NEOX NETWORKS

Threat Hunting mit forensischer Zustandsanalyse

Infocyte hat vor Kurzem an der Preisverleihung des „SC Magazins“ als einer der Nominierten für die beste Forensik-Lösung teilgenommen. Es ist ohne jeden Zweifel eine Ehre, für diese Auszeichnung nominiert zu werden, aber offen gesagt sind wir eher eine Ausnahme in dieser Kategorie.

Im Gegensatz zu anderen Lösungen, wie „Guidance Software Encase“, ist „Infocyte HUNT“ keine reine Forensik-Lösung. Im Gegenteil, was wir kreiert haben, ist eine neuartige Lösung unter den kommerziellen Cybersecurity-Produkten. Wir haben eine digitale Forensiklösung für Endpunkte in eine proaktive und skalierbare Lösung zur Findung von Kompromittierungen umgewandelt (die Suche nach unbekannten Kompromittierungen/ Bedrohungen, die bereits andere Sicherheitskontrollen umgangen haben). Wir nennen es forensische Zustandsanalyse (FSA).

An diesem Punkt werden wahrscheinlich die Skeptiker unter Ihnen hier aufhören zu lesen und behaupten, dass die „Digital Forensics & Incident Response Community“ (DFIR) und führende Incident Response (IR) Firmen, wie Mandiant, schon seit Jahren etwas Ähnliches anbieten. Lesen Sie bitte weiter, denn ich verspreche Ihnen, es ist nicht dasselbe. Unsere, als Finalist nominierte Lösung, „Infocyte HUNT“, ist eine agentenlose Threat-Hunting-Plattform für Endpunkte, die FSA verwendet, um verborgene Bedrohungen und Risikofaktoren innerhalb eines Netzwerks zu entdecken. Es durchsucht tausende von Endpunkten, wobei es nur ein paar Minuten auf jedem Host verbringt und abschließend deren Zustand bestätigt: "kompromittiert" oder "nicht kompromittiert".

Forensische Zustandsanalyse (FSA)

Die forensische Zustandsanalyse ist im Vergleich etwas ganz anderes als eine Endpunktüberwachung oder Verhaltensanalyse. Es ist nicht nur ein „Indicator of Compromise Scanner“ (Scanner für Gefährdungsindikatoren). IOC-Scanner sind zwar nützlich, aber sie sind nicht tiefgründig genug, um eine breite Palette von anhaltenden Bedrohungen in einem Netzwerk festzustellen. Allerdings kann ein umfassendes FSA-Tool mit hoher Genauigkeit ermitteln, ob ein Endpunkt sicher ist. Monitoring-Tools für Endpunkte, wie beispielsweise EDR, werden hingegen nicht in der Lage sein, dies zu tun, da es nicht ihre vorgesehene Funktion ist.

Auf der höchsten Ebene dringen wir tief in einen Endpunkt ein, um herauszufinden, was dort aktiv ist und wodurch es getriggert wurde.

Der nächste Schritt ist, jegliche Manipulation des Betriebssystems (OS) oder der aktiven Prozesse zu identifizieren, die beispielsweise ein Rootkit durchführt, um seine Präsenz zu verstecken. Oder auch, um Herauszufinden, was eine Bedrohung getan haben könnte, um die Sicherheitskontrollen des Systems zu umgehen. Dadurch legt es offen, ob z B. Die OS-Konfiguration verändert, oder ein API-Aufruf durch einen versteckten oder kompromittierten Prozess gestartet wurde.

Beachten Sie, dass sich diese Art der Erkennung deutlich von den Verhaltensanalysetechniken unterscheiden, die von herkömmlichen „Endpoint Detection and Response“ (EDR) oder „User Behavior Analytics“ (UBA) Produkten verwendet werden, die nur Änderungen an einem System oder Netzwerk als Ereignisse aufzeigen. Dies sind beispielsweise ein neuer Prozess, eine Änderung von Registrierungsschlüsseln oder ein Benutzer, dessen Berechtigungen erhöht wurden. FSA sucht hingegen viel ausführlicher.

Um dies etwas besser zu veranschaulichen, wollen wir einen genaueren Blick auf die Unterschiede werfen.

Zustand- vs. Verhaltensanalyse

Heutzutage verlässt sich die Sicherheitsindustrie vorwiegend auf Verhaltensanalysen und Erkennung. Manche glauben fälschlicherweise, dass es die einzige Möglichkeit ist, um moderne Bedrohungen zu erkennen. Wir werden gelegentlich von Analysten und Interessenten gleichermaßen gefragt: "Wie führt Infocyte eine Verhaltensanalyse durch, wenn es doch agentenlos ist?"

Die Antwort lautet: überhaupt nicht. Außer beim Sandboxing, während der binären Analysephasen, verwenden wir überhaupt keine Verhaltenserkennungstechniken.

Eine forensische Zustandsanalyse unterscheidet sich völlig von einer Endpunktüberwachung oder Verhaltensanalyse. Es ist nämlich nicht nur ein „Indicator of Compromise (IOC) Scanner". IOC-Scanner sind zwar nützlich, aber sie sind nicht tiefgründig genug, um eine breite Palette von anhaltenden Bedrohungen in einem Netzwerk zu identifizieren. Allerdings kann ein umfassendes FSA-Tool mit hoher Genauigkeit ermitteln, ob ein Endpunkt sicher ist. Monitoring-Tools für Endpunkte, wie beispielsweise EDR, werden hingegen niemals in der Lage sein, dies zu tun. Es ist einfach nicht ihre vorgesehene Funktion. EDR-Tools überwachen Endpunkte für Verhaltensweisen, die darauf hinweisen, dass es einen Angriff gibt, sie führen keine forensische Validierung der Sicherheit durch. Analog dazu basieren die Annahmen von EDR und der Verhaltensüberwachung auf der Vorstellung, dass bei der Überwachung aller Türen, eventuell niemand im Haus sein könnte. Zahlreiche Sicherheitsverletzungen haben bewiesen, dass diese Annahme falsch ist.

Auch unser CTO würde zustimmen, dass nichts absolut sicher ist. Betrachten wir dies nun aus der Unternehmensperspektive. Wenn beispielsweise der Präsident der Vereinigten Staaten in einem ausländischen Hotel übernachtet, trifft ein Team von Secret Service Agenten im Voraus dort ein und durchsucht die Wohnräume des Präsidenten auf Wanzen. Erwarten sie, dass ihre Ausrüstung jede unbekannte Spionagetechnik findet? Natürlich nicht. Aber ein Raum, der mit einem umfassenden Verfahren auf Wanzen durchsucht wurde, ist exponentiell sicherer als ein nicht durchsuchter Raum.

Im Vergleich dazu, wenn Sie CISO sind (Beauftragter für die zentrale IT-Sicherheit), ist es Ihr Job, zufriedenstellend und kostengünstig, jegliche Risiken innerhalb eines Unternehmens zu reduzieren. Mit der Gewissheit, dass jede Woche alle vernetzten Informationssysteme forensisch validiert wurden und das ihre Operationen, E-Mails oder Finanzgeschäfte nicht gehackt wurden, gibt einem zunehmend nervösen Vorstand ein gewisses Maß an Vertrauen, um ohne Bedenken in die Zukunft blicken zu können.

Also, was ist nun der Unterschied auf technischer Ebene? Es beginnt damit, welche Arten von Daten gesammelt und analysiert werden.

Verhaltensanalyse

Bei einer Verhaltensüberwachung und -analyse, wie beispielsweise einem EDR-Produkt, ist eine Erfassung und Analyse ereignisorientiert. Beispiele hierfür sind die Aufzeichnung von:

- Prozessausführungsereignissen (mit der Verwendung von Kommandozeilen, falls aktiviert)
- Prozessänderungen (Erhöhung von Privilegien, Prozessabstürzen usw.)
- ausgewählte Änderungen der Registry
- Ausgewählte Schreiboperationen (z B.. Download/Benutzerordner, Windows Ordner usw.)
- Dateierstellungsereignisse
- Überwachung von ausgewählten API-Aufrufen (eine vollständige Überwachung wäre unmöglich)
- Netzwerkverbindungsereignisse (oder deren Probeentnahme)

Dies sind alles wichtige Dinge, die überwacht werden müssen, wenn Sie einen Angriff feststellen möchten.

Forensische Zustandsanalyse

Im Gegensatz dazu setzt eine forensische Zustandsanalyse nicht auf Protokolle oder eine Überwachung von Ereignissen/Veränderungen in einem System. Stattdessen geht eine forensische Zustandsanalyse davon aus, dass das Gerät bereits kompromittiert wurde und versucht, jeden Aspekt des Systems so ausführlich wie nur möglich zu validieren. Um dies zu erreichen, beinhaltet die Analyse und Erfassung folgende Merkmale:

- Eine Auswertung aller aktiven Prozesse
- Eine Auswertung aller geladenen Module und Treiber
- Eine Identifizierung und Auswertung von Speicher-injizierten Modulen (Anmerkung: Infocyte geht in diesem Hinblick weit über eine Identifizierung hinaus. Wir verwenden proprietäre „Memory-Un-Mapping“ Techniken, um Speicherobjekte für eine Offline-Aufbewahrung und Analyse zu exportieren)
- Eine Identifizierung und Auswertung von Prozessmanipulationen (Function Hooks, Inline-Modifikationen/Patches usw.)
- Identifizierung und Auswertung der Betriebssystemmanipulation (Listenmodifikationen, versteckte Prozesse, Manipulation des Kernels)
- Identifizierung von deaktivierten Sicherheitskontrollen (deaktivierte AV, reduzierte Authentifizierungsanforderungen von Konfigurationen, GPO-Blockierung usw.)
- Aufzählen und Auswerten der Persistenz (Cronjobs, Autostarts/Auslöser des Registers, DLL-Hijacking, WMI-Events, Umleitung des Boot-Prozesses, Watchdog-Prozesse usw.)
- Auswertung von Artefakten der Anwendungsausführung (Prefetch, Shimcache und SuperFetch)
- Identifizierung und Auswertung von Web-Shells (Linux- oder IIS-Webserver)
- Überprüfung legitimer Remote-Admin-Service (cmd, Powershell, NetSH, SSH, VNC, PSExec, RDP, Tunnel, WMI)
- Auswertung aller aktiven Host-Verbindungen (inklusive Interprozesskommunikation und Weiterleitungen)
- Überprüfung aller privilegierten Benutzerkonten (gefährlich lokale Admin-Konten, usw.)

Vielleicht ist der wichtigste Aspekt, um eine erfolgreiche Zustandsanalyse einer kompromittierten Maschine zu gewährleisten, die Möglichkeit bestimmte Anti-Forensik-Techniken zu umgehen. Dies wird erreicht, indem man übergeordnete Betriebssystem-APIs umgeht und direkt mit flüchtigen Speicherstrukturen arbeitet, wozu „Infocyte HUNT“ in der Lage ist.

Warum Sie es benötigen:

Wir behaupten nicht, dass eine forensische Zustandsanalyse die Notwendigkeit einer zentralen Protokollierung oder Verhaltensüberwachung in Echtzeit ersetzt. Im Gegenteil, sie sind äußerst komplementär und füllen die Lücke in der Erkennung von nachträglichen Kompromittierungen. „Infocyte HUNT" ermöglicht es Ihnen, auf benutzerdefinierte Skripte und andere DFIR-Prozesse zu verzichten, die Sie verwenden, um verdächtige Verhaltensweisen zu überprüfen, die schon bekannt sind. Nun können Sie iterativ und effektiv alle Endpunkte überprüfen, um hartnäckige Bedrohungen zu finden, die sich auf einem Ihrer Endpunkte verstecken. Viele SOCs verwenden derzeit wahrscheinlich schon eine einfachere Version, indem sie ein benutzerdefiniertes Tool-Set verwenden oder ein Endpoint-Abfragetool skripten, die jedoch Anti-Forensik-Techniken nicht umgehen werden.

Neben der Verbesserung Ihrer Überwachungs- und Erkennungsprozesse ermöglicht eine forensische Zustands-analyse völlig neue Verwendungszwecke:

- Laptops, mobile Geräte und andere vorübergehende Systeme (BYOD), die bisher noch nicht verwaltet wurden, können nun validiert werden, wenn sie auf das Netzwerk zugreifen
- Systeme ohne Endpunktüberwachung (aufgrund von Richtlinien, Fehlverwaltung oder Manipulation) können identifiziert und regelmäßig beurteilt werden
- Für Organisationen, die nicht über genügend historische Protokolle oder die Fähigkeit verfügen, große Daten in eine definitive Aktion umzuwandeln, bietet die forensische Zustandsanalyse ein sehr gutes Preis-/ Leistungsverhältnis
- Für Berater und IR-Profis ist die forensische Zustandsanalyse der schnellste und einfachste Weg, um eine Sicherheitsbewertung oder „Threat Hunting Engagement Service" durchzuführen. Indem Sie zusätzlich eine agentenlose Methode wie „Infocyte HUNT" verwenden, verringert es die Notwendigkeit für die meisten Change-Management-Prozesse, was Ihren Aufwand erheblich verringert.

Es gibt eine Vielzahl von Gründen, um eine forensische Zustandsanalyse in Ihre Sicherheitsbetriebsprozesse zu integrieren. Sind Sie bereit sich selbst davon zu überzeugen? Sie können sich gerne jederzeit direkt mit uns in Verbindung setzen.

+49 6103 37 215 910
+49 6103 37 215 919
www.neox-networks.com
sales@neox-networks.com
NEOX NETWORKS GmbH
Otto-Hahn-Straße 8
D-63225 Langen (Hessen)