Detection Rules

github.com/elastic/detection-rules

elastic

python 3.8+ Unit Tests passing chat #security-detection-rules ATT&CK Navigator

Detection Rules is the home for rules used by Elastic Security. This repository is used for the development, maintenance, testing, validation, and release of rules for Elastic Security's Detection Engine.

This repository was first announced on Elastic's blog post, Elastic Security opens public detection rules repo. For additional content, see the accompanying webinar, Elastic Security: Introducing the public repository for detection rules.

Table of Contents

Overview of this repository

Detection Rules contains more than just static rule files. This repository also contains code for unit testing in Python and integrating with the Detection Engine in Kibana.

folder	description
`detection_rules/`	Python module for rule parsing, validating and packaging
`detection_rules/etc/`	Miscellaneous files, such as ECS and Beats schemas
`kibana/`	Python library for handling the API calls to Kibana and the Detection Engine
`kql/`	Python library for parsing and validating Kibana Query Language
`rta/`	Red Team Automation code used to emulate attacker techniques, used for rule testing
`rules/`	Root directory where rules are stored
`tests/`	Python code for unit testing rules

Getting started

Although rules can be added by manually creating `.toml` files, we don't recommend it. This repository also consists of a python module that aids rule creation and unit testing. Assuming you have Python 3.8+, run the below command to install the dependencies:

```
$ pip install -r requirements.txt
Collecting jsl==0.2.4
  Downloading jsl-0.2.4.tar.gz (21 kB)
Collecting jsonschema==3.2.0
  Downloading jsonschema-3.2.0-py2.py3-none-any.whl (56 kB)
     |████████████████████████████████| 56 kB 318 kB/s
Collecting requests==2.22.0
  Downloading requests-2.22.0-py2.py3-none-any.whl (57 kB)
     |████████████████████████████████| 57 kB 1.2 MB/s
Collecting Click==7.0
  Downloading Click-7.0-py2.py3-none-any.whl (81 kB)
     |████████████████████████████████| 81 kB 2.6 MB/s
...
```

To confirm that everything was properly installed, run with the `--help` flag

```
$  python -m detection_rules --help

Usage: detection_rules [OPTIONS] COMMAND [ARGS]...

  Commands for detection-rules repository.

Options:
  -d, --debug / -n, --no-debug  Print full exception stacktrace on errors
  -h, --help                    Show this message and exit.

Commands:
  create-rule     Create a detection rule.
  dev             Commands for development and management by internal...
  es              Commands for integrating with Elasticsearch.
  import-rules    Import rules from json, toml, or Kibana exported rule...
  kibana          Commands for integrating with Kibana.
  mass-update     Update multiple rules based on eql results.
  normalize-data  Normalize Elasticsearch data timestamps and sort.
  rule-search     Use KQL or EQL to find matching rules.
  test            Run unit tests over all of the rules.
  toml-lint       Cleanup files with some simple toml formatting.
  validate-all    Check if all rules validates against a schema.
  validate-rule   Check if a rule staged in rules dir validates against a...
  view-rule       View an internal rule or specified rule file.
```

The contribution guide describes how to use the `create-rule` and `test` commands to create and test a new rule when contributing to Detection Rules.

For more advanced command line interface (CLI) usage, refer to the CLI guide.

How to contribute

We welcome your contributions to Detection Rules! Before contributing, please familiarize yourself with this repository, its directory structure, and our philosophy about rule creation. When you're ready to contribute, read the contribution guide to learn how we turn detection ideas into production rules and validate with testing.

Licensing

Everything in this repository — rules, code, RTA, etc. — is licensed under the Elastic License v2. These rules are designed to be used in the context of the Detection Engine within the Elastic Security application. If you’re using our Elastic Cloud managed service or the default distribution of the Elastic Stack software that includes the full set of free features, you’ll get the latest rules the first time you navigate to the detection engine.

Occasionally, we may want to import rules from another repository that already have a license, such as MIT or Apache 2.0. This is welcome, as long as the license permits sublicensing under the Elastic License v2. We keep those license notices in `NOTICE.txt` and sublicense as the Elastic License v2 with all other rules. We also require contributors to sign a Contributor License Agreement before contributing code to any Elastic repositories.

Questions? Problems? Suggestions?

- Want to know more about the Detection Engine? Check out the overview in Kibana.
- This repository includes new and updated rules that have not been released yet. To see the latest set of rules released with the stack, see the Prebuilt rule reference.
- If you’d like to report a false positive or other type of bug, please create a GitHub issue and check if there's an existing one first.
- Need help with Detection Rules? Post an issue or ask away in our Security Discuss Forum or the **#security-detection-rules** channel within Slack workspace.