IOprotect

ATTACK CHAIN EMULATION

ÜBERPRÜFT SECURITY CONTROLS

Service

Attack Chain Emulation erlaubt es Unternehmen ihre Sicherheitsmassnahmen (Security Controls) umfassend zu überprüfen und Schwachstellen in der IT-Umgebung aufzudecken.

Dazu analysiert IOprotect reale Cyberangriffe und deren Angriffsketten, wie sie von staatlichen Akteuren (APT), Ransomware-Gruppen und Cybercrime-Gangs genutzt werden. Auf dieser Grundlage werden authentische Angriffsvektoren nachgebildet. Diese beinhalten unter anderem gängige Dateien für Endbenutzer-Geräte, wie infizierte PDF-Dokumente, ZIP-Archive, JavaScript, OneNote-Dateien oder Batch-Files. Zusätzlich kommen fortgeschrittene Techniken wie HTML Smuggling, Code Obfuscation, DLL Sideloading, Process Injection, Recursive DLL Injection, Ghostloading und File-less Infections zum Einsatz.

Der Quellcode aller nachgebildeten Angriffsvektoren ist vollständig einsehbar. Dies gewährleistet maximale Transparenz und stellt sicher, dass kein schädlicher Code verwendet wird.

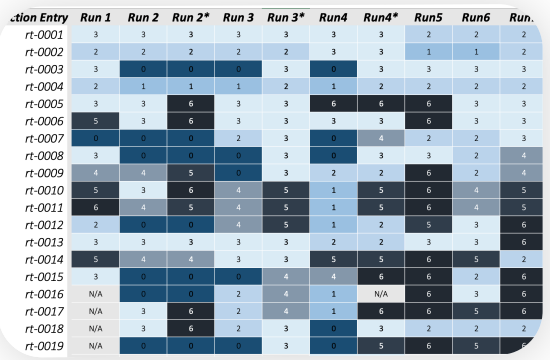
Attack Chain Emulation kommt gänzlich ohne Software-Agents aus.

Diese Methode ermöglicht Unternehmen eine realitätsnahe Bedrohungssimulation und die Entwicklung gezielter Abwehrstrategien, bevor ein tatsächlicher Angriff erfolgt.

KEY BENEFITS

- Validierung der Präventions- und Detektionsmassnahmen gegenüber aktuellen und realen Angriffen
- Einfaches Benchmarking mit Peers
- Prüfen der externen SOC Fähigkeiten
- Keine Installation, keine Agents notwendig
- Kostengünstig durch Automatisierung
- Simuliert reale Angriffe, keine fiktiven Szenarien
- Detailliertes Reporting für jede einzelne Angriffskette

Benchmark der Test Resultate



ction Entry	Run 1	Run 2	Run 2*	Run 3	Run 3*	Run4	Run4*	Run5	Run6	Run.
rt-0001	3	3	3	3	3	3	3	2	2	2
rt-0002	2	2	2	2	2	3	3	1	1	2
rt-0003	3	0	0	0	3	0	3	3	3	3
rt-0004	2	1	1	1	2	1	2	2	2	2
rt-0005	3	3	6	3	3	6	6	6	3	3
rt-0006	5	3	6	3	3	3	3	6	3	3
rt-0007	0	0	0	2	3	0	4	2	2	3
rt-0008	3	0	0	0	3	0	3	3	2	4
rt-0009	4	4	5	0	3	2	2	6	2	4
rt-0010	5	3	6	4	5	1	5	6	4	5
rt-0011	6	4	5	4	5	1	5	6	4	5
rt-0012	2	0	0	4	5	1	2	5	3	6
rt-0013	3	3	3	3	3	2	2	3	3	6
rt-0014	5	4	4	3	3	5	5	6	5	2
rt-0015	3	0	0	0	4	4	6	6	2	6
rt-0016	N/A	0	0	2	4	1	N/A	6	3	6
rt-0017	N/A	3	6	2	4	1	6	6	5	6
rt-0018	N/A	3	6	2	3	0	3	2	2	2
rt-0019	N/A	0	0	0	3	0	5	6	5	6

+41 (0)44 533 00 05 info@ioprotect.ch www.ioprotect.ch

Ihre Vorteile

Cyberbedrohungen und regulatorische Anforderungen entwickeln sich ständig weiter – eine einmalige Sicherheitsbewertung reicht daher nicht aus.

Eine regelmässige Sicherheitsvalidierung mit Attack Chain Emulation ermöglicht Unternehmen eine fortlaufende Einschätzung ihrer Sicherheitslage und die gezielte Optimierung ihrer Schutzmassnahmen (Security Controls).

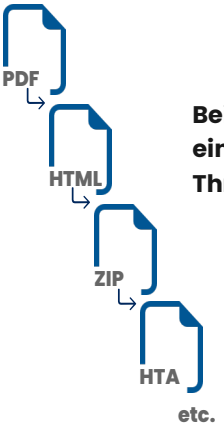
Zudem trägt eine regelmässige Validierung entscheidend zur Optimierung von Incident-Response-Plänen bei. Durch fortlaufende Tests können Schwachstellen im Krisenmanagement frühzeitig identifiziert und Notfallprozesse gezielt verbessert werden, sodass im Ernstfall schneller und effizienter reagiert werden kann.

Ein besonderer Vorteil von Attack Chain Emulation ist die Flexibilität der Angriffsszenarien. Unternehmen können gezielt auf branchenspezifische Bedrohungen eingehen und sich gleichzeitig gegen neuartige Angriffsmethoden wappnen. Dies gewährleistet eine praxisnahe Sicherheitsbewertung, die mit den realen Gefahren der digitalen Welt Schritt hält.

Im Gegensatz zu sporadischen Penetrationstests ermöglicht dieses Verfahren eine wiederkehrende, kosteneffiziente Überprüfung der gesamten IT-Infrastruktur. Dadurch erhalten Unternehmen nicht nur eine Momentaufnahme ihrer Sicherheitslage, sondern eine langfristige, datenbasierte Entscheidungsgrundlage.

Dank einer transparenten Berichterstattung lassen sich Massnahmen gezielt ableiten und fundierte Entscheidungen treffen. Dies schafft nicht nur Klarheit über die aktuelle Bedrohungslage, sondern ermöglicht auch eine strategische Weiterentwicklung der Sicherheitsarchitektur.

Attack Chain



Beispiel einer Angriffskette einer Advanced Persistent Threat Gruppe (APT).

Der initiale Angriff beginnt mit einer präparierten PDF-Datei, die eine eingebettete HTML-Datei enthält. Durch die Verwendung von JavaScript wird diese Datei geöffnet und leitet den nächsten Schritt der Infektionskette ein.
Innerhalb der HTML-Datei befindet sich ein ZIP-Archiv, das mithilfe der HTML-Smuggling-Technik unbemerkt auf das lokale System heruntergeladen wird. Nach dem erfolgreichen Download enthält das ZIP-Archiv eine HTA-Datei, die beim Ausführen zwei DLL-Dateien extrahiert und gemeinsam mit einem von Microsoft signierten Living-off-the-Land Binary (LOLBin), msoev.exe, nutzt, um den Angriff weiter voranzutreiben.

+41 (0)44 533 00 05 info@ioprotect.ch www.ioprotect.ch