What are the Metrics Used to Determine the Default Ruleset for each Firepower Intrusion Base Policy

Contents

Introduction

Cisco Talos releases Snort Rule Updates (SRU) to address the latest threats and vulnerabilities. A new SRU release may contain updated rulesets for each base policy. This document explains the process used by the Talos for deciding how rules are assigned to each Intrusion base policy for Firepower devices.

Talos Base Policy Intent defined in rule metadata

The base policies are maintained by Metadata within the SRUs themselves. The state of any give rule in any of the default policies is defined in the metadata portion of the rule body. For example:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC 1.php outbound connection
attempt"; sid:38753; gid:3; rev:1; classtype:trojan-activity; metadata:engine shared, soid
3|38753, policy balanced-ips drop, policy security-ips drop, impact_flag red; )
```

Notice in the example rule shown above, the metadata section contains **policy balanced-ips drop, policy security-ips drop**.**This indicates thats this rule 1:38753 is enabled and set to drop in the *Balanced Security and Connectivity policy* as well as the *Security Over Connectivity policy*.**

Metrics Used to Determine Default Ruleset

- The main metric used is the Common Vulnerability Scoring System (CVSS) score assigned to each vulnerability that might be covered by a rule.
- The second metric is temporal based and concerns the age of a particular vulnerability.
- The final metric is the particular area of coverage for the rule. So for example, SQL Injection rules are considered to be important enough to have influence when being considered for policy inclusion.

Note: The vulnerabilities covered by the rules in these categories are considered important, regardless of age.

Connectivity over Security Base Policy

Note: The **Connectivity** policy is specifically designed to favor device performance over the security controls in the policy. It should allow a customer to deploy one of our devices with minimal false positives and full rated performance of the box in most network deployments. In addition, this policy should detect the most common and most prevalent threats our customers will experience.

1. CVSS Score must be 10

2. The vulnerability is from the last two years (inclusive). For example:

   - Current year (2019 for example)
   - Last year (2018 in this example)
   - Year before last (2017 in this example)

3. Rule Category

   - Not used for this policy

Balanced Base Policy

Note: The **Balanced** policy is the default policy that is recommended for initial deployments. This policy attempts to balance security needs and performance characteristics of our systems. Customers should be able to start with this policy and get a very good block rate with public evaluation tools, and relatively high performance rate with evaluation and testing tools. Additionally, this policy should perform at 80% of the rated capacity of the device under normal in the wild networking conditions. The main thing to always keep in mind with the Balanced policy is that this is the customers starting point, if they have a bad experience with false positives, limited detection, or poor performance most customers will investigate other devices for deployment in their infrastructure. It is the default shipping state of the Snort Subscriber Rule Set for Open-Source Snort sold on Snort.org.

1. CVSS Score 9 or greater

2. The vulnerability is from the last two years (inclusive). For example:

   - Current year (2019 for example)
   - Last year (2018 in this example)
   - Year before last (2017 in this example)

3. Rule Category

   - Malware-CnC

- Blacklist
- SQL Injection
- Exploit-kit

4. If the rule is in the **Connectivity** policy

Security over Connectivity Base Policy

> **Note**: The **Security** policy is designed for the small segment of our customer base that is exceptionally concerned about organizational security. Customers deploy this policy in protected networks, that have a lower bandwidth requirements, but much higher security requirements. Additionally, customers care less about false positives and noisy signatures. Application control, and locked down network usage are also concerns to customers deploying this policy. It should provide maximum protection, and application control, but should not bring the network down.

1. CVSS Score 8 or greater

2. The vulnerability is from the last three years (inclusive). For example:

- Current year (2019 for example)
- Last year (2018 in this example)
- Year before last (2017 in this example)
- Year prior (2016 in this example)

3. Rule Category

- Malware-CnC
- Blacklist
- SQL Injection
- Exploit-kit

4. If the rule is in the **Balanced** and **Connectivity** policy

Max-Detect (Maximum Detection) Base Policy:

> **Note**: The **Maximum Detection** ruleset is meant to be used in testing environments and as such is not optimized for performance. False Positives for many of the rules in this policy are tolerated and/or expected and FP investigations will normally not be undertaken.

1. The coverage is required for in-field testing.

2. Includes rules in the **Security**, **Balanced,** and **Connectivity** rule sets.

3. Includes all active rules above Sid: 10000, unless otherwise specified.

Frequency of Policy Updates

All new rules are placed into the policies based on these criteria. **Every year** the policies will be

re-assessed and rules from previous years, as the vulnerabilities age, will be removed from the policy to keep the policy compliant with our temporal selection criteria.

Should the CVSS score change for a particular vulnerability that is covered by a rule, it’s presence in a policy based on the CVSS metric is re-assessed.

Policies continually grow. Apart from major rebalanced to align them to a specific objective, major drops of rules from policies don't always happen if we are satisfied with the number of rules and the performance of the policy on the product

> **Note**: Base policies can grow apart from the yearly major rebalance to align them to a specific objective. Major drops of rules from policies don't always happen if Talos is satisfied with the number of rules and the performance of the policy on the product under normal network conditions. Rules in the listed policies are evaluated on a rule by rule basis. There will be some rules that are older and not in the criteria above that will be in the default policies. The above is the selection criteria for default rules, and is always subject to change based upon the threat landscape.

> **Note**: Rules in the listed policies are evaluated on a rule by rule basis. There will be some rules that are older and not in the criteria above that will be in the default policies. The above is the selection criteria for default rules, and is always subject to change based upon the threat landscape