

You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks

Rafael Uetz^{*} Marco Herzog^{*} Louis Hackländer^{*} Simon Schwarz[†] Martin Henze^{‡,*}

^{*}*Fraunhofer FKIE*

[†]*University of Göttingen*

[‡]*RWTH Aachen University*

arXiv preprint arXiv:2311.10197 (2023)

Outline

- Introduction
 - SIEM
 - Sigma
- Analysis of SIEM Rules for Evasions
- Overview
- Approach
- Evaluation
- Limitations and Discussion
- Conclusion

Introduction

- Security Information and Event Management (SIEM)
 - Organizations utilize SIEM to collect **security-related events** and scan them using expert-written detection **rule-sets**

IBM Security QRadar SIEM

重新定义 SIEM，释放分析师的潜力，凭借速度、规模和准确性超越对手

开始免费试用 →

估算定价 →

- 端点安全 (EDR、XDR、MDR)
- 日志管理
- SIEM
- SOAR

The screenshot shows the 'Events - All Events' page in the IBM Security QRadar SIEM console. The left sidebar contains a 'FILTERS' section with an 'Overview' tab and a 'Security' tab. The 'Overview' tab shows counts for 'All Events' (3726), 'Subscriptions' (0), 'SEM Internal Events' (80), 'New Unmatched Connector Data' (0), and 'Rule Activity' (32). The 'Security' tab shows counts for 'Incidents' (17), 'Security Events' (16), 'Network Event Threats' (0), 'All Firewall Events' (27), 'All Threat Events' (60), 'Unusual Network Traffic' (8), 'Blocked Web Traffic' (0), 'Virus Attacks' (2), and 'IDS Scan/Attack Activity' (2). The main table displays a list of events with columns: NAME, EVENT INFO, DETECTION IP, and DETECTION TIME. The table shows 2000 latest items, and there is an 'Export to CSV' button.

NAME	EVENT INFO	DETECTION IP	DETECTION TIME
WebTrafficAudit	URL Access By megatron.corp.trigeo.com	192.168.168.10	2019-06-20 15:24:01
MachineLogon	Network Logon "CORP\CTX\$"	WALLACE	2019-06-20 15:24:01
MachineLogoff	Logoff "CORP\CTX\$"	WALLACE	2019-06-20 15:24:01
PolicyScopeChange	Privilege assigned to "\CTX\$"	WALLACE	2019-06-20 15:24:01
ServiceWarning	duplex mismatch discovered on Fast	192.168.168.204	2019-06-20 15:23:59
ConfigurationTrafficAudit	DHCP: Renew from 192.168.168.48 ()	192.168.168.5	2019-06-20 15:23:55
SystemStatus	56 connections in use	192.168.167.1	2019-06-20 15:23:55
TCPTrafficAudit	Deny TCP (no connection)	192.168.167.1	2019-06-20 15:23:53
RegistryDelete	Registry Value Delete "\REGISTRY...	10.110.250.54	2019-06-20 15:23:53
WebTrafficAudit	Secure URL Access By scotty.corp.trigeo...	192.168.168.10	2019-06-20 15:23:47
RegistryRead	Registry Value Read "\REGISTRY...	10.110.250.54	2019-06-20 15:23:46
RegistryRead	Registry Key Read "\REGISTRY...	10.110.250.54	2019-06-20 15:23:45

security-related events

The screenshot shows the 'All rules' page in the IBM Security QRadar SIEM console. The page displays a list of rules with columns: Rule, Risk score, Severity, Last run, Last response, Tags, and Activated. The table shows 29 rules, and there is a 'Refresh' button. The rules are categorized into 'Elastic rules (0)' and 'Custom rules (29)'.

Rule	Risk score	Severity	Last run	Last response	Tags	Activated
Host Without Firewall	50	Medium	Sep 1, 2020 @ 10:40:43.328	succeeded	CSC3, CSC3.4	On
Default Credentials Usage	50	Medium	Sep 1, 2020 @ 10:40:43.345	succeeded	CSC4, CSC4.2	On
Minikatz through Windows Remote Management	50	Medium	Sep 1, 2020 @ 10:35:46.074	succeeded	attack.credential_access	On
CMSTP Execution	50	Medium	Sep 1, 2020 @ 10:35:47.089	succeeded	attack.defense_evasion	On
Unsniff Malware C2 URL Pattern	50	Medium	Sep 1, 2020 @ 10:35:47.094	succeeded	attack.defense_evasion	On
CMSTP Execution	50	Medium	Sep 1, 2020 @ 10:40:43.326	succeeded	attack.defense_evasion	On
Unsniff Malware Download URL Pattern	50	Medium	Sep 1, 2020 @ 10:35:47.090	succeeded	attack.defense_evasion	On
CMSTP Execution	50	Medium	Sep 1, 2020 @ 10:40:43.343	succeeded	attack.defense_evasion	On
CMSTP Execution	50	Medium	Sep 1, 2020 @ 10:40:43.312	succeeded	attack.defense_evasion	On
CMSTP Execution	50	Medium	Sep 1, 2020 @ 10:40:43.333	succeeded	attack.defense_evasion	On
CMSTP Execution	50	Medium	Sep 1, 2020 @ 10:40:43.329	succeeded	attack.defense_evasion	On
Minikatz through Windows Remote Management	50	Medium	Sep 1, 2020 @ 10:35:44.118	succeeded	attack.credential_access	On
Password Dumper Remote Thread in LSASS	50	Medium	Sep 1, 2020 @ 10:40:43.328	succeeded	attack.credential_access, attack.l1003	On
TropicTrooper Campaign November 2018	50	Medium	Sep 1, 2020 @ 10:35:44.119	succeeded	attack.execution, attack.l1005	On
CMSTP UAC Bypass via COM Object Access	50	Medium	Sep 1, 2020 @ 10:35:44.154	succeeded	attack.defense_evasion	On
Addition of SID History to Active Directory Object	50	Medium	Sep 1, 2020 @ 10:35:44.120	succeeded	attack.persistence	On
Password Change on Directory Service Restore Mode (DSRM) Account	50	Medium	Sep 1, 2020 @ 10:35:44.113	succeeded	attack.persistence	On

rule-sets

Introduction

- Sigma <https://github.com/SigmaHQ/sigma>
 - Sigma is an **open source** standardized format for describing SIEM rules
 - Solve the interoperability problem between different SIEM platforms such as Splunk, ELK, ArcSight, QRadar
 - Assumes that public Sigma rules are being used by a victims

Windows Event Log :

```
Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Event ID: 4688
Task Category: Process Creation
Level: Information
Keywords: Audit Success
Description:
A new process has been created.
Subject:
  Security ID:      S-1-5-21-3623811015-3361044348-30300820-1013
  Account Name:     johndoe
  Account Domain:   CONTOSO
  Logon ID:         0x3e7
New Process:
  New Process ID:   0x1f4
  New Process Name: C:\Windows\System32\cmd.exe
  Token Elevation Type: %1936
  Creator Process ID: 0x1c4
  Process Command Line: C:\Windows\System32\cmd.exe /c whoami
Network Information:
  Workstation Name: WIN-PC
  Source Network Address: 192.168.1.101
  Source Port:      12345
```



Sigma Rule for whoami :

```
title: Suspicious Process Creation - whoami Command
id: a1b2c3d4-5678-90ab-cdef-1234567890ab
description: Detects the creation of a cmd.exe process with the whoami command
author: Example Author
date: 2023/05/21
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4688
    NewProcessName: C:\Windows\System32\cmd.exe
  condition: selection and cmdline
  cmdline:
    CommandLine|re: '.*whoami.*'
fields:
  - EventID
  - NewProcessName
  - ProcessCommandLine
falsepositives:
  - Administrative scripts
level: high
```



ALERT !

Analysis of SIEM Rules for Evasions

1. Analyzed all process creation rules that were contained in the Sigma repository
2. Re-enact the malicious process creation as described by the rules
3. If we succeeded to match the rule, then tried to find command lines that **perform the exact same action**, but without matching the rule

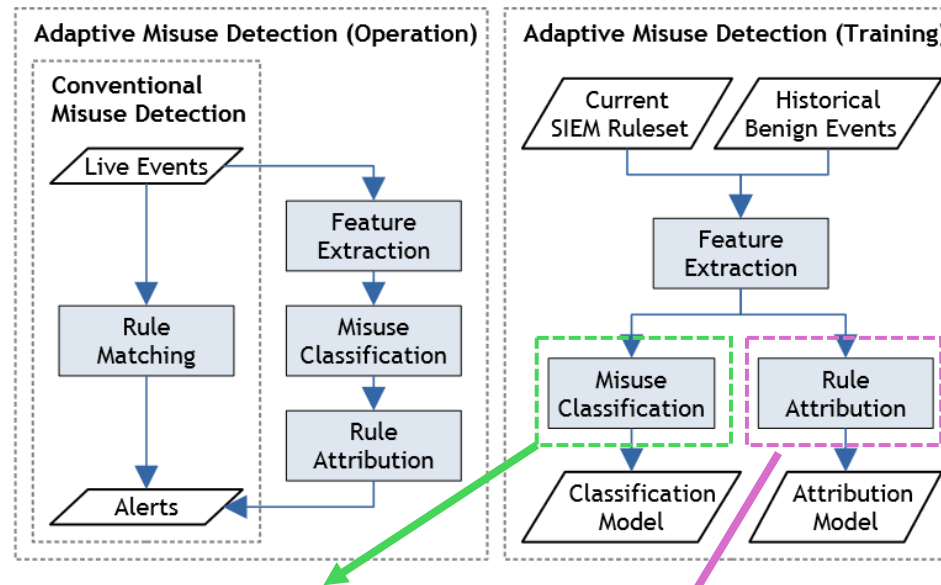
292 Sigma rules, 110 (38 %) can be fully evaded, 19 (7 %) can be partially evaded

Summarized five evasion types:

Evasion type	Sample affected rule	Affected search term	Sample match	Sample evasion
Insertion	win_susp_schtask_creation	* /create *	schtasks.exe /create ...	schtasks.exe /"create" ...
Substitution	win_susp_curl_download	_-O_	curl -O http://...	curl --remote-name http://...
Omission	win_mal_adwind	*cscript.exe *Retrive*.vbs *	cscript.exe ...\\Retrive.vbs	cscript ...\\Retrive.vbs
Reordering	win_susp_procdump	* -ma ls*	procdump -ma ls	procdump ls -ma
Recoding	win_vul_java_remote_dbg	*address=127.0.0.1*	...address=127.0.0.1,...	...address=2130706433,...

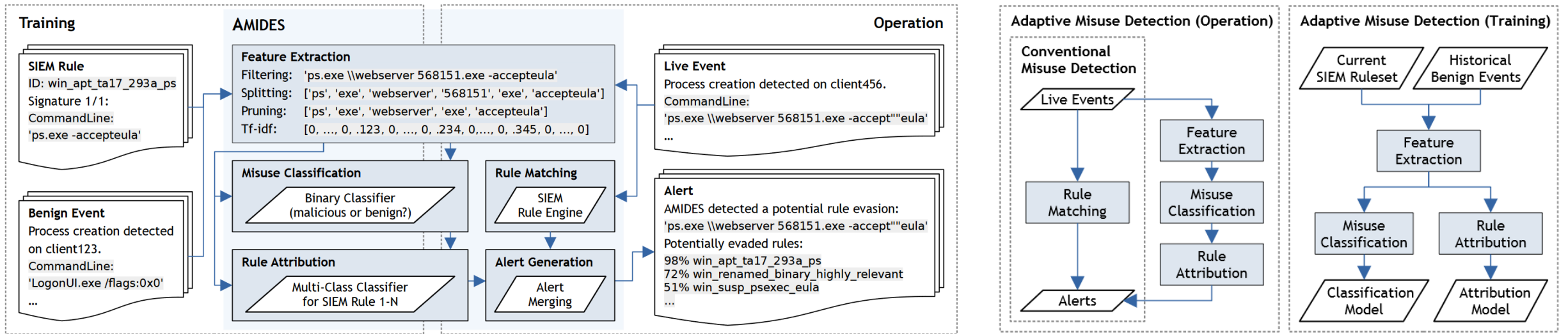
Overview

- A methodology to reduce blind spots by **detecting rule evasions** in addition to **conventional rule matches**



- Assume that SIEM events of successful evasions are still very similar to those of the original attack.
- When a command line is executed that is very “similar” to a signature of some rule, the respective rule should be proposed to the analyst within the alert

Approach



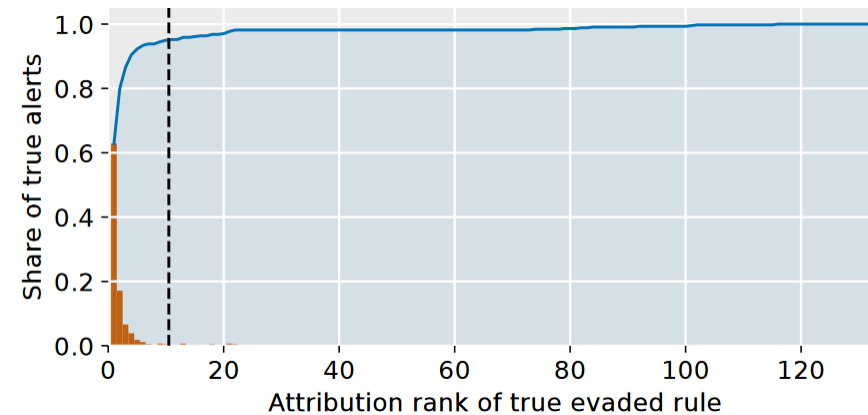
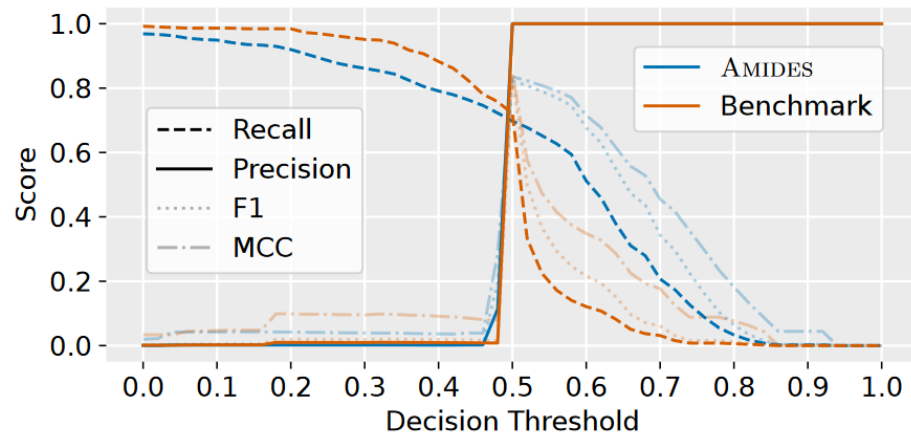
- Feature Extraction: Filtering + Splitting + Pruning + Tf-idf
- Misuse Classification: SVM
- Rule Attribution: train a SVM for every rule
- Performance Considerations: Implement an in-memory cache to avoid repeated classification of already-seen feature vectors

Evaluation

- RQ1: How well does AMIDES detect SIEM rule evasions?
- RQ2: How accurate is the rule attribution?
- RQ3: Is AMIDES suited for real-world operation?
- Dataset: collect SIEM events from a large enterprise network with more than 50000 users.

Evaluation

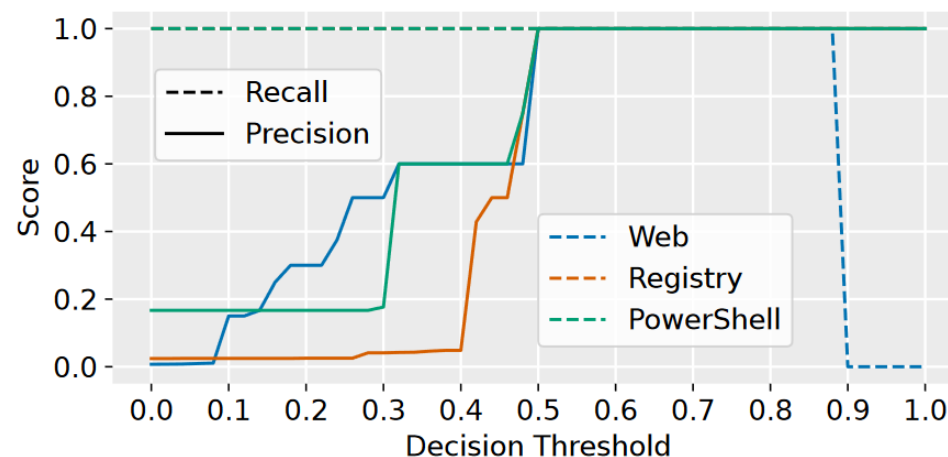
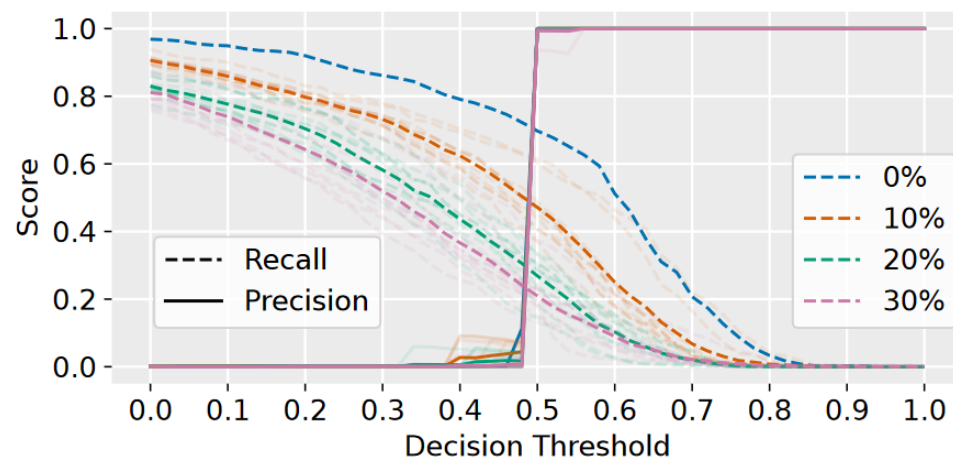
- RQ1: How well does AMIDES detect SIEM rule evasions?
 - Benchmark: learn from attack events and benign events



- RQ2: How accurate is the rule attribution?
 - A vast majority of the true rules (95 %) are contained within the top 10

Evaluation

- RQ3: Is AMIDES suited for real-world operation?
 - A commodity Linux server with 40 physical CPU cores (80 virtual), 384 GiB RAM, and a single SSD drive
 - AMIDES required 0.0763 ms per event on average ($\sigma = 3.19$ ms) on a single core
 - Consider the case that supposedly benign training data inadvertently contain evasions
 - Consider the case that supposedly benign training data inadvertently contain evasions



Limitations and Discussion

- Cannot detect fundamentally different classes of evasion attacks such as (undetected) code injection into benign processes
- Attackers could try to evade AMIDES itself
- Focus on Windows process creation events, particularly their command line field

Conclusion

- Analyzed 292 Windows process creation rules from the Sigma repository, finding 110 fully evadable and 19 partially evadable.
- Evaluated the open-source implementation AMIDES in a large enterprise network, detecting 70% of evasions with zero false alerts at default sensitivity.
- AMIDES processes approximately 156,000 events per second and requires 42 minutes of training, making it suitable for large enterprise networks.
- For 95% of evasions, AMIDES included the actually evaded rule within its top 10 propositions.