Best Practices für die Anfrage zur sicheren Endgeräteabdeckung

Inhalt

Einleitung

In diesem Dokument wird der Prozess beschrieben, der verwendet werden muss, wenn Talos Coverage für eine bekannte Bedrohung angefordert wird, die bereits identifiziert wurde, aber derzeit von Secure Endpoint nicht erkannt wird.

Verschiedene Informationsquellen

Diese Bedrohungen können aus mehreren Quellen identifiziert und veröffentlicht werden. Hier einige der gebräuchlichen Plattformen:

- Veröffentlichte Cisco CVE
- Veröffentlichter CVE (Common Vulnerabilities and Exposures)
- Microsoft-Empfehlungen
- Bedrohungsinformationen von Drittanbietern

Cisco möchte sicherstellen, dass die Datenquellen legitim sind, bevor wir Talos dazu bringen, die Informationen zu überprüfen und die relevante Abdeckung zu identifizieren.

Um die Position von Cisco und die Abdeckung der fraglichen Bedrohungen zu überprüfen, müssen verschiedene Quellen von Cisco/Talos geprüft werden, bevor ein neuer Abdeckungsantrag gestellt werden kann.

Cisco Vulnerability Portal

Weitere Informationen zu CVEs von Cisco Produkten finden Sie in diesem Portal: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Talos-Portal

Das Talos Intelligence Portal muss als erster Bezugspunkt dienen, wenn diese Bedrohung untersucht wurde oder derzeit von Talos untersucht wird: https://talosintelligence.com/

Talos Blogs

Die Cisco Talos Blogs bieten auch Informationen zu den Bedrohungen, die von Talos ausgewertet und untersucht werden: https://blog.talosintelligence.com/

Die meisten relevanten Informationen finden wir unter "**Vulnerability Information",** die auch alle veröffentlichten "**Microsoft Advisories" enthält.**

Zusätzliche Untersuchung unter Verwendung von Cisco Produkten

Cisco bietet mehrere Produkte an, die dabei helfen können, die Bedrohungsvektoren/Hashes zu überprüfen

und festzustellen, ob ein sicheres Endgerät die Bedrohung abdeckt.

Cisco SecureX Cisco Threat Response Investigation (CTR)

Wir können die Bedrohungsvektoren im Rahmen von CTR-Untersuchungen untersuchen. Weitere Informationen finden Sie hier: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR ermitteln

Cisco XDR bietet erweiterte Funktionen zur Untersuchung von Bedrohungsvektoren. Weitere Informationen zu diesen Funktionen finden Sie hier:
https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Nützliche Cisco Blogs

Lesen Sie sich diese Blogs durch, um einige der im vorherigen Abschnitt behandelten Funktionen zu besprechen:

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

Nächste Schritte

Wenn wir die Bedrohungsvektoren nicht finden, die mit den obigen Schritten abgedeckt sind, können wir Talos-Abdeckung für die Bedrohung anfordern, indem wir eine TAC-Support-Anfrage einreichen.

https://www.cisco.com/c/en/us/support/index.html

Um die Evaluierung und Untersuchung für den Abdeckungsantrag zu beschleunigen, benötigen wir folgende Informationen zur Bedrohung:

- Quelle für Bedrohungsinformationen (CVE/Advisory/Third Party Investigation/Technotes/Blogs)
- Zugehörige SHA256-Hashes
- Beispiel der Datei (sofern verfügbar)

Sobald die Informationen verfügbar sind, bewertet Talos die Anfrage und prüft sie entsprechend.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.