster, was ein völlig anderes Problem darstellt.

## Was sie unterscheidet

- **Eigens für Sicherheit entwickelt**, nicht von einem allgemeinen Textmodell abgeleitet.
- **Verhaltensbasiert, nicht signaturbasiert** – keine Signaturen, keine Threat-Intelligence-Feeds, kein Warten darauf, dass jemand anderes den Angriff zuerst entdeckt.
- **Vollständig autonom** – herkömmliche Tools setzen auf das Zusammenspiel von Mensch und Maschine; Genetic AI entscheidet und handelt eigenständig.
- **Präventiv vor der Ausführung** – sie blockiert bösartiges Verhalten, bevor es ausgeführt wird, statt es nachträglich zu beschreiben.

## Vertikale KI

Genetic AI ist ein Beispiel für vertikale KI: künstliche Intelligenz, die auf die spezifischen Herausforderungen eines bestimmten Sektors zugeschnitten ist, anstatt auf allgemeines Schlussfolgern. Im Bereich Sicherheit ermöglicht genau diese Spezialisierung eine Entscheidung über die Absicht in unter 200 Millisekunden.

Die Ergebnisse sind messbar – Cyber Crucible hat mehrere Zero-Day-Angriffe auf Kundennetzwerke gestoppt, bis zu 90 Tage bevor ein anderer Anbieter diese meldete oder darauf reagierte.

# Wie trifft Cyber Crucible eine Entscheidung in unter 200 Millisekunden?

**Kurze Antwort:** Es durchläuft eine dreistufige Schleife – Detect, Decide, Respond –, die vollständig auf dem Endpunkt auf Kernel-Ebene ausgeführt wird, unter Verwendung einer patentierten Edge-Computing-Analyse-Engine. Da nichts zu einem Cloud-Dienst und zurück übertragen werden muss und kein Mensch involviert ist, wird der gesamte Zyklus in unter 200 Millisekunden abgeschlossen.

## Die Schleife

1. **Detect** – neuartige Sensoren auf Kernel-Ebene identifizieren bösartige Verhaltensmuster im Arbeitsspeicher, in der Prozessaktivität und beim Dateizugriff.
2. **Decide** – das KI-gestützte Verhaltensmodell bewertet sofort die Absicht des Datenzugriffs des Programms.
3. **Respond** – ist die Absicht bösartig, wird das Programm abgefangen und angehalten.

## Warum lokale Verarbeitung unverzichtbar ist

Das Senden von Telemetriedaten an einen Cloud-Server, das Warten auf die Analyse und der Empfang einer Antwort kostet Millisekunden, die der Angreifer nur allzu gerne nutzen wird. Zur Einordnung der Größenordnung: Diese Entscheidung erfolgt schneller, als ein Nervenimpuls vom Auge zum Gehirn gelangt. Jede Architektur mit einem Netzwerk-Roundtrip im kritischen Pfad hat dieses Rennen bereits verloren.

Rohe Telemetriedaten werden im Nachhinein weiterhin zu Servern kopiert, um Beweise zu sichern und Daten anzureichern – doch die Schutzentscheidung wartet niemals darauf.

# Was ist Rogue Process Prevention (RPP)?

**Kurze Antwort:** Rogue Process Prevention ist Cyber Crucibles patentierter Ansatz, aktiv gegen einen bösartigen Prozess einzuschreiten, statt ihn lediglich zu beobachten. Ob es sich um Ransomware handelt, die mit der Verschlüsselung beginnt, oder um einen Infostealer, der nach einem Sitzungstoken greift – der Prozess wird gestoppt, bevor Daten das Gerät verlassen.

# Beobachten versus eingreifen

Der Großteil des Endpoint-Marktes ist darauf ausgelegt, zu beobachten. RPP ist darauf ausgelegt, einzugreifen. Der Unterschied entspricht dem zwischen einer Überwachungskamera, die einen Einbruch zur späteren Auswertung aufzeichnet, und einem Wachmann, der den Dieb am Tresor aufhält.

# Wogegen es schützt

RPP adressiert die drei zentralen Bedrohungen gemeinsam, da moderne Angriffe in der Regel mehrgleisig erfolgen:

- **Identitätsdiebstahl** — Zugriff auf Schlüssel, Token und Passwörter, häufig völlig ohne Zutun des Mitarbeiters.
- **Informationsdiebstahl** — Massenexfiltration von Daten in Maschinengeschwindigkeit.
- **Ransomware** — Verhaltensanalyse in Kombination mit Hacker-Täuschungstechnologie, die die Verschlüsselung selbst einer einzigen Datei verhindert.

Eine Verteidigung, die sich eng auf Ransomware allein konzentriert, würde die ersten beiden Phasen übersehen – dort, wo der eigentliche Schaden meist beginnt.

# Welche Rolle spielt Speicheranalyse innerhalb der gesamten Plattform?

**Kurze Antwort:** Speicheranalyse ist das Fundament, auf dem alles andere aufbaut. Sie ist die Sensor- und Analysequelle, die sämtliche Verhaltensmodellierung speist – Datenschutz, Identitätsschutz und FortressAI gleichermaßen. Jede Entscheidung, die diese Funktionen treffen, beruht darauf zu wissen, was der Speicher eines Programms tatsächlich tut.

## Ein Fundament, drei Fähigkeiten

Cyber Crucible verfolgt den Zustand des Speichers eines Programms über dessen gesamten Lebenszyklus hinweg, vom Start bis zum Ende, einschließlich seiner speicherinternen Interaktionen mit anderen Programmen. Genau dieser eine Analyse-Datenstrom macht alles Weitere erst möglich:

- **Datenschutz** – verhält sich dieser Prozess so, als stünde er kurz davor, zu verschlüsseln oder Daten zu exfiltrieren?
- **Identitätsschutz** – ist dieser Prozess der rechtmäßige Inhaber der Anmeldedaten, auf die er zugreift, oder wurde er übernommen?
- **FortressAI** – ist dieses KI-Tool noch es selbst, und liegt sein Datenzugriff innerhalb der Richtlinien?

Dies sind keine drei getrennten Engines mit drei getrennten Sensor-Sets. Es sind drei Richtlinien, die auf demselben Speicher-Verhaltensmodell aufbauen.

## Warum Speicher das richtige Fundament ist

Moderne Angriffe hinterlassen zunehmend keine Datei mehr, die untersucht werden könnte. Code wird in vertrauenswürdige Prozesse eingeschleust und im Speicher aufgebaut, sodass die Aktivität nur im Speicherzustand eines laufenden Programms sichtbar ist. Eine Verteidigung, die dort nicht hinsehen kann, ist für diese gesamte Angriffsklasse blind.

Die Speicheranalyse beantwortet zudem die Frage, die vor der Gewährung von Zugriff auf irgendetwas Sensibles am wichtigsten ist: **Ist dieses Programm noch das, was es vorgibt zu sein?** Eine vertrauenswürdige Anwendung, deren Prozess oder Bibliotheken manipuliert wurden, ist nicht mehr vertrauenswürdig – und nur eine Untersuchung auf Speicherebene deckt dies auf.

# Kein Speicher-Scanning

Hierbei handelt es sich um eine live erfolgende Verhaltensverfolgung, nicht um periodisches Scannen. Beim Scannen wird ein Speicherblock kopiert und der Schnappschuss analysiert – eine Fotografie statt einer Live-Aufnahme. Auf einem stark ausgelasteten Rechner kann sich der Zustand des Programms einen Moment später bereits völlig verändert haben, was Schnappschüsse für kontrollierte forensische Untersuchungen nützlich, für den Echtzeitschutz jedoch deutlich schwächer macht.

> Weitere technische Details dazu, wie sich dies vom Speicher-Scanning unterscheidet, sowie dazu, was geschieht, wenn ein Speicherangriff erkannt wird, finden Sie in den bestehenden Artikeln zur *Speicheranalyse*.

# Warum arbeitet Cyber Crucible auf Kernel-Ebene?

**Kurze Antwort:** Der Kernel ist die tiefste und privilegierteste Schicht des Betriebssystems. Der Betrieb auf dieser Ebene ermöglicht es Cyber Crucible, sämtliche Systemaktivitäten zu sehen und zu kontrollieren, die Absicht eines bösartigen Prozesses zu erkennen und ihn innerhalb von Millisekunden zu stoppen — und macht das Tool zudem weitaus widerstandsfähiger gegen Manipulation oder Deaktivierung durch einen Angreifer.

# Was Kernel-Zugriff ermöglicht

- **Vollständige Sichtbarkeit** von Speicherverhalten, Prozessverhalten und Dateizugriffen, einschließlich Aktivitäten, die niemals auf die Festplatte geschrieben werden.
- **Die Fähigkeit zu handeln**, nicht nur zu beobachten — Berechtigungen können entzogen und Prozesse in dem Moment ausgesetzt werden, in dem böswillige Absicht erkannt wird.
- **Resilienz**, da Angreifer unweigerlich versuchen werden, das Sicherheitstool selbst zu deaktivieren.

# Zur Kritik an der Kernel-Entwicklung

Einige etablierte Anbieter und Analysten raten von einer Entwicklung auf Kernel-Ebene ab. Kernel-Entwicklung ist tatsächlich schwierig und kostspielig — genau deshalb hat ein Großteil des Marktes sie gemieden, wodurch Endpunkte auf User-Space-Telemetrie angewiesen blieben, die durch Angriffe auf Root-Ebene neutralisiert werden kann.

Die Qualität und Manipulationssicherheit von Cyber Crucible wird durch das Windows Hardware Compatibility Program (WHCP) von Microsoft validiert.

# Was bedeutet es, dass Cyber Crucible unabhängig von Windows-Bibliotheken ist?

**Kurze Antwort:** Cyber Crucible ist nicht auf die Windows-Systembibliotheken angewiesen, die es schützt. Es wurde bewusst von diesen entkoppelt, sodass Cyber Crucible auch dann weiterläuft, weiter durchsetzt und weiter meldet, wenn Angreifer diese Bibliotheken kompromittieren, zum Absturz bringen oder kapern.

## Warum dies entwickelt wurde

In der zweiten Hälfte des Jahres 2025 verlagerten sich Angreifer darauf, zentrale Windows-Bibliotheken im Arbeitsspeicher zu infizieren. Da nahezu jeder Sicherheitsanbieter auf dieselben Bibliotheken angewiesen ist, um zu funktionieren, machte dieser eine Schritt einen Großteil des Marktes blind.

Cyber Crucible investierte rund neun Monate in die Entwicklung neuartiger Sensoren und weitere fünf Monate technische Arbeit, um Abhängigkeiten von Windows-Bibliotheken vollständig zu beseitigen – einschließlich der Eliminierung volatiler MiniFilter-Abhängigkeiten.

## Wie sieht das architektonisch aus

Die Architektur betreibt sieben vollständig unabhängige Subsysteme innerhalb des Kernels, einschließlich eigener isolierter Verschlüsselung, Netzwerkkommunikation, Metadatenanalyse und Ereignisverfolgung. Eine weitere Phase dieser Arbeit ersetzt die standardmäßige Windows-Netzwerkbibliothek (`ws32_2.dll`) durch einen eigens entwickelten Netzwerk-Stack auf Kernel-Ebene.

## In der Praxis bewährt

Bei zwei Kunden versuchten Angreifer, die von der ausschließlich im Kernel arbeitenden Entscheidungs-Engine blockiert wurden, anschließend zu verhindern, dass der Kunde benachrichtigt wird, indem sie die Netzwerkschicht des Betriebssystems angriffen. Da die Netzwerkkommunikation von Cyber Crucible unabhängig vom Betriebssystem ist, blieb der Schutz bestehen, und die Informationen erreichten den Kunden dennoch.

# Funktioniert Cyber Crucible offline oder in Air-Gapped-Umgebungen?

**Kurze Antwort:** Ja. Die gesamte Analyse und Durchsetzung erfolgt lokal auf dem Endpunkt, sodass Cyber Crucible vollständigen Schutz ohne Internetverbindung, ohne Cloud-Dienst und ohne jegliches Signal bietet. Es ist geeignet für Air-Gapped-Netzwerke, OT- und ICS-Umgebungen sowie für getrennte Feldeinsätze.

## Warum es ohne Konnektivität funktioniert

Da der Detect-Decide-Respond-Zyklus vollständig im Kernel auf dem Gerät ausgeführt wird, ist für eine Schutzentscheidung niemals eine Verbindung erforderlich. Telemetriedaten werden opportunistisch synchronisiert, um Beweise und Berichte bereitzustellen, sobald eine Verbindung verfügbar ist, aber der Schutz ist davon nicht abhängig.

## Bewährt auf See

Bei einem Einsatz auf See arbeitete Cyber Crucible eigenständig während mehrtägiger Reisen ohne IT-Personal an Bord, passte sich an Verbindungen mit geringer Bandbreite und unregelmäßige Satellitenverbindungen mit wetterbedingten Unterbrechungen an und bewahrte umfangreiche forensische Protokolle über lange getrennte Zeiträume für die Analyse nach der Reise. Die geschützten Systeme reichten von für Passagiere zugänglichen Freizeitterminals bis hin zu unternehmenskritischen maritimen Steuerungssystemen.

Aus diesem Grund eignet sich derselbe Agent auch für Produktionshallen, Logistikflotten und andere Edge-Umgebungen, in denen die Cloud-Konnektivität unzuverlässig oder bewusst nicht vorhanden ist.

# Warum reagiert Cyber Crucible mit dem Anhalten eines Prozesses anstatt das System herunterzufahren?

**Kurze Antwort:** Das Anhalten nur des bösartigen Prozesses — manchmal auch als Selective Freeze bezeichnet — neutralisiert den Angriff, während alles andere weiterläuft. Es gibt keine vollständige Systemsperre, keinen Neustart und keine Unterbrechung der legitimen Arbeit.

## Das Problem mit Lockdown-artigen Reaktionen

Wenn viele Erkennungstools eine Anomalie identifizieren, sind die Eindämmungsoptionen grobschlächtig: die Maschine isolieren oder vom Netz nehmen. In einem Krankenhaus, einer Fabrik oder einem Handelsbetrieb kann diese Reaktion nahezu so schädlich sein wie der Angriff selbst.

## Was selektives Anhalten erreicht

Der Angriff wird im Arbeitsspeicher angehalten. Legitime Transaktionen werden niemals gestoppt. In der Implementierung im Finanzdienstleistungsbereich, bei der fast 10.000 bösartige Prozesse abgefangen wurden, liefen die legitimen SQL-Transaktionen durchgehend ununterbrochen weiter — der Betrieb wurde nie eingestellt.

Genau das macht Prävention mit Geschäftskontinuität vereinbar, anstatt einen Kompromiss dazu darzustellen.