ONLINE APPENDIX: How It's Made: Uncovering Detection Engineering Processes for Network Intrusion Detection Rules

Anonymous author(s)

Anonymous

A Recruitment message

Dear CTF enthusiasts / students,

Can you write the best network intrusion detection rules?

On [Date] starting at [Time] in [On-Campus Location], we will be organizing a fun and educational activity in the form of a Capture the Flag in which you will focus on writing network intrusion detection rules using Suricata. We have developed a platform for the CTF, which will give you continuous feedback as you are writing Suricata rules and competing with the other participants for a place on the leaderboard. The activity is open to all students and non-students, so you may forward this as an invitation to friends from other courses to take part in this CTF as well.

The day will be an excellent opportunity to learn more about network intrusion detection, and Suricata in particular. We have previously run the CTF before in [City] and it was very well-received. Based on the feedback we received we are confident it will be an exciting and interesting experience for you even if you have never worked with Suricata or intrusion detection before.

During the activity you will work on several network scenarios for which you will be asked to engineer a network intrusion detection rule using Suricata. While you are writing these rules, you can compete (anonymously, if you wish) with other participants for a place on the leaderboard.

When you sign up for the activity, you will fill in a short survey with contact information. Optionally (but desirably) if you accept the informed consent form, you will be presented several additional questions regarding your experience in related topics. If you do so, we will use your answers combined with the rules you write during the CTF in an anonymized way to conduct our research on the engineering of (better) network intrusion detection rules.

In preparation for the Capture the Flag, you will receive some instruction materials in the form of a video lecture that will inform you about the setup and some basics regarding Suricata. You can watch this video lecture any time before the CTF that suits you best (possibly from the comfort of your home).

Sign up for the activities using this link: [Enrollment Form URL] Although registration will remain open, you should register before the end of [Date].

If you have any questions in the meantime, please do not hesitate to contact us. ([Author Email])

Kind regards, [Author Name]

Participation is anonymous, voluntary; and you can withdraw consent at any time. (Non-)participation in the activity and/or research, as well as performance during the activity have zero consequences for course outcomes.

B Instruction contents

As part of the preparatory instruction practical aspects of Wireshark [2], a tool to inspect network traffic captures, are covered by discussing commonly used features such as protocol recognition, display filters, and the following of streams. Subsequently, the concept of intrusion detection is generally introduced and Suricata is covered more in-depth by explaining the rule syntax and highlighting common functional keywords including `content`, `file.data`, `flow`, `flowbits`, and `threshold` as well as transformations, modifiers, and protocol-specific keywords for DNS, HTTP, and TLS. The existence of other options is emphasized with reference to the official Suricata documentation [1], which is also accessible through the platform interface. Moreover, we exemplify how a minimal rule containing all mandatory keywords can be constructed. This instruction also explains the various scenarios that users will tackle during the activity, highlighting why one would want to detect such scenarios and potentially relevant information without prescribing a characteristic that they should focus on. The general instruction ends with some practical details on the employed platform and the leaderboard scoring method, as well as an explanation of the User Interface (UI) through a live demonstration. The general instruction takes approximately one hour.

C Questionnaires

Appendix C.1 contains the contents of the intake questionnaire presented to participants when they enroll for our study. Thereafter, **??** describes how the experience of participants is assessed using the questionnaire responses to derive the experience scores that were used in the regression presented in **??**.

C.1 Intake questionnaire

Question 1: What is the email address you would like us to contact you on?

Question 2: What is the username you would like to reflect your performance on the leaderboard?

Question 3: Are you 16 years or older?

(a) Yes

(b) No

[Informed Consent Form with details about the study, as well as contact details, etc.]

Question 4: By selecting "yes" below, I confirm:

1. I have enough information about the research project from the separate information sheet. I have read it and I had the chance to ask questions, which have been answered to my satisfaction.
2. I take part in this research project voluntarily. There is no explicit or implicit pressure for me to take part in this research project and I understand I can stop my participation at any moment, without explaining why. I do not have to answer any question I do not want to answer.
3. I know my personal data will be collected and used for the research, as explained to me in the information sheet.

(a) Yes
(b) No

Question 5: How did you first learn about the CTF activity?

(a) Promotion channel 1 (e.g., course)
(b) Promotion channel 2 (e.g., CTF association)
(c) ...

Question 6: What is your gender?

(a) Male
(b) Female
(c) Other
(d) I prefer not to disclose

Question 7: What is the highest level of education that you have completed?

(a) Primary education (ISCED 1)
(b) Lower secondary education (ISCED 2)
(c) Upper secondary education (ISCED 3)
(d) Post-secondary non-tertiary education or Short-cycle tertiary education (ISCED 4 or 5)
(e) Bachelor's or equivalent (ISCED 6)
(f) Master's or equivalent (ISCED 7)
(g) Doctorate or equivalent (ISCED 8)

Question 8: What is your level of expertise regarding Capture the Flags (or similar activities)?

(a) I have never heard of a Capture the Flag.
(b) I know what a Capture the Flag is but have never participated in one.
(c) I have previously participated in a Capture the Flag.
(d) I have participated in multiple Capture the Flags.

(e) I have previously organized a Capture the Flag.

Question 9: Do you have any other relevant experiences (such as a job related to Security Operations or high expertise in another area you deem relevant) that may be relevant for the research? If so, describe the topic and the relevant experience below.

Question 10: How does the TCP protocol ensure that the packets are delivered in the correct order?

(a) Through the use of SYN and ACK flags.
(b) Through the encryption and decryption of data packets.
(c) Through the use of sequence and acknowledgment numbers.
(d) Through the use of checksums.
(e) I do not know.

Question 11: What types of information can be exchanged during the initiation of a TLS session?

☐ Plain-text HTTP requests
☐ Server and client Hello messages
☐ Encrypted handshake messages
☐ Certificate
☐ I do not know.

Question 12: Which of the following statements regarding network scanning are true?

☐ Lack of response (SYN,ACK) to a TCP SYN implies a port is closed.
☐ If a vulnerability scanner detects a vulnerability, the scanned device has an exploitable vulnerability.
☐ Nmap can only perform UDP/TCP scans.
☐ If you want to know which ports may be open on a public-facing IP address, you must scan it.
☐ Network scanning may be used to inspect application layer features such as used software and versions.
☐ I do not know.

Question 13: Which of the following statements regarding Cross-Site Scripting (XSS) are true?

☐ During a successful XSS attack malicious code is executed on a server distributing content.
☐ XSS attacks may be prevented through input sanitization.
☐ XSS attacks can be used to steal credentials.
☐ During a successful XSS attack the attacker may execute malicious code within the web browsers of other users visiting a website.
☐ XSS attacks are considered to be a subset of SQL injection attacks.
☐ I do not know.

Question 14: Which of the following statements regarding Persistence are true?

☐ Persistence always implies that following a malware infection, malware will remain present after reinstallation of the operating system.
☐ Persistence must be obtained in order for malware to accomplish its goal.
☐ In order to obtain persistence, malware must add an executable file to the startup folder on Windows.
☐ Metasploit is a tool that may be used to obtain persistence depending on the targeted system.
☐ Persistence always has associated network traffic.
☐ I do not know.

Question 15: What is/are (a) feature(s) offered by Wireshark?

☐ Filtering of packets
☐ Decoding of transmitted data
☐ Blocking network traffic
☐ Decrypting all encrypted network traffic
☐ Producing network I/O statistics
☐ Inspecting raw bytes transmitted in streams
☐ I do not know.

Question 16: What is the purpose of the ip.addr==192.168.178.1/24 filter in Wireshark?

(a) To only show network packets originating from the subnet 192.168.178.1/24
(b) To only show network packets sent to the subnet 192.168.178.1/24
(c) To only show network packets originating from or sent to the subnet 192.168.178.1/24
(d) To only show network packets originating from and sent to the subnet 192.168.178.1/24
(e) It is an invalid filter.
(f) I do not know.

Question 17: This question is just to check if you are actually reading questions carefully. It is an attention check. If you read this, please click the third option.

(a) HTTP
(b) DNS
(c) SSH
(d) TLS
(e) UDP
(f) TCP
(g) I do not know.

Question 18: Which of the following statements regarding different intrusion detection paradigms are true?

☐ Signature-based intrusion detection methods always rely on Atomic Indicators of Compromise (IOCs).
☐ Anomaly-based intrusion detection methods always rely on machine learning.
☐ Signature-based intrusion detection methods primarily rely on knowledge of malicious behaviors.
☐ Anomaly-based intrusion detection methods primarily rely on knowledge of benign behaviors.
☐ Anomaly-based intrusion detection methods are a subset of signature-based intrusion detection methods.
☐ I do not know.

Question 19: What are built-in functionalities offered by Suricata?

☐ Matching bytes at specific locations
☐ Stateful detection across different flows in which the same IP address is involved
☐ Matching specific traffic directions
☐ Decoding of certain HTTP buffers
☐ Stateful detection within the same flow
☐ Matching using a remote API
☐ Matching using regular expressions
☐ I do not know.

Question 20: Which of the following buffers would be matched by the following sequence of Suricata options:
CONTENT:"FOO"; CONTENT:"BAR"; DEPTH:5;

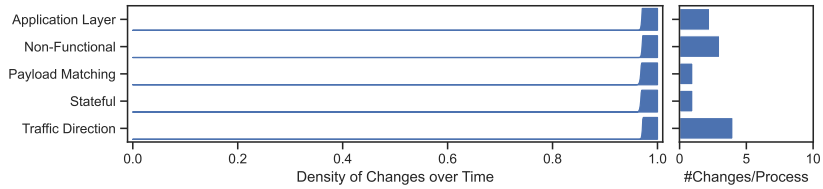
☐ FOObar
☐ barFOO
☐ foobar
☐ barfoo
☐ I do not know.

Question 21: Read the following Suricata documentation and select the factually correct statements one can derive from the given sentence.
[SURICATA DOCUMENTATION SNIPPET ON *STARTSWITH* AND *DOTPREFIX*]
Now consider a typical DNS request to *google.com* Which of the following rules are valid rules and will match this request?

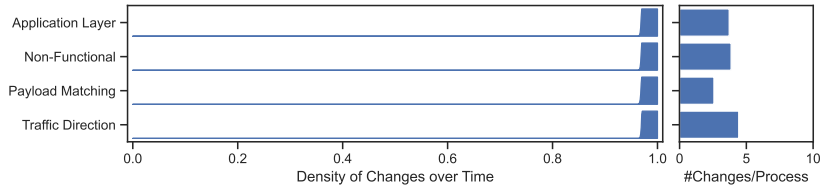
☐ alert dns any any → any 53 (msg:"DNS Request to google.com"; dns.query; content:"google.com"; startswith; sid:1;)
☐ alert dns any any → any 53 (msg:"DNS Request to google.com"; dns.query; content:".google.com"; startswith; sid:1;)
☐ alert dns any any → any 53 (msg:"DNS Request to google.com"; dns.query; dotprefix; content:"google.com"; startswith; sid:1;)
☐ alert dns any any → any 53 (msg:"DNS Request to google.com"; dns.query; dotprefix; content:".google.com"; startswith; sid:1;)
☐ alert dns any any → any 53 (msg:"DNS Request to google.com"; dns.query; content:"google.com"; startswith; dotprefix; sid:1;)
☐ alert dns any any → any 53 (msg:"DNS Request to google.com"; dns.query; content:".google.com"; startswith; dotprefix; sid:1;)
☐ I do not know.

D Detailed cluster overviews

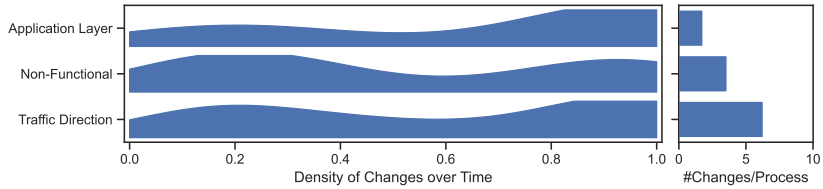
Figure 1 contains the detailed overview of the clusters described in **??** similar to how the expert cluster is depicted in **??**



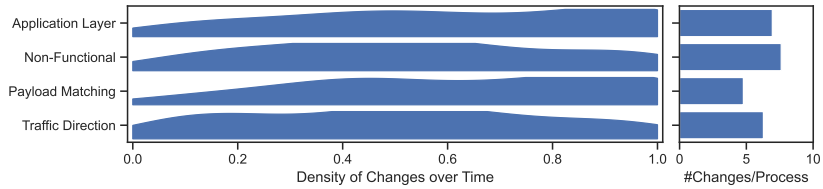
(a) Cluster 0



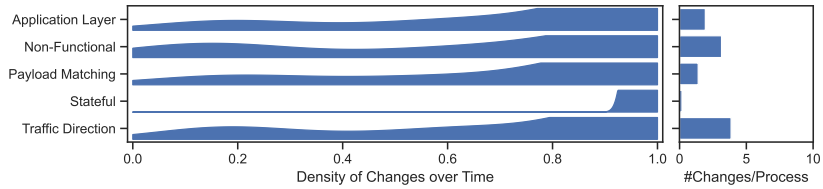
(b) Cluster 1



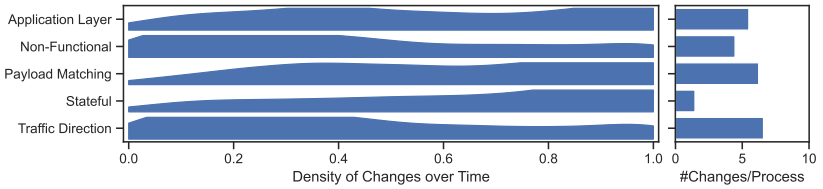
(c) Cluster 2



(d) Cluster 3



(e) Cluster 4



(f) Rejected engineering processes

Fig. 1: Detailed overview of the five clusters of engineering processes and the group of rejected engineering processes, depicting within each subfigure, the changes made over time (left), and the number of changes per category (right).

References

1. Fernandes, G., Rodrigues, J.J.P.C., Carvalho, L.F., Al-Muhtadi, J.F., Proença, M.L.: A comprehensive survey on network anomaly detection. Telecommunication Systems **70**(3), 447–489 (2019). https://doi.org/10.1007/s11235-018-0475-8. http://link.springer.com/10.1007/s11235-018-0475-8
2. Wireshark, (2025). https://www.wireshark.org/ (visited on 02/13/2025)