Cisco Secure Endpoints Coverage Request Best Practices

Contents

Introduction

Different Sources of Information

- Cisco Vulnerability Portal
- Talos Portal
- Talos Blogs

Additional Investigation using Cisco Products

- Cisco XDR Investigate
- Useful Cisco Blogs

Next Steps

Overview

Introduction

This document describes the process that must be used when requesting Talos Coverage for a known threat that has already been identified but is not currently detected by Secure Endpoint.

Different Sources of Information

There can be multiple sources from which these threats are identified and published, and here are some of the commonly used platforms:

- Published Cisco CVE
- Published CVE (Common Vulnerabilities and Exposures)
- Microsoft Advisories
- 3rd Party Threat Intelligence

Cisco wants to ensure that the Data Sources are legitimate before we get Talos to review the information and identify the relevant coverage.

For reviewing Cisco's stance and coverage for the threats in question, we have various Cisco/Talos Sources that must be reviewed before requesting a new Coverage Request.

Cisco Vulnerability Portal

For any CVE related to Cisco Products, please review this Portal for more information: Cisco Vulnerability Portal

Talos Portal

Talos Intelligence Portal must be the first point of reference to review if this threat has been investigated or is currently under investigation by Talos: Talos Portal

Talos Blogs

Cisco Talos Blogs also provide information about the threats that are evaluated and investigated by Talos: Talos Blogs

We would be able to find most of the pertinent information under **"Vulnerability Information"** which also includes all the published **"Microsoft Advisories".**

Additional Investigation using Cisco Products

Cisco offers multiple products that can help in reviewing the Threat vectors/hashes and identifying if Secure Endpoint provides coverage for the threats.

Cisco XDR Investigate

Cisco XDR provides enhanced capabilities for investigating threat vectors, and more information on the functionality can be found here: Cisco XDR Investigate

Useful Cisco Blogs

Please review these blogs as they go over some of the functionalities discussed in the previous section such as Cisco Extended Detection and Response

Next Steps

If we do not find the Threat Vectors covered using the steps above, we can request Talos Coverage for the Threat by filing a TAC Support Request.

To expedite the evaluation and investigation for the Coverage Request, we would request this information:

- Source of the Threat Intelligence (CVE/Advisory/3rd Party Investigation/Technotes/Blogs)
- Associated SHA256 Hashes
- Sample of the File (If Available.)



Note: For coverage requests related to Penetration Testing or Red Teaming, the requirements may vary depending on the type of testing. In some cases, additional information may be required from the customer. Once the necessary information is provided, Talos reviews, evaluates, and investigates the request accordingly.

Overview

Once the required information is received, we begin a specialized review process. To ensure the highest level of protection, the timeline for delivery is guided by several critical factors:

Tailored Analysis
Because every threat scenario and customer environment is unique, we perform customized validation to ensure effective security coverage without disrupting your business operations.

Data-Driven Response
The speed of our analysis is directly supported by the availability of relevant telemetry, artifacts, or malware samples.

Rigorous Quality Assurance
To maintain product stability and reliability, every solution undergoes comprehensive testing and phased deployment.

Secure Release Management
We align updates with established release cycles to ensure all protections are delivered in a controlled and dependable manner.

Adaptive Protection
Security is an ongoing process. Following deployment, we continuously monitor and tune our detections to stay ahead of the evolving threat landscape.

Prioritization of Critical Issues
We evaluate every request individually. Issues involving high-severity vulnerabilities, active exploitation, or critical false positives are automatically fast-tracked through expedited workflows to minimize your risk exposure.

We appreciate your partnership as we work to deliver robust, accurate protection designed to keep your organization secure and productive.