

Synthesizing Intrusion Detection System Test Data

Jared Chandler

jared.chandler@tufts.edu

Tufts University

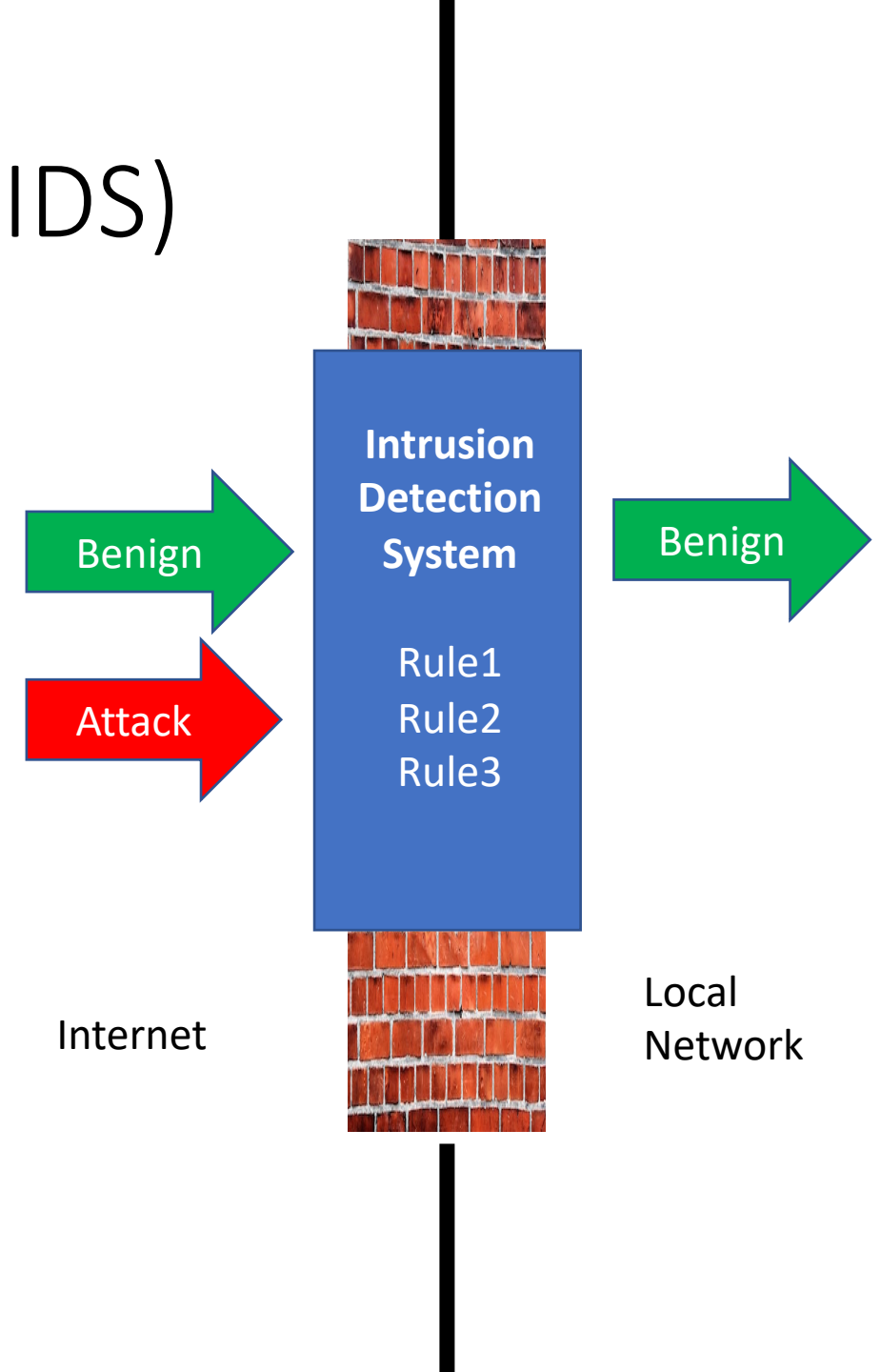
Adam Wick

awick@fastly.com

Fastly

Intrusion Detection Systems (IDS)

- Recognize traffic using Rules.
- Rules describe Malicious Packets
- Shared Rules allow us to recognize threats we've never encountered.
- We don't share the malicious traffic to trigger those rules because it contains sensitive data.
- Without test data it's hard to know if your IDS is working correctly.



Example Suricata Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"ET TROJAN Possible Metasploit Payload Common
Construct Bind_API (from server)";
flow:from_server,established; content:"|60 89 e5
31|"; content:"|64 8b|"; distance:1; within:2;
content:"|30 8b|"; distance:1; within:2;
content:"|0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff|";
distance:1; within:13; content:"|ac 3c 61 7c 02 2c
20 c1 cf 0d 01 c7 e2|"; within:15; content:"|52 57
8b 52 10|"; distance:1; within:5; metadata:
former_category TROJAN; classtype:trojan-activity;
sid:2025644; rev:1; metadata:affected_product Any,
attack_target Client_and_Server, deployment
Perimeter, deployment Internet, deployment Internal,
deployment Datacenter, tag Metasploit,
signature_severity Critical, created_at 2016_05_16,
updated_at 2018_07_09;)
```

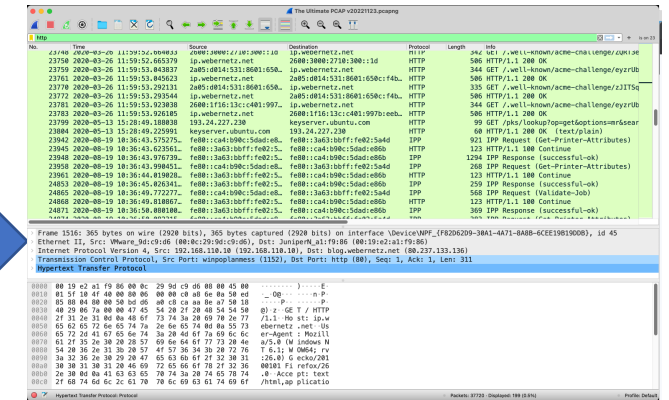
**Domain
Specific
Language**

Direction
Ports
Byte Values
Reg-Ex
Positions
Ordering

Research Goal

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21
(msg:"ET SCAN PRO Search Crawler Probe";
flow:to_server,established; content:"PASS ";
nocase; depth:5; content:"crawler"; nocase;
within:30; pcre:"/^PASS\s+PRO(-
|\s)*search\s+Crawler/smi";
reference:url,sourceforge.net/project/showfile
s.php?group_id=149797;
reference:url,doc.emergingthreats.net/2008179;
classtype:not-suspicious; sid:2008179; rev:3;
metadata:created_at 2010_07_30, updated_at
2010_07_30;)
```

IDS Rules



Packets for Testing

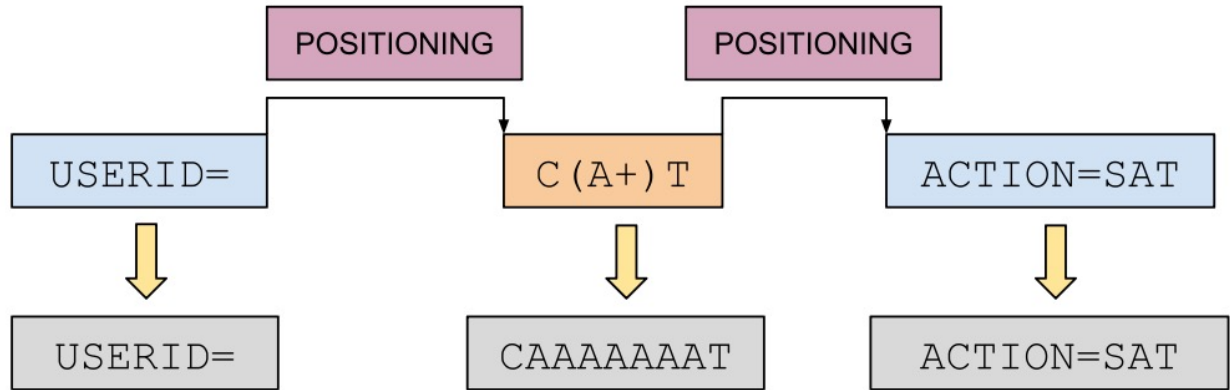
Prior Work

- *Deceptive Self-Attack for Cyber Defense, HICSS 2023*
- Originally Developed to Blind an IDS / Distract an Adversary
- Bombard a network with spurious attacks

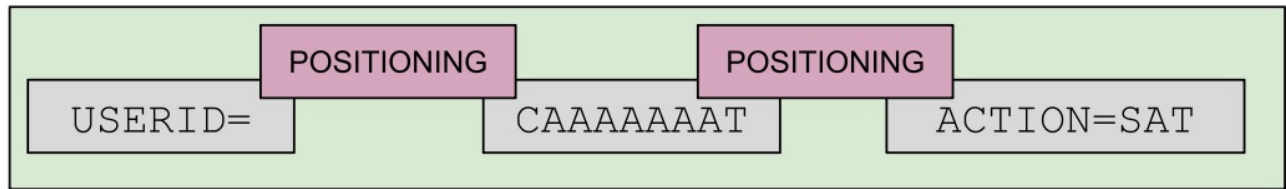
1 Signature is parsed.

```
content:"USERID="; offset:0; pcre:"C(A+)T"; distance:2;  
content:"ACTION=SAT"; distance:6; within:20;
```

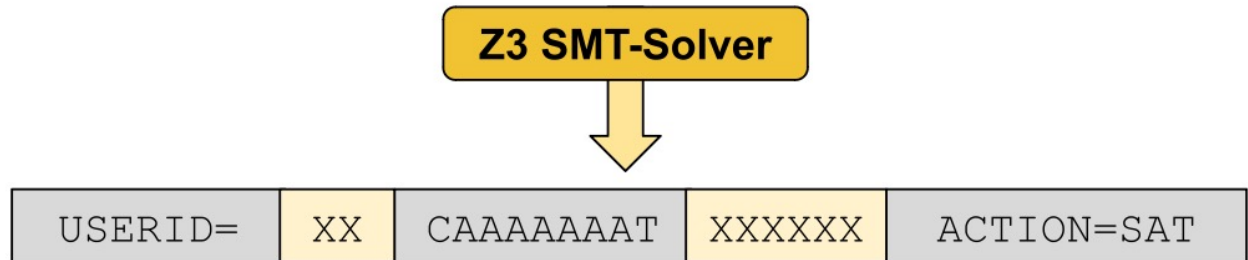
2 Content generated for regular expressions.



3 Generated content and positioning constraints encoded as SMT problem.

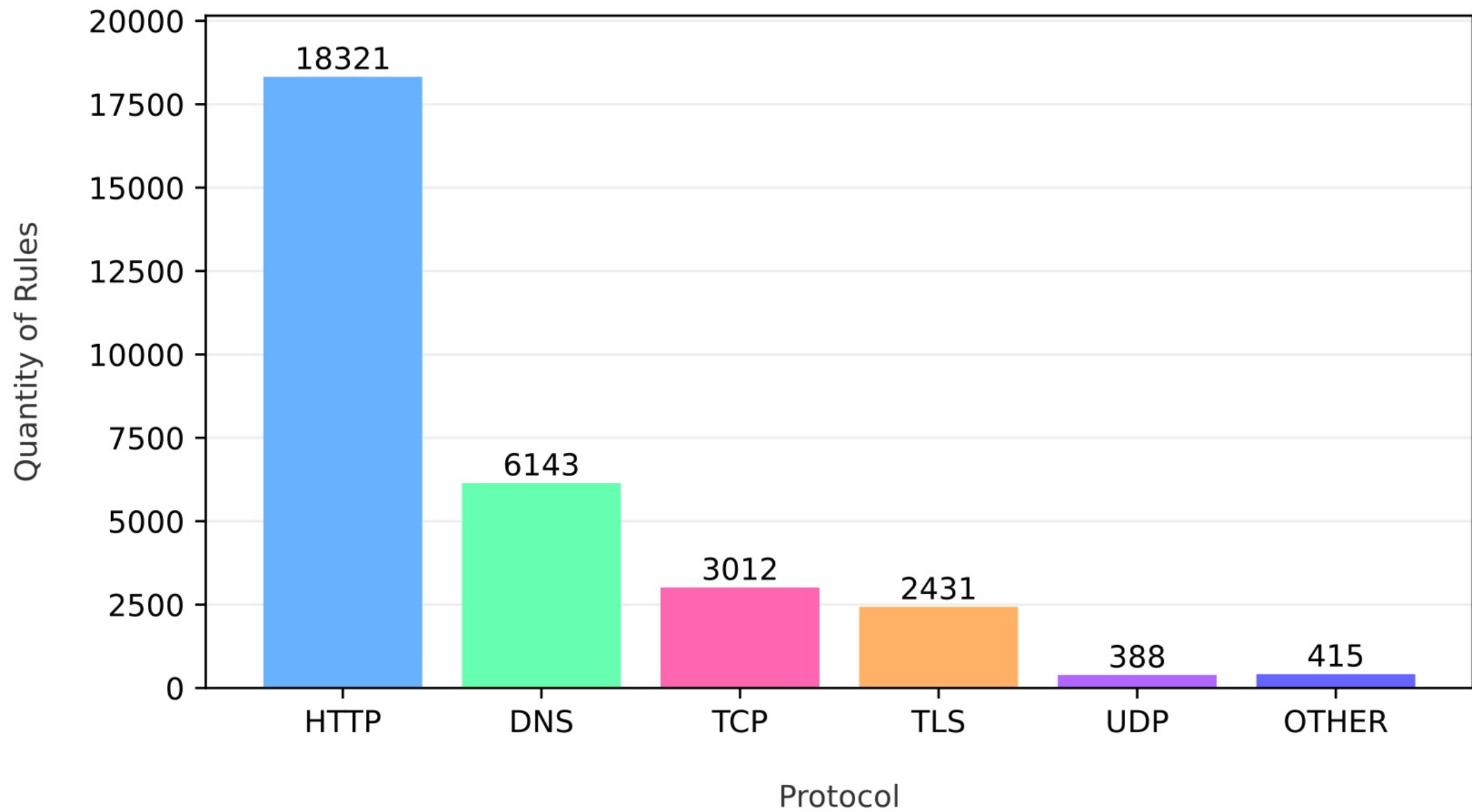


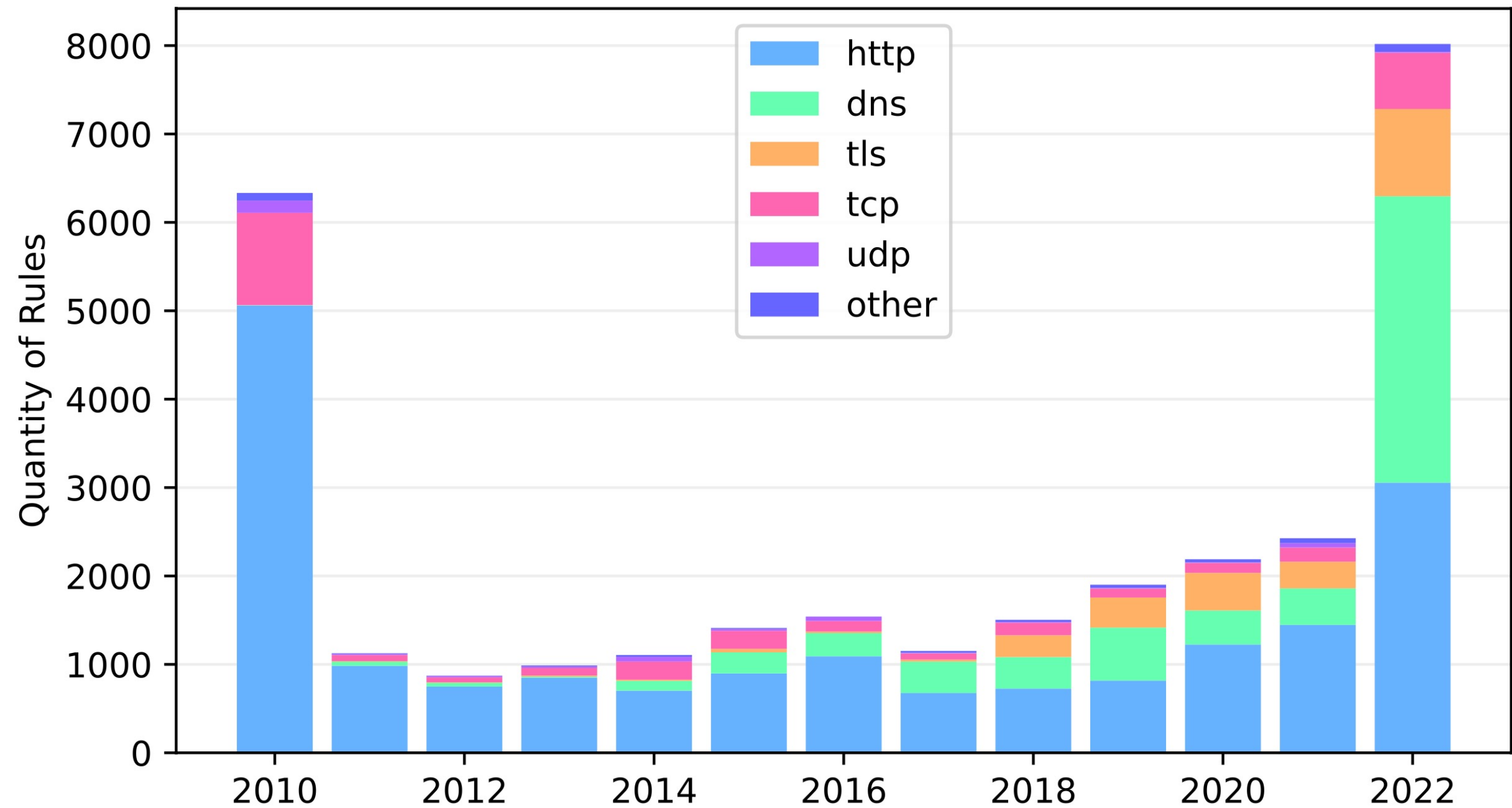
4 Generated content positioned according to SMT solution.



Survey of Rules In Practice

- Proof Point Emerging Threats Dataset
- Open Source Corpus of over 30,000 rules
- Contributions spanning more than a decade





Protocol	Named Buffer	Qty of Uses
HTTP	<code>http.uri</code>	10426
	<code>http.method</code>	6449
	<code>http.request_body</code>	2916
	<code>http.host</code>	2668
	<code>http.header_names</code>	2550
	<code>http.user_agent</code>	2354
	<code>http.header</code>	1251
	<code>http.stat_code</code>	813
	<code>http.content_type</code>	605
	<code>http.request_line</code>	326
	<code>http.cookie</code>	271
	<code>http.accept</code>	126

Expanded Approach

- Handle named buffers

```
alert http any any -> [$HOME_NET,$HTTP_SERVERS]
any (msg:"ET EXPLOIT eMerge E3 Command
Injection Inbound (CVE-2019-7256)";
flow:established,to_server;
http.method; content:"GET";
http.uri; content:"/card_scan"; startswith;
fast_pattern; content:".php"; distance:0;
within:15; content:"=|60|"; reference:cve,2019-
7256; classtype:attempted-admin; sid:2033757;
rev:1; metadata:created_at 2021_08_22, cve
CVE_2019_7256, former_category EXPLOIT,
updated_at 2021_08_22;)
```

1

Example Signature
Fragment

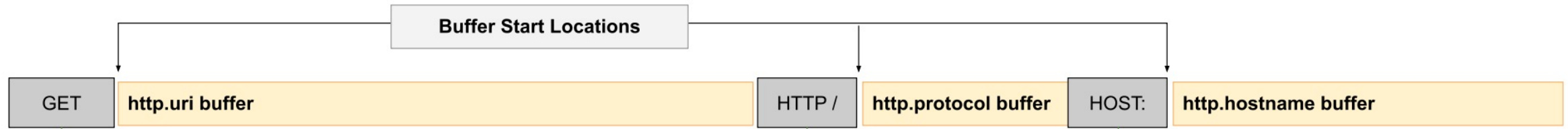
```
http.method;content:"get";  
http.uri; content:"json" ; distance:4; within:10;  
http.protocol; content:"3.0";  
http.hostname; content "abc.com"
```

1

Example Signature
Fragment

```
http.method;content:"get";  
http.uri; content:"json" ; distance:4; within:10;  
http.protocol; content:"3.0";  
http.hostname; content "abc.com"
```

2



Synthesize Each Named Buffer Individually

1

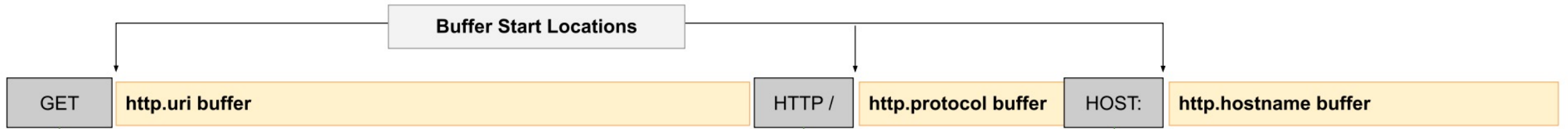
Example Signature Fragment

```

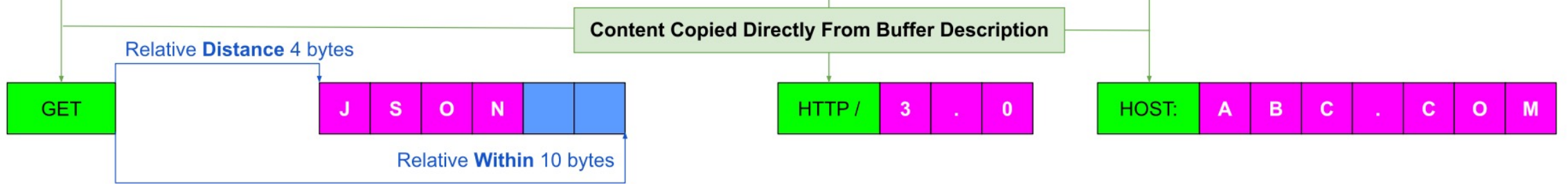
http.method;content:"get";
http.uri; content:"json" ; distance:4; within:10;
http.protocol; content:"3.0";
http.hostname; content "abc.com"

```

2



3



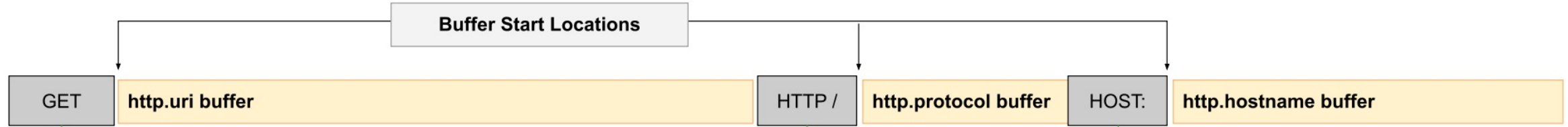
Insert Into Template

1

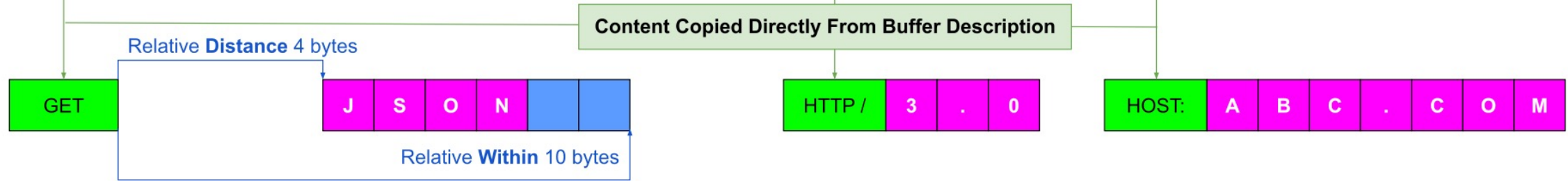
Example Signature Fragment

```
http.method;content:"get";
http.uri; content:"json" ; distance:4; within:10;
http.protocol; content:"3.0";
http.hostname; content "abc.com"
```

2



3



4

```
GET /XY.JSON HTTP/3.0 HOST: ABC.COM
GET /AB.JSON HTTP/13.0 HOST: FOOABC.COM
GET /WXYJSONABC HTTP/ABC123.0 HOST: ABC.COM
GET /ABCD/JSON HTTP/13.0.XYZ HOST: FOOABC.COM
```

Evaluation Setup

```
Rule X
311: content:"144 Bb"; distance:1; within:2;
content:"130 Bb"; distance:2; within:2;
content:"100 Bb 52 14 Bb 72 28 0f b7 4a 26 31 fef";
distance:1; within:13; content:"a0 50 63 70 02 20
20 03 0f 0d 05 07 a2"; within:15; content:"152 57
Bb 52 10"; distance:1; within:5; metadata:
former_category:TROJAN; classtype:trojan-activity;
sid:2025444; rev:1; metadata:affected_product:Any,
attack_target:Client_and_Server; deployment:
Perimeter; deployment:Internet; deployment:Internal;
deployment:Datacenter; tag:Metasploit;
signature_severity:Critical; created_at:2014_05_16;
updated_at:2018_07_29;
```

Figure 1. Example Suricata Signature.

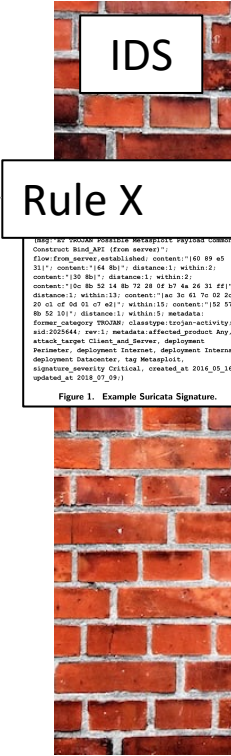
```
Rule X
311: content:"144 Bb"; distance:1; within:2;
content:"130 Bb"; distance:1; within:2;
content:"100 Bb 52 14 Bb 72 28 0f b7 4a 26 31 fef";
distance:1; within:13; content:"a0 50 63 70 02 20
20 03 0f 0d 05 07 a2"; within:15; content:"152 57
Bb 52 10"; distance:1; within:5; metadata:
former_category:TROJAN; classtype:trojan-activity;
sid:2025444; rev:1; metadata:affected_product:Any,
attack_target:Client_and_Server; deployment:
Perimeter; deployment:Internet; deployment:Internal;
deployment:Datacenter; tag:Metasploit;
signature_severity:Critical; created_at:2014_05_16;
updated_at:2018_07_29;
```

Figure 1. Example Suricata Signature.

Packet Synthesis

PACKET GENERATED

FAILS TO GENERATE



```
Rule X
311: content:"144 Bb"; distance:1; within:2;
content:"130 Bb"; distance:1; within:2;
content:"100 Bb 52 14 Bb 72 28 0f b7 4a 26 31 fef";
distance:1; within:13; content:"a0 50 63 70 02 20
20 03 0f 0d 05 07 a2"; within:15; content:"152 57
Bb 52 10"; distance:1; within:5; metadata:
former_category:TROJAN; classtype:trojan-activity;
sid:2025444; rev:1; metadata:affected_product:Any,
attack_target:Client_and_Server; deployment:
Perimeter; deployment:Internet; deployment:Internal;
deployment:Datacenter; tag:Metasploit;
signature_severity:Critical; created_at:2014_05_16;
updated_at:2018_07_29;
```

Figure 1. Example Suricata Signature.

NO ALARM

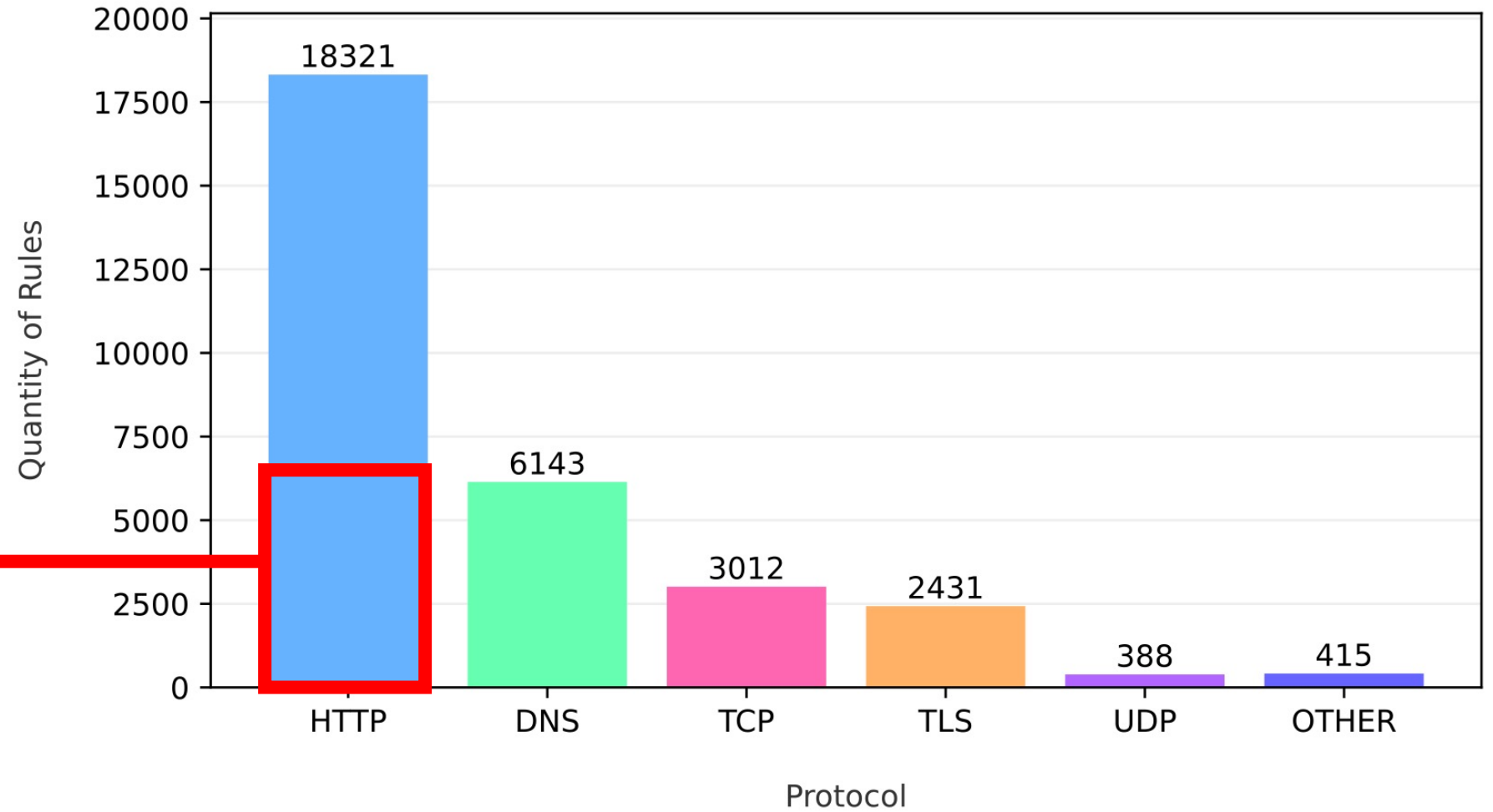
ALARM



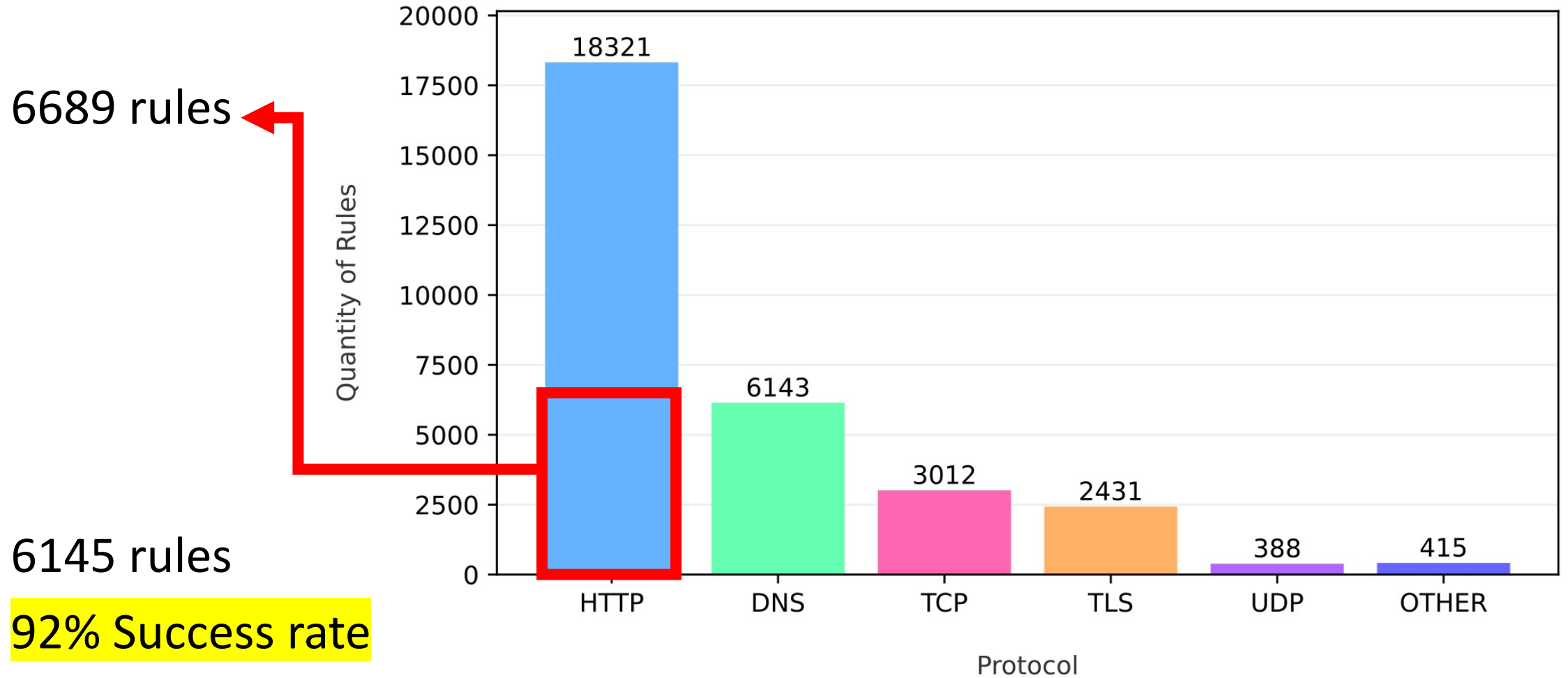
Goal

Evaluation

6689 rules



Evaluation



Interesting Failures

```
http.uri; content:"Flash Player.exe";
```

Interesting Failures

```
http.uri; content:"Flash Player.exe";
```

← → ↻ redmine.openinfosecfoundation.org/issues/2881

▼ **Suricata**

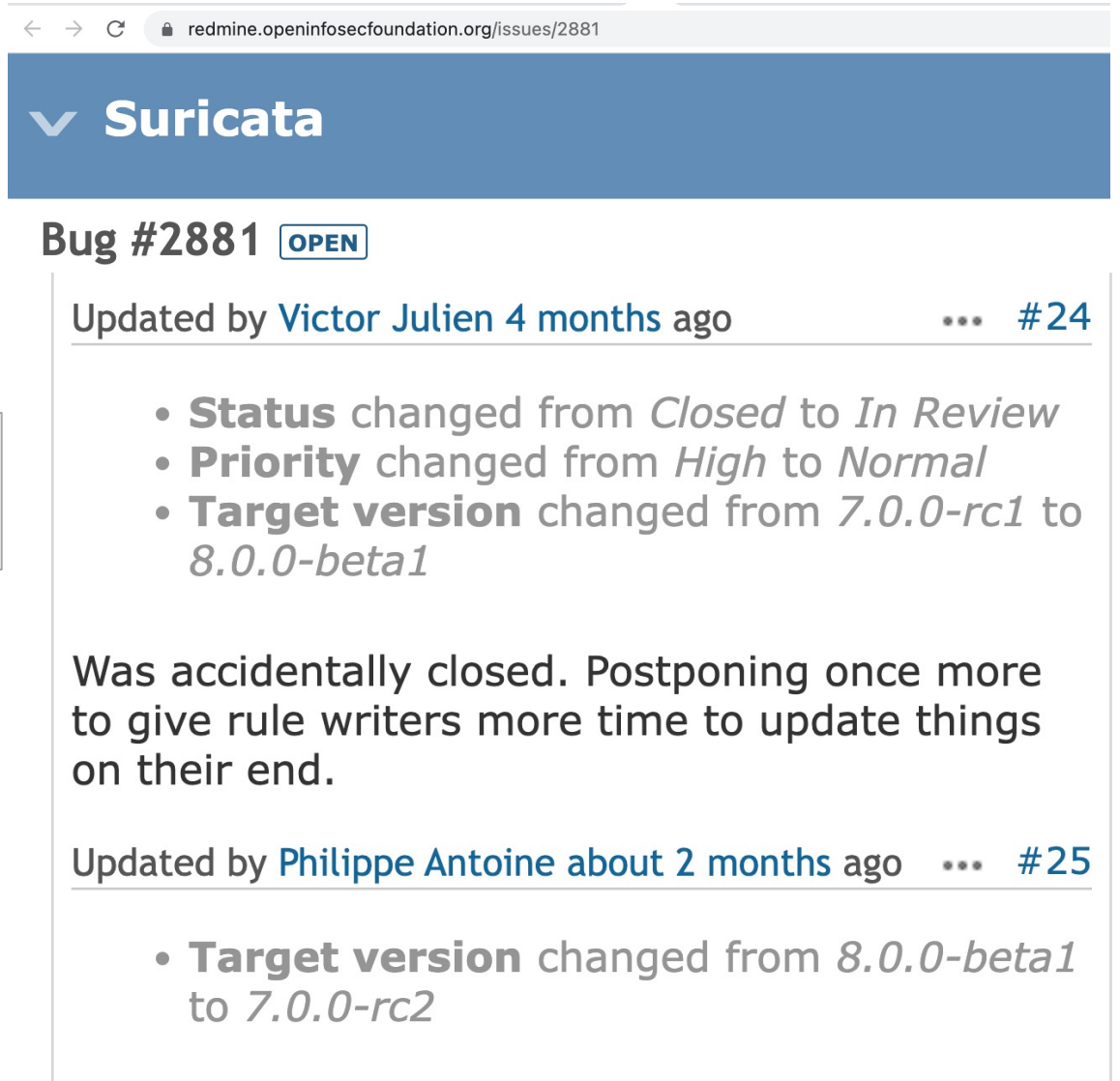
Bug #2881 OPEN

http.protocol parsing inaccuracy
Added by [chris lujan](#) about 4 years ago. Updated 5 days ago.

Status:	In Review
Priority:	Normal
Assignee:	Philippe Antoine
Target version:	8.0.0-beta1
Affected Versions:	
Effort:	
Difficulty:	low
Label:	

Interesting Failures

```
http.uri; content:"Flash Player.exe";
```



The screenshot shows a web browser window with the URL `redmine.openinfosecfoundation.org/issues/2881`. The page title is "Suricata". The issue is labeled "Bug #2881" with an "OPEN" status. The issue history shows two updates:

- Updated by [Victor Julien](#) 4 months ago ... #24
 - **Status** changed from *Closed* to *In Review*
 - **Priority** changed from *High* to *Normal*
 - **Target version** changed from *7.0.0-rc1* to *8.0.0-beta1*

Was accidentally closed. Postponing once more to give rule writers more time to update things on their end.
- Updated by [Philippe Antoine](#) about 2 months ago ... #25
 - **Target version** changed from *8.0.0-beta1* to *7.0.0-rc2*

PCRE Introduced Constraints

```
http.uri; content:"index.html"; offset:0;
```

```
http.uri; pcre:"^index.html";
```

Overlap for Performance

```
content: "foo"; offset: 0;  
pcre: "fooba+r"; offset: 0;
```

Rule Debugging

```
content:"a";content:"b";
```

```
content:"a";depth:1,content:"b";depth:1;
```

```
content:"a";depth:1,content:"cb";depth:2;
```


Next Steps

- Expand to handle more named buffers.
- More complex relationships: Move byte-string synthesis within Z3.
- Help rule authors debug rules.
- Synthesize examples which are usefully dissimilar.

Thank You! Questions?

Jared Chandler

jared.chandler@tufts.edu