SnortML

Type	Inspector (passive)
Usage	Inspect
Instance Type	Singleton
Other Inspectors Required	`snort_ml_engine, http_inspect`
Enabled	Max Detect

Every day new vulnerabilities are discovered in software critical to the function of the modern world. Security analysts take apart these new vulnerabilities, isolate what is necessary to trigger them, and write signatures to detect exploits targeting them. Most signatures can only really be written for specific vulnerabilities.

SnortML is a neural network-based exploit detection for the Snort intrusion prevention system. It is designed to not only learn to detect known attacks from training data, but also learn to detect attacks it has never seen before.

The `snort_ml` inspector searches primarily for SQL injection attacks over HTTP. As this inspector may affect performance, it is only enabled by default when in `Max Detect` mode.

SnortML Rules

Enable the `snort_ml` inspector rule to generate events and, in an inline deployment, drop offending packets. The `snort_ml` inspector rule is only enabled by default under the Maximum Detection NAP policy.

Table 1: Snort ML Inspector Rules

GID:SID	Rule Message
411:1	(snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection.

SnortML Parameters

uri_depth

Specifies the number of bytes to scan from the HTTP URI. The value `-1` means unlimited.

Type: integer

Valid range: `-1` to `2147483648`

Default value: `-1`

client_body_depth

Specifies the number of bytes to scan from the HTTP client body. The value `-1` means unlimited.

Type: integer

Valid range: `-1` to `2147483648`

Default value: `0`