Credible Threat Detection? Measuring Contribution Dynamics and Quality Control in a Crowdsourced Threat Detection Ecosystem

Apurva Virkud, Gang Wang, Adam Bates
University of Illinois Urbana-Champaign







Small & Medium-sized Businesses (SMBs) Face Increasing Attacks

One in three SMBs have been victims of a cyberattack

Cyber-attacks on small firms: The US economy's 'Achilles heel'?

Smaller organizations nearing cybersecurity breaking point

Cyberattacks Could Shutter One In Five Small Businesses, Report Finds

New Data Shows 80% of SMBs Recognize Their Cyber Vulnerabilities, but Significant Resource Constraints Keep Them at Risk

Cyberattacks are on the rise, and that includes small businesses. Here's what to know

Small & Medium-sized Businesses (SMBs) Face Increasing Attacks

SMBs often rely on Managed Security Service Providers (MSSPs) for their security needs.

New Data Shows 80% of SMBs Recognize Their Cyber Vulnerabilities, but Significant Resource Constraints Keep Them at Risk

Services include:
- Firewall
- Managed detection and response
- Threat hunting

Open-source Threat Detection is Critical to SMB Security

MSSPs are sourcing threat detections from open-source repositories!



Open-source Threat Detection

Application or Platform Specific

Crowdsourced

Commercial and Open-Source

wazuh.

panther

Sublime Security

Open-source Threat Detection

Application or Platform Specific

Crowdsourced

Commercial and Open-Source

wazuh.

panther

Sublime Security

elastic

splunk>

Open-source Threat Detection

Application or Platform Specific

Crowdsourced

Commercial and Open-Source

wazuh.

panther

Sublime Security



Sigma

SIEM Detection Format

elastic

splunk>

Open-source Threat Detection

Application or Platform Specific

wazuh.

panther

Sublime Security

Crowdsourced



Sigma

SIEM Detection Format

Commercial and Open-Source



elastic



How are threat detection rules developed?

Dataset

	Sigma	Splunk	Elastic
Type of Ruleset	crowdsourced	commercial, open-source	commercial, open-source
Number of Rules	3,543	1,797	1,503

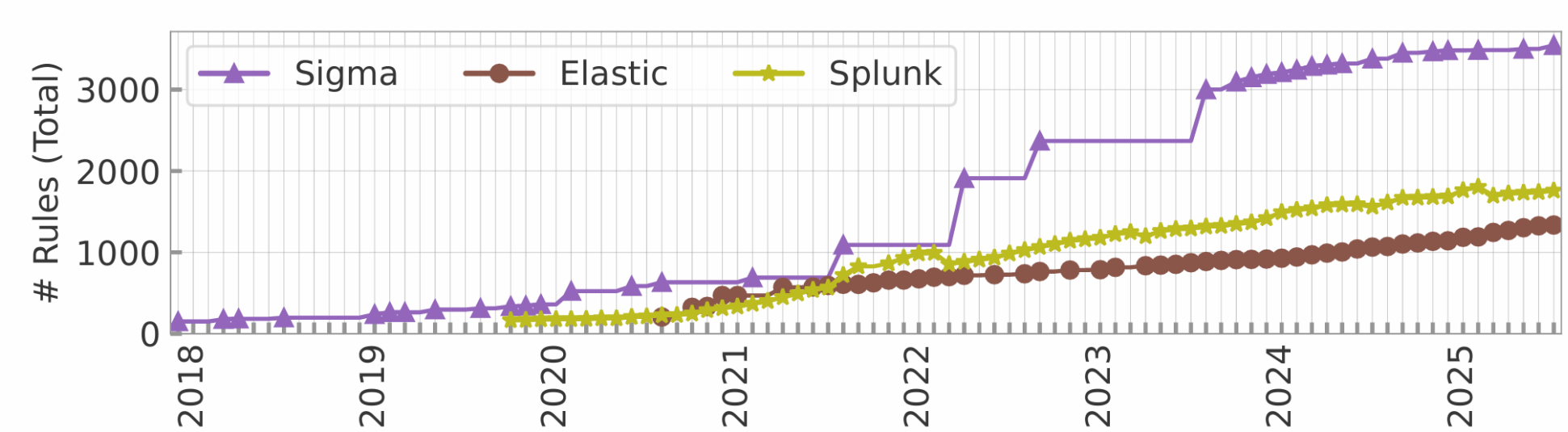
```
detection:
  selection:
    ParentImage|endswith: '\UMWorkerProcess.exe'
  filter:
    Image|endswith:
      - 'wermgr.exe'
      - 'WerFault.exe'
  condition: selection and not filter
```

Example Sigma Rule: CVE-2021-26857, abnormal child processes from Exchange Server's Unified Messaging service

Research Questions

1. **What are the dynamics of rule contribution?**
2. Who are the rule contributors and downstream users?
3. What quality control processes are in place?
4. How does Sigma compare to major commercial systems?

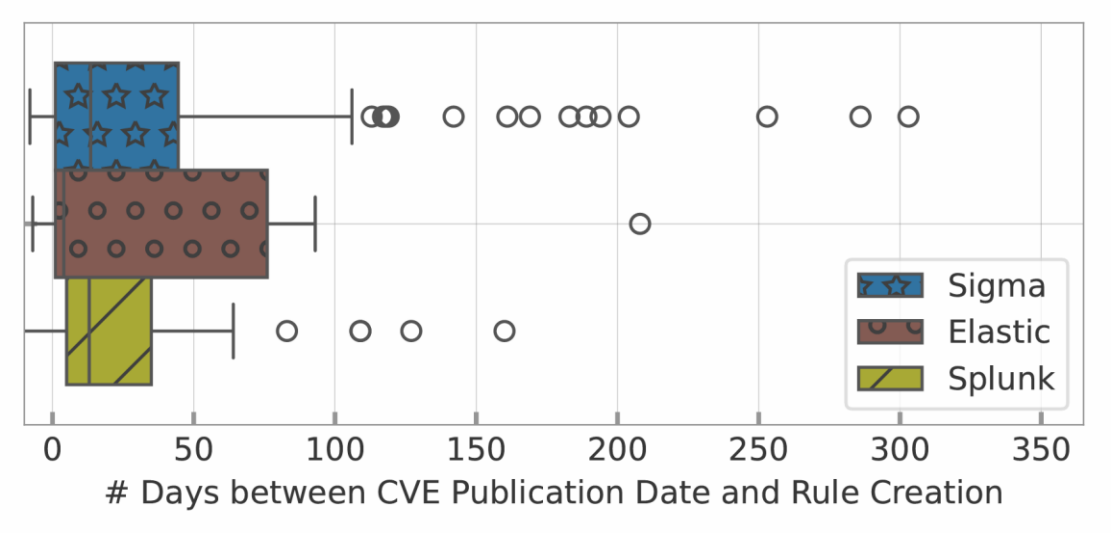
Longitudinal Rule Activity



Findings:

- There is a steady increase in total rules over all three repositories, although Sigma began to outpace Splunk and Elastic in rule additions in 2022.

Reactivity to CVEs



Findings:

- There is not a statistically significant difference between the CVE reactivity of any of the three rulesets.

Rule Modifications

Overall Scope	Selection Scope	Filter Scope	% Mods
Decreased	No Change Decreased Decreased	Increased Increased No Change	61.6%
Increased	Increased Increased No Change	No Change Decreased Decreased	33.4%
Unknown	Increased Decreased	Increased Decreased	5.0%

Findings:

- Rules are modified primarily to address false positives.
- *CommandLine* and *Image* were the most common subjects of modification.

Rule Modifications

Overall Scope	Selection Scope	Filter Scope	% Mods
Decreased	No Change Decreased Decreased	Increased Increased No Change	61.6%
Increased	Increased Increased No Change	No Change Decreased Decreased	33.4%
Unknown	Increased Decreased	Increased Decreased	5.0%

Decrease in selections or an increase in filters corresponds to false positive reduction

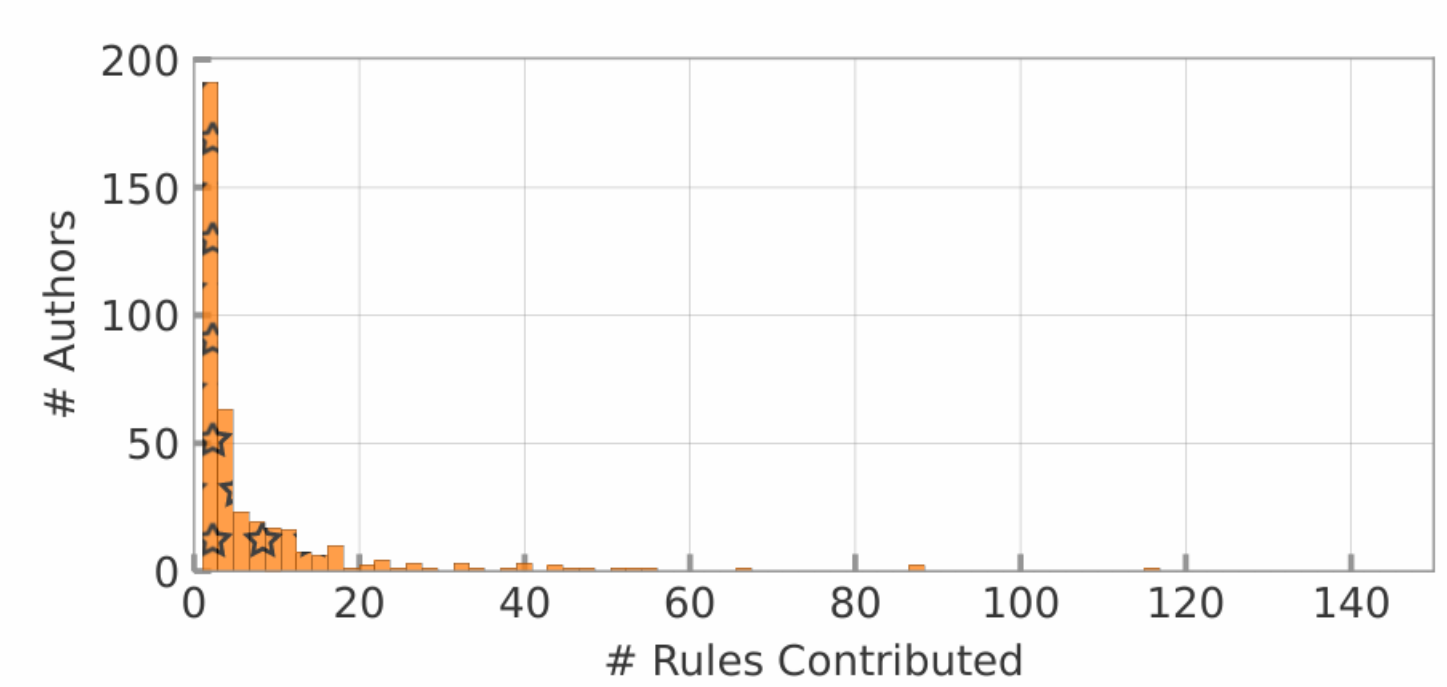
Findings:

- Rules are modified primarily to address false positives.
- *CommandLine* and *Image* were the most common subjects of modification.

Research Questions

1. What are the dynamics of rule contribution?
2. **Who are the rule contributors and downstream users?**
3. What quality control processes are in place?
4. How does Sigma compare to major commercial systems?

Contributing Authors

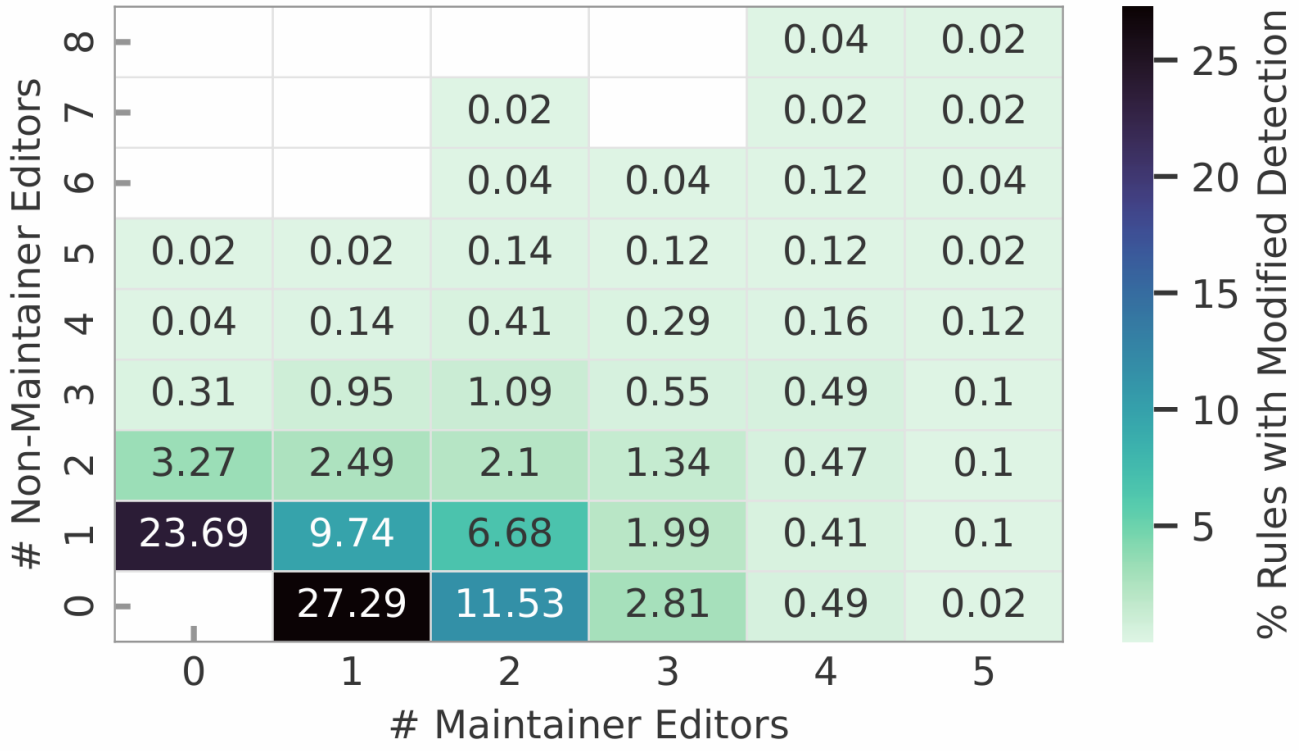


Maintainers have authored > 150 rules and are not visible on this figure

Findings:

- Sigma's contributor patterns resemble that of other open-source communities: a small maintainer team that authors many rules and a large group of external contributors that each author a handful of rules.

Crowdsourced Editing

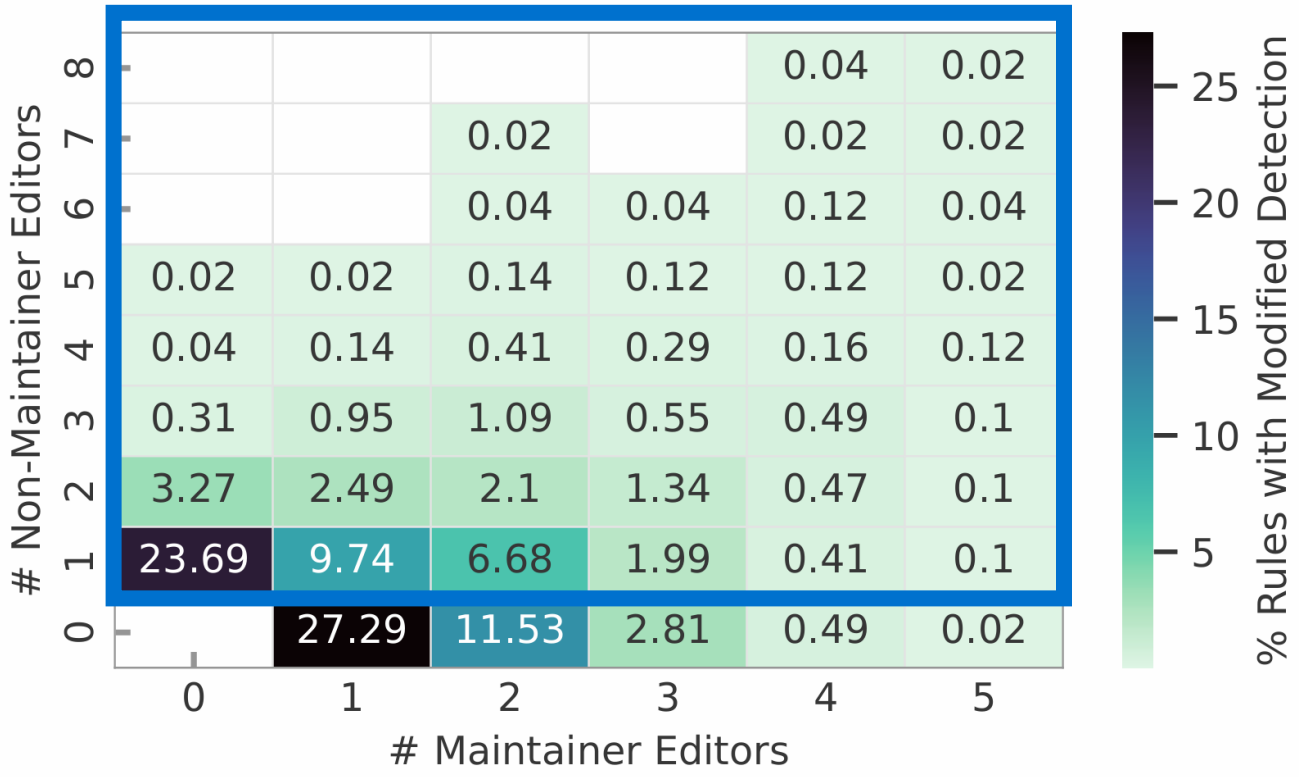


Findings:

- Non-maintainers play an active role in editing rules, with 57.9% of rules modified by at least one non-maintainer.

The bottom row represents the % of rules edited by only maintainers. The remaining cells sum to 57.9%, or rules edited by at least one non-maintainer.

Crowdsourced Editing



Findings:

- Non-maintainers play an active role in editing rules, with 57.9% of rules modified by at least one non-maintainer.

The bottom row represents the % of rules edited by only maintainers. The remaining cells sum to 57.9%, or rules edited by at least one non-maintainer.

Contributing Organizations

Organization	# Contributors	# Rules Authored	# Rules Edited
Nextron Systems	13	2,124	2,030
Microsoft	13	180	18
HAWK.io	1	66	76
Elastic	3	106	1
Positive Technologies	5	21	45
Zero Networks	2	17	17
Splunk	4	25	1
SCYTHE	1	22	0
Artic Wolf	3	0	17
Kaspersky	2	4	14
Other Organizations	153	887	313

Findings:

- Sigma benefits from the expertise of contributors that work for security vendors and other security-relevant roles.

Research Questions

1. What are the dynamics of rule contribution?

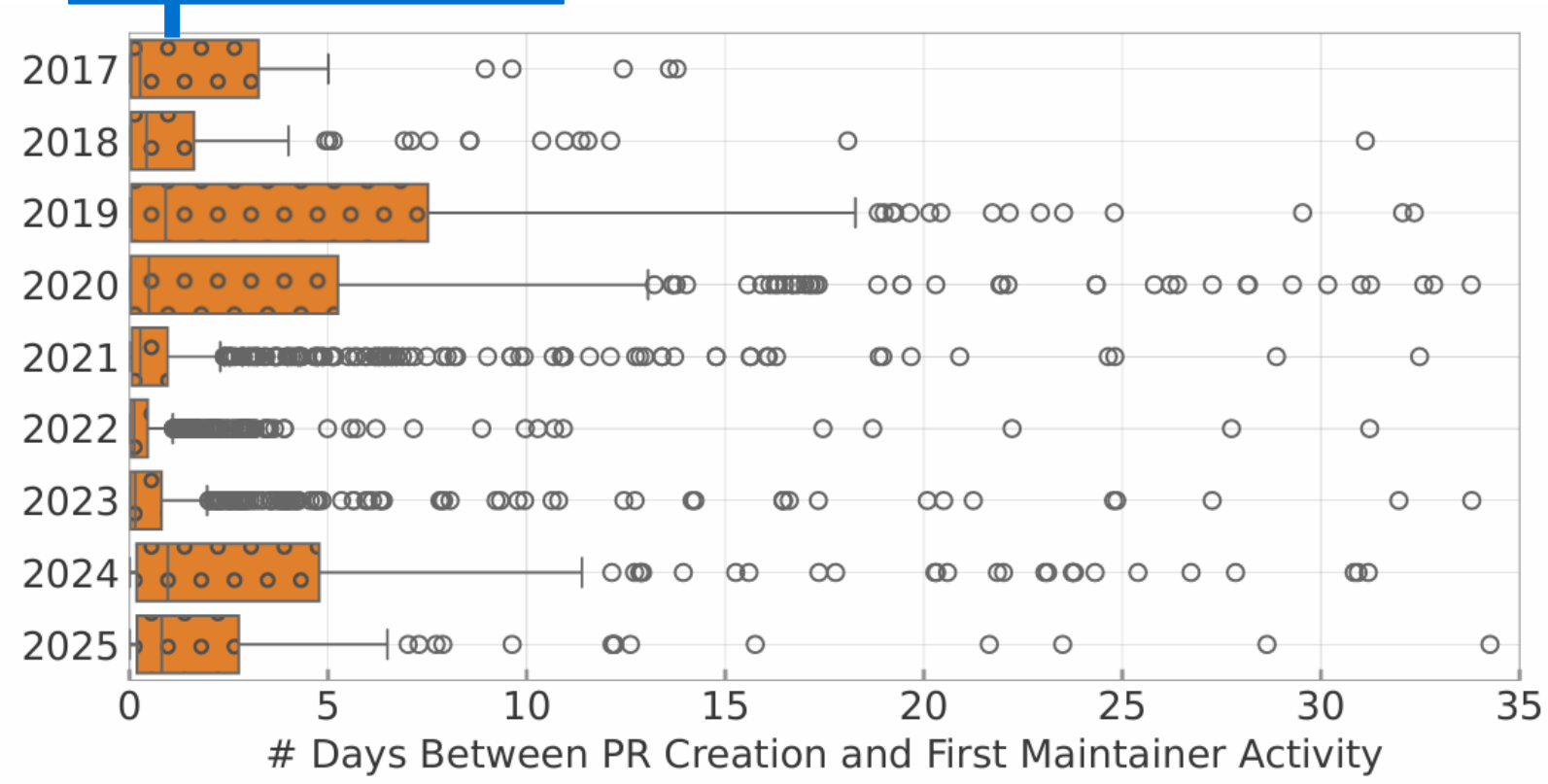
2. Who are the rule contributors and downstream users?

3. **What quality control processes are in place?**

4. How does Sigma compare to major commercial systems?

Pull Request Review

medians also ~1 day



Findings:

- Maintainers have had a rapid response time to new PRs consistently over the repository history, within a day on average.

Reasons for Rejecting PRs

Reasoning	# PRs	Example
Closed by PR Author	262	#3777
Repository Management	151	#4147
Overlapping or Duplicate Rule	65	#2916
Rule Quality	29	#700
Additional Discussion Required	11	#2502
Total	518	

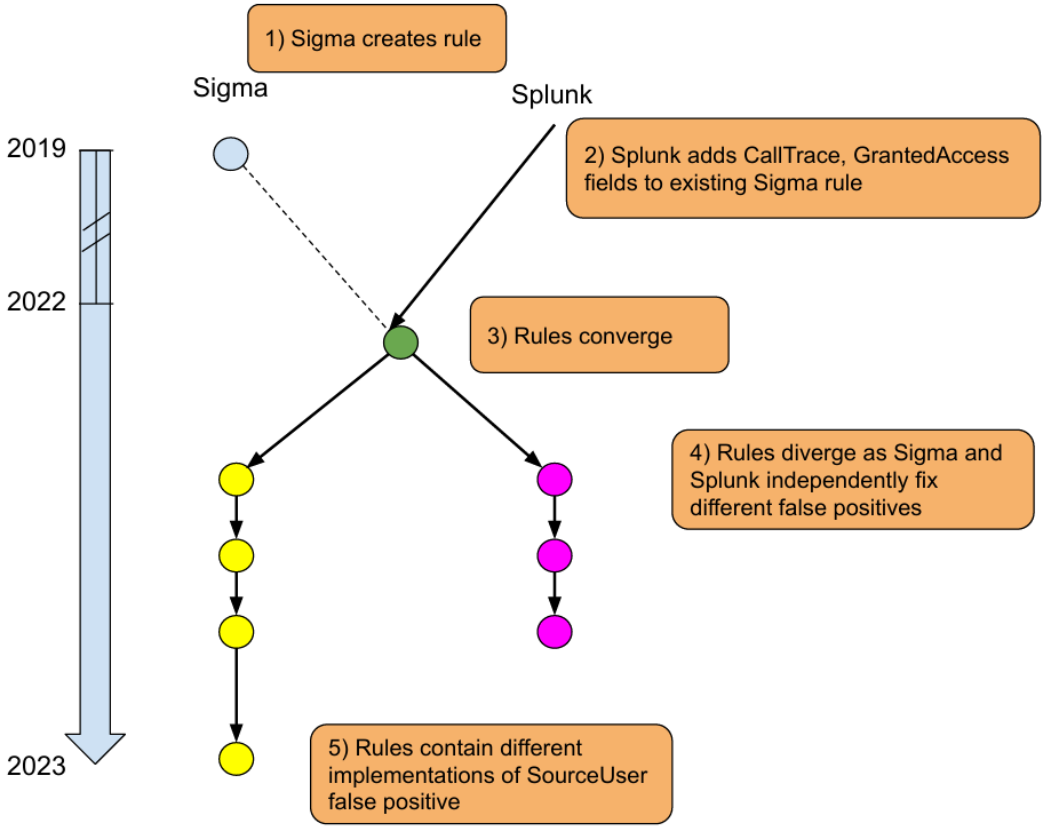
Findings:

- Rejected PRs reflect common low-level issues from crowdsourcing, such as inexperienced authors and general repository management. However, other PRs indicate how the quality control process manifests specific to evaluating threat detection rules.

Research Questions

1. What are the dynamics of rule contribution?
2. Who are the rule contributors and downstream users?
3. What quality control processes are in place?
4. **How does Sigma compare to major commercial systems?**

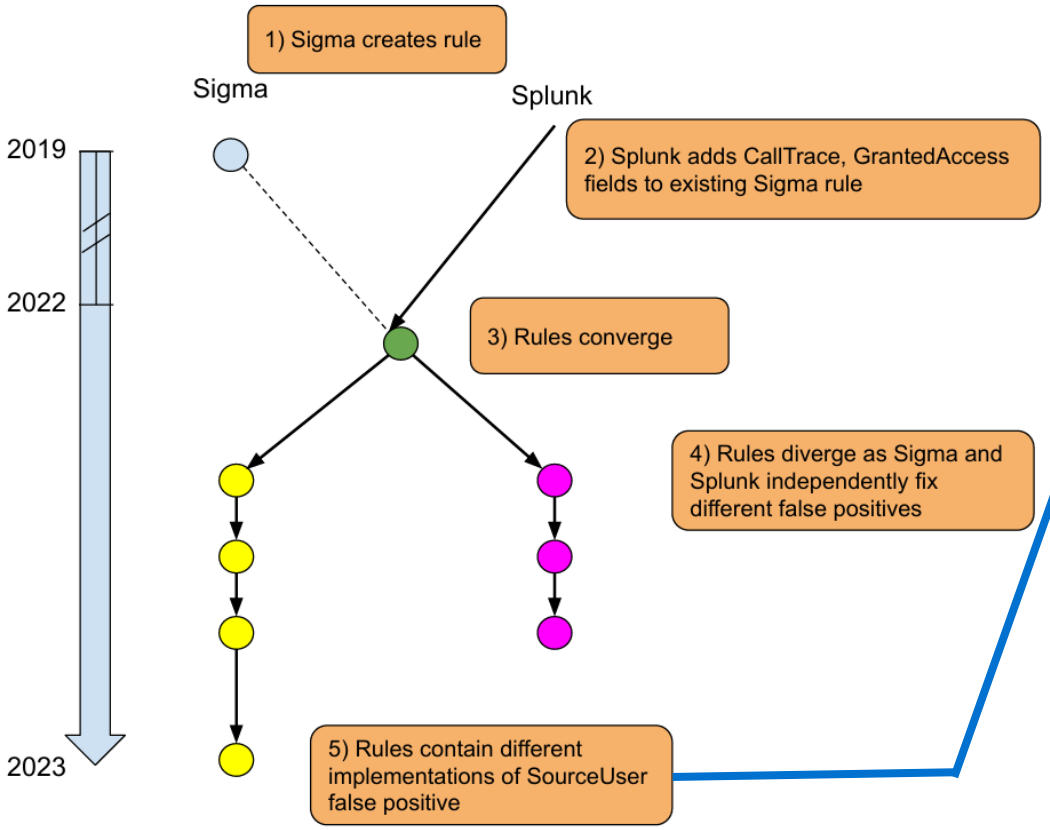
Convergence and Divergence of Credential Dumping Rule



Findings:

- Crowdsourcing enables widespread collection of false positive sources.
- The updated false positive filter permits adversary to potentially evade detection.

Convergence and Divergence of Credential Dumping Rule



Sigma:
SourceUser|contains: “AUTHORI” or “AUTORI”

Splunk:
SourceUser: “NT AUTHORITY\\SYSTEM”

Findings:

- Crowdsourcing enables widespread collection of false positive sources.
- The updated false positive filter permits adversary to potentially evade detection.

Takeaways

1. What are the dynamics of rule contribution?

   Sigma's rule base has steadily increased over time, with rules being consistently modified to address false positives and negatives.

2. Who are the rule contributors and downstream users?

   Sigma has an active community of contributors from other security vendors and the broader industry.

3. What quality control processes are in place?

   Sigma's quality control process relies on the institutional knowledge of a small group of maintainers, although it has moved to a more systematic review process in recent years.

4. How does Sigma compare to major commercial systems?

   Sigma's crowdsourcing enables iteration on vendor-provided rules based on widespread FP identification; however, these FP updates can also permit evasion.

Operationalizing Our Findings

- We introduce a tool to detect overlapping and duplicate rules, with 78.7% efficacy on our ground truth dataset.
- There is potential for further (semi-)automatic evaluation of rules (e.g., using a model to identify general heuristics for variable assignments within detection rules).
- Future work may also investigate how inexperienced contributors can be trained to write threat detection rules.

Thank you!

Credible Threat Detection? Measuring Contribution Dynamics and Quality Control in a Crowdsourced Threat Detection Ecosystem

Apurva Virkud, Gang Wang, Adam Bates

University of Illinois Urbana-Champaign

avirkud.github.io





