Cisco Secure Endpoints Coverage Request Best Practices

Contents

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 Ciscoâ€™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: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

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: https://talosintelligence.com/

Talos Blogs

Cisco Talos Blogs also provide information about the threats that are evaluated and investigated by Talos: https://blog.talosintelligence.com/

We would be able to find most of the pertinent information under **â€œVulnerability Informationâ€¯** which also includes all the published **â€œMicrosoft Advisoriesâ€¯.**

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 SecureX Cisco Threat Response Investigation (CTR)

We can investigate the Threat Vectors as part of CTR investigations, and more information can be reviewed here: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR Investigate

Cisco XDR provides enhanced capabilities for investigating threat vectors, and more information on the functionality can be found here: https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Useful Cisco Blogs

Please review these blogs as they go over some of the functionalities discussed in the previous section:

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

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.

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

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

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

Once the information is available, Talos reviews evaluates, and investigates the request accordingly.