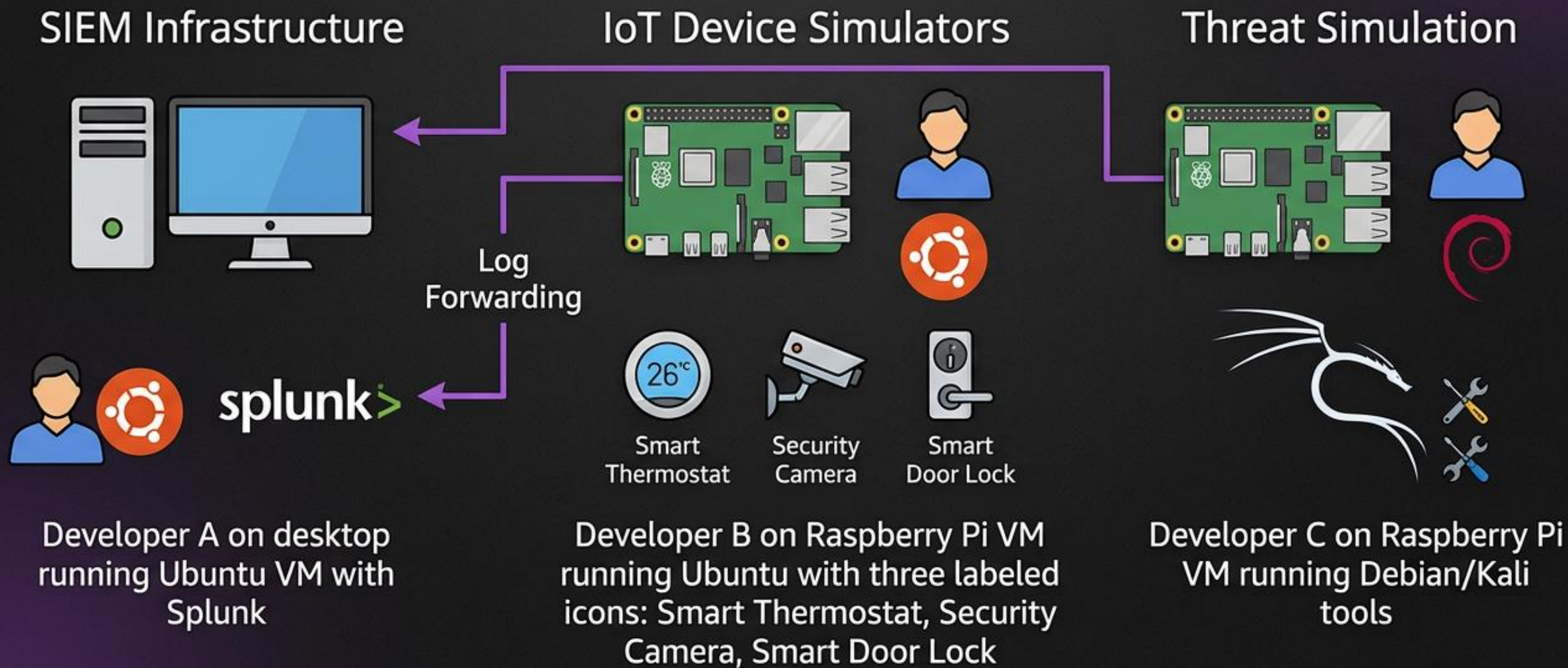
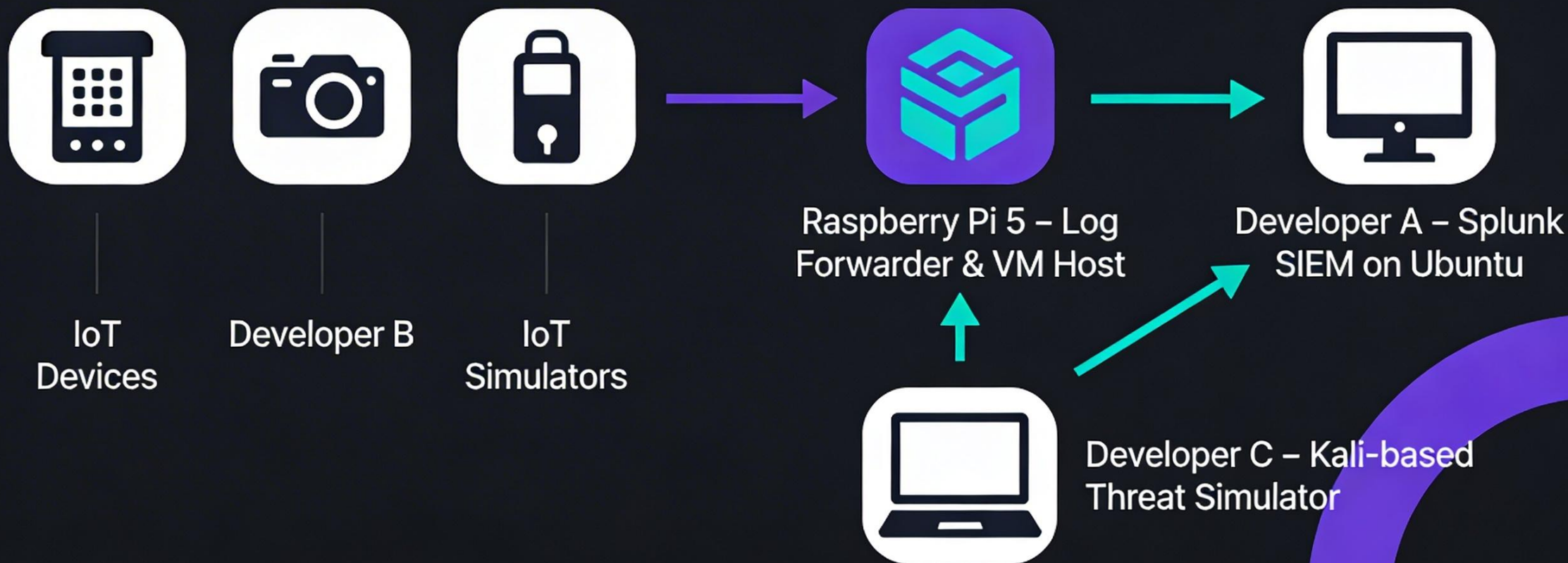


IoT Shield Capstone Overview



IoT Shield – Raspberry Pi Powered IoT SIEM Lab

Lightweight IoT threat simulation with desktop-hosted Splunk Enterprise



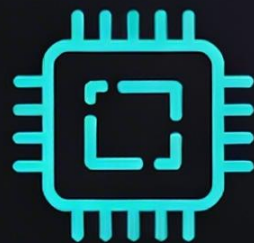
IoT Shield – System Architecture & Team Roles

Developer A – SIEM Engineer



- Ubuntu Desktop VM
- Splunk Enterprise 10.0.1
- Indexes: `iot_devices`, `security_events`, `threat_analysis`
- 12 custom alerts, 3 dashboards

Developer B – IoT Device Engineer



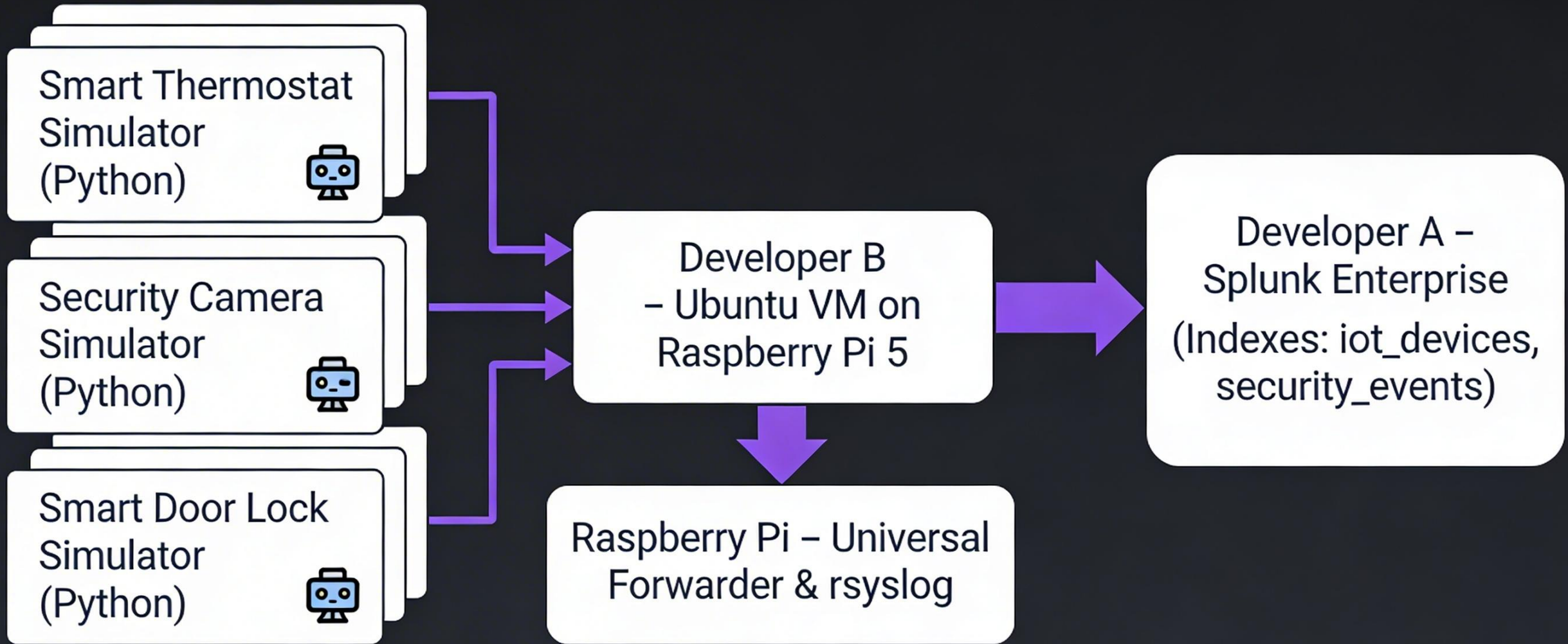
- Ubuntu VM on Raspberry Pi
- Python IoT simulators: `thermostat`, `camera`, `door lock`
- Sends logs via Pi forwarder

Developer C – Threat Engineer



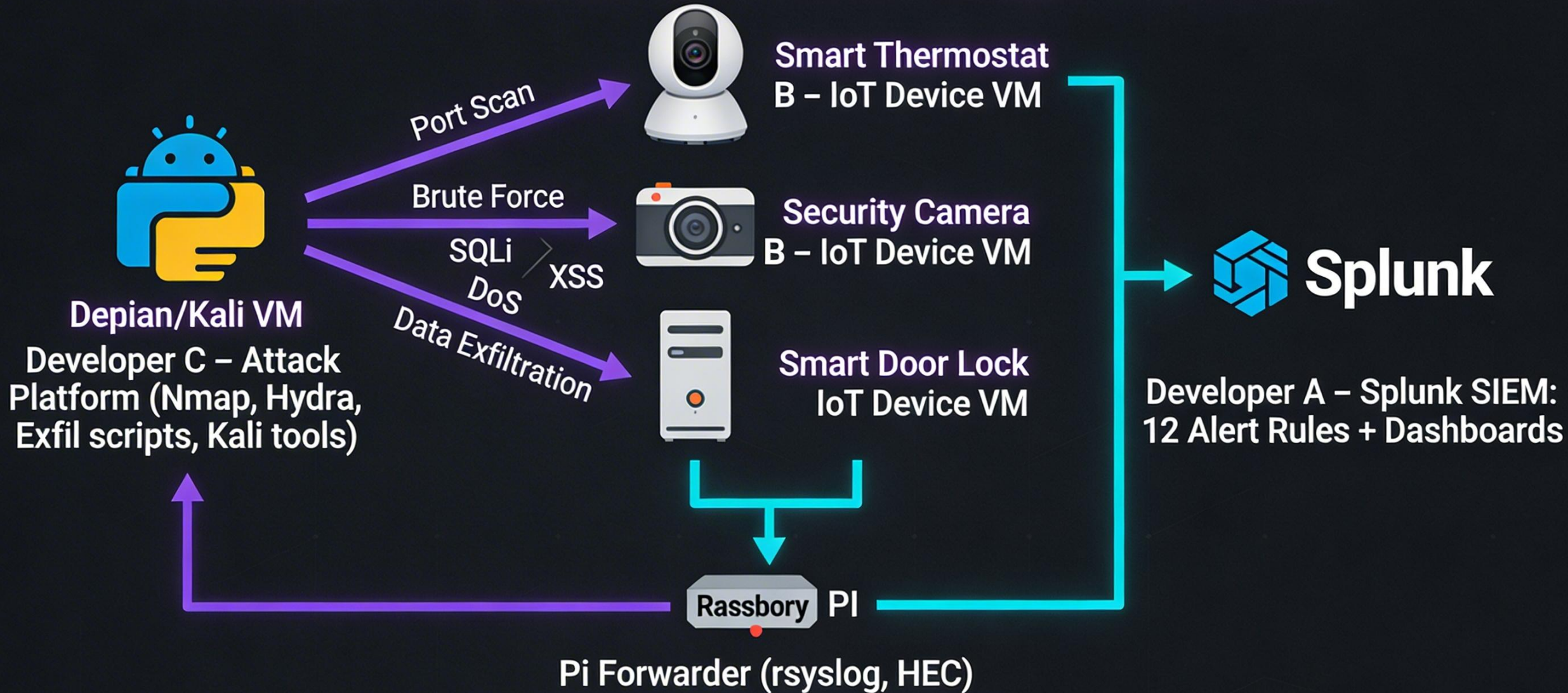
- Debian VM with Kali tools
- Nmap, Hydra, exfil scripts
- Executes 12 mapped attacks against IoT devices

IoT Device Simulation & Log Flow



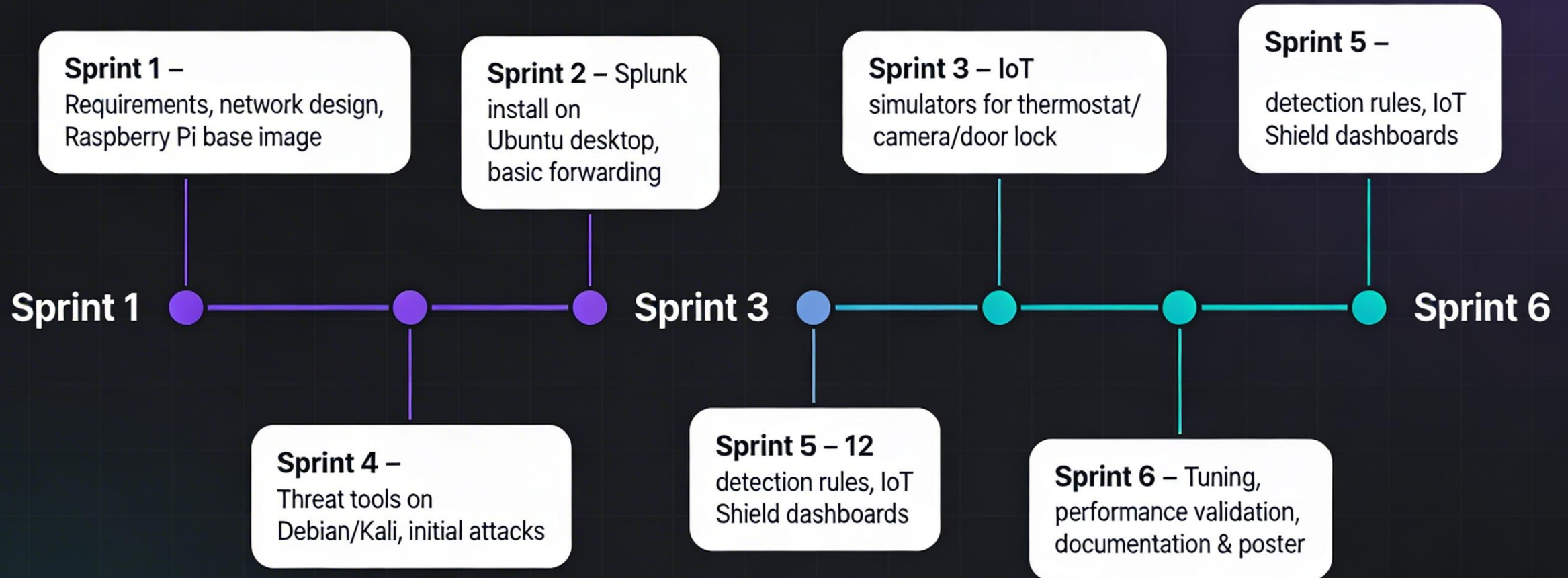
Goal: Prove a low-cost Pi can generate realistic IoT telemetry and forward it reliably to a desktop SIEM.

Threat Simulation & Alerting Workflow



Each simulated attack must trigger at least one security alert in IoT Shield.

IoT Shield – 6 Sprint Development Timeline



IoT Shield – Security Outcomes

3

Dashboards

Main Operations,
Security Alerts,
Threat Analysis

12

Alert Rules

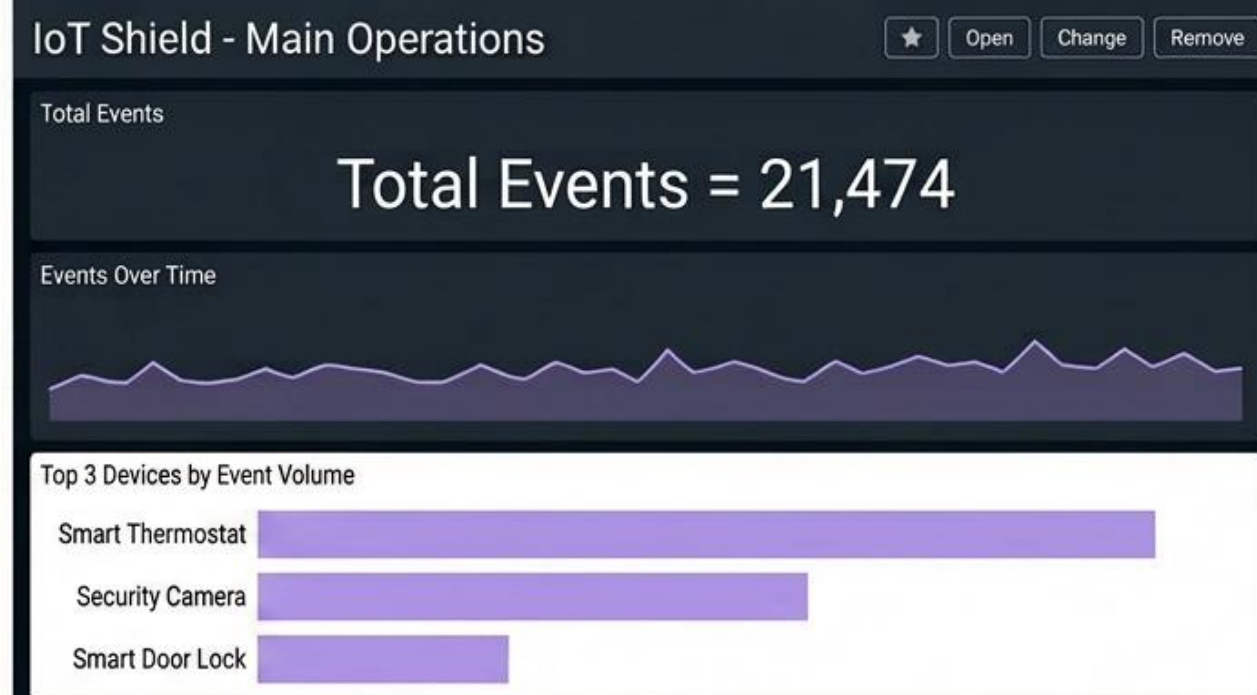
Brute Force, Port Scan,
Data Exfiltration,
SQLi, XSS, etc.

900+

Alerts Observed

Across Jan 1 – Apr 13,
2026 in test lab

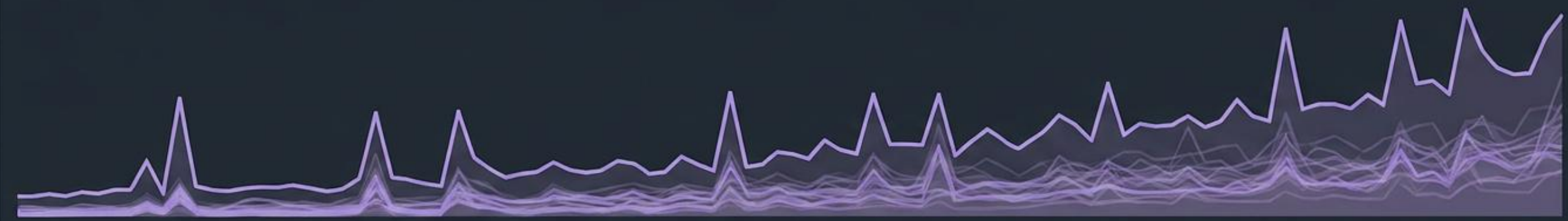
- Validated Raspberry Pi as reliable log-forwarding hub
- Demonstrated full attack chain from IoT devices to SIEM alerts
- Showed need for desktop-class hardware for heavy SIEM analytics



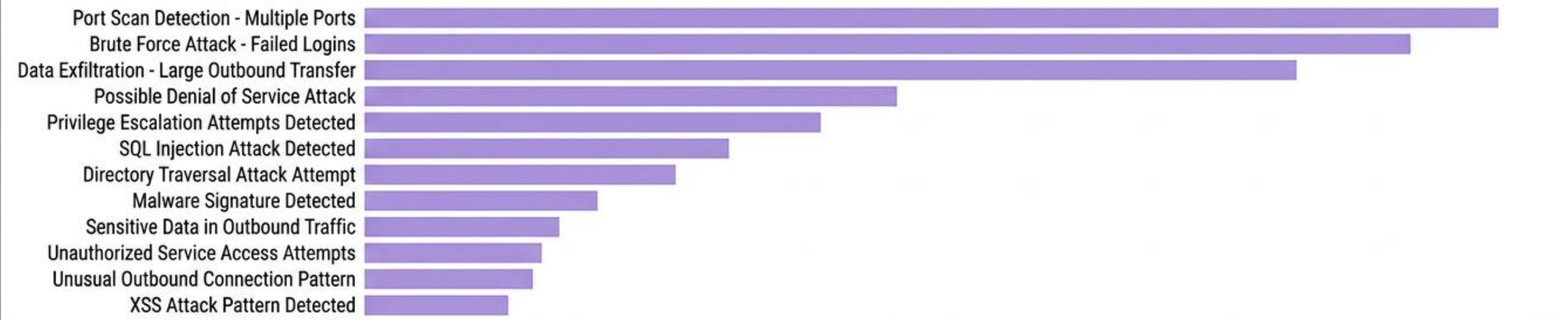
Total Security Alerts

900

Alerts Over Time



Top Alert Types by Volume



Active Attack Campaigns

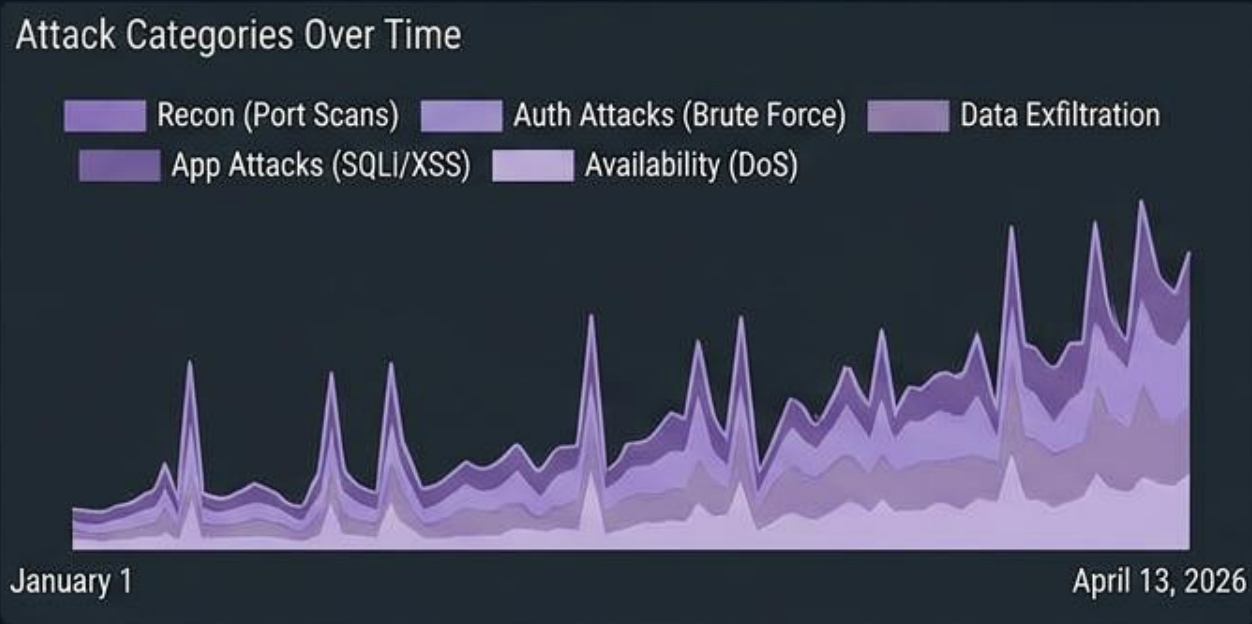
12

Distinct campaigns run in lab (Jan–Apr 2026)

Impacted IoT Devices

3/3

Thermostat, Camera, Door Lock affected



Top Offending Sources

src_ip	campaign_tag	alerts	first_seen	last_seen
203.0.113.10	Recon-01	150	Jan-01, 2026	Aan-13, 2026
198.51.100.23	Bruteforce-02	90	Jan-01, 2026	Aan-13, 2026
192.0.2.88	Exfil-03	30	Jan-01, 2026	Jan-13, 2026
172.16.254.1	Auth-04	20	Jan-01, 2026	Jan-13, 2026
10.0.0.10	App-05	150	Jan-01, 2026	April 13, 2026
192.0.2.100	DoS-06	20	Jan-01, 2026	April 13, 2026
203.0.113.50	Bruteforce-07	20	Jan-01, 2026	April 13, 2026
198.51.100.100	Exfil-08	20	Jan-01, 2026	April 13, 2026



Searches, Reports, and Alerts

12 Searches, Reports, and Alerts

Types All

App: search

Owner: Administrator (siem)

Name

Brute Force Attack - Failed Logins

Detects 5+ failed login attempts from same IP

Data Exfiltration - Large Outbound Transfer

Detects outbound transfers >50MB

Directory Traversal Attack Attempt

Path traversal patterns detected

Malware Signature Detected

Known malware patterns found in logs

Port Scan Detection - Multiple Ports

Detects when a source scans more than 15 ports in 5 minutes

Possible Denial of Service Attack

Abnormally high request rate from single source

Privilege Escalation Attempts Detected

Multiple failed sudo/su commands from same user

SQL Injection Attack Detected

Sensitive keywords detected in network traffic

Sensitive Data in Outbound Traffic

Sensitive keywords detected in network traffic

Unauthorized Service Access Attempts

Multiple blocked connection attempts to same port

Unusual Outbound Connection Pattern

Connections to non-standard ports detected

XSS Attack Pattern Detected

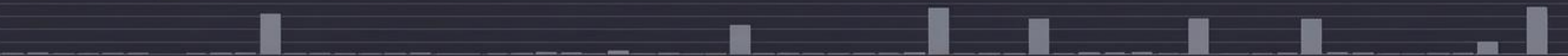
JavaScript injection attempts found

index=security_events sourcetype=auth_logs action=failure | stats count BY src_ip, user | where count>=5

All time

Q

Events timeline (All time)



_time ↕	src_ip ↕	user ↕	count ↕
2026-01-05 08:12:30.123	192.168.1.1	admin	35
2026-01-20 14:22:45.001	10.0.x.10	iot-admin	25
2026-02-10 09:55:00.888	192.168.2.22	devops	22
2026-02-11 11:30:15.555	10.0.x.10	iot-admin	20
2026-03-01 16:40:20.222	192.168.2.1	devops	18
2026-03-15 07:15:55.777	192.168.2.1	admin	16
2026-04-01 12:01:01.111	192.168.10.20	pi-user	14
2026-04-05 22:59:30.999	10.0.x.1	iot-admin	12
2026-04-10 10:00:10.010	192.168.2.14	pi-user	9
2026-04-13 18:00:00.000	192.168.2.14	pi-user	7

index=iot_devices sourcetype=netflow direction=outbound | eval mb=bytes/1824/1024 | where mb>50 | stats sum(mb) AS total_MB BY src_ip, dest_ip

All time ▾ 🔍

Alex ▾ In s M These tooes ▾



_time ↕	src_ip ↕	dest_ip ↕	total_MB ↕
2026-01-15 10:23:45	192.168.1.10	8.8.8.8	450
2026-02-02 09:12:00	192.168.1.10	8.8.8.8	450
2026-02-28 21:55:10	192.168.1.10	52.23.14.100	230
2026-03-05 08:30:30	10.0.5.21	52.23.14.100	250
2026-03-14 14:01:22	10.0.5.21	52.23.14.100	240
2026-03-29 23:40:00	192.168.1.10	8.8.8.8	250
2026-04-03 07:11:59	10.0.5.21	52.23.14.100	200
2026-04-10 18:05:01	192.168.1.10	52.23.14.100	60
2026-04-12 08:30:00	10.0.5.21	52.23.14.100	60



IoT Shield – Search & Reporting

"Directory Traversal Attack Attempt"

```
index=security_events sourcetype=web_logs uri_path="../../../" OR uri_query="../../../" | stats count BY src_ip, uri_path
```

All time ▾



✓ Search Save As ▾ Export ▾

All ▾

h

1h

w



Time outstones ▾

Events timeline Standards Hattribute

Security events, frequency, time, and 0 hours

■ Security events



1 Unsorted Alerts :) View results

_time ↕	src_ip ↕	uri_path ↕	count ↕
2026-02-15 10:30:60	203.0.113.5	/app/../../../etc/passwd	20
2026-01-10 09:15:30	198.51.100.12	/../../../../windows/system32/cmd.exe	15
2026-04-01 16:45:10	203.10.113.5	/api/v1/../../../../admin/config	18
2026-03-11 11:20:00	198.51.100.12	/cgi-bin/../../../../etc/passwd	10
2026-02-19 14:30:80	203.0.113.20	/images/../../../boot.ini	7
2026-04-12 14:30:00	203.10.113.5	/static/../../../../etc/shadow	1
2026-03-01 08:00:15	198.51.100.30	../../../../../../../../windows/win.ini	5
2026-04-12 13:30:00	203.10.113.5	/include/../../../../etc/groups	1
2026-01-25 07:12:00	198.51.100.12	/theme/../../../../etc/resolv.conf	1
2026-03-31 23:59:59	203.0.113.5	../../../../../../../../etc/hosts	1

IoT Shield – Search & Reporting

Malware Signature Detected

index=security_events sourcetype=av_logs action=blocked signature=* | stats count BY signature, src_host

All time ▾



Events Timeline

Visualized

All ▾



Search Execute ▾

Show 11 events



About 10 unsorted rows

_time ↕	signature ↕	src_host ↕	count ↕
2026-02-19 11:10:00	Adware.Inject	ubuntu-siem	50
2026-03-29 09:33:05	Ransomware.Sample.A	iot-gateway-01	1
2026-01-14 02:20:45	Adware.Inject	camera-02	30
2026-04-05 18:45:30	Backdoor.Bot	sensor-hub-03	5
2026-02-28 23:59:59	Worm.AutoRun	sensor-hub-03	8
2026-01-08 14:15:22	Trojan.Generic	ubuntu-siem	25
2026-03-18 10:05:55	Ransomware.Sample.A	iot-gateway-01	3
2026-01-22 21:00:11	Worm.AutoRun	camera-02	15
2026-03-05 06:12:34	Trojan.Generic	iot-gateway-01	10
2026-04-12 17:01:00	Backdoor.Bot	ubuntu-siem	12

Search & Reporting

Flurs ▾ Help

index=security_events sourcetype=firewall action=blocked | stats dc(dest_port) AS unique_ports BY src_ip span=5m | where unique_ports>15

All time ▾

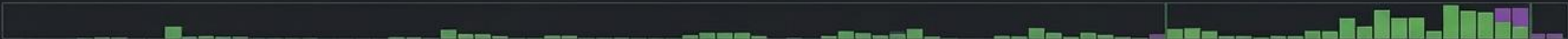


A10 ▾ 1h 1h → 🔊 📄 ⋮

Events timelined

■ Metrics

■ Metric



_time ↕	src_ip ↕	unique_ports ↕
2026-02-18 11:22:33	192.168.1.5	19
2026-01-05 09:15:20	203.0.113.10	32
2026-03-25 16:40:00	203.0.113.10	74
2026-01-11 08:55:00	203.0.113.10	80
2026-04-02 23:01:15	172.16.0.4	51
2026-02-14 10:05:01	203.0.113.10	32
2026-01-20 03:22:15	192.168.1.5	19
2026-03-10 12:00:00	10.0.0.1	26
2026-04-10 21:12:30	172.16.0.4	51
2026-01-01 10:05:01	203.0.113.10	32

index=security_events sourcetype=web_logs | bin _time span=1m | stats count BY _time, src_ip | where count>1000

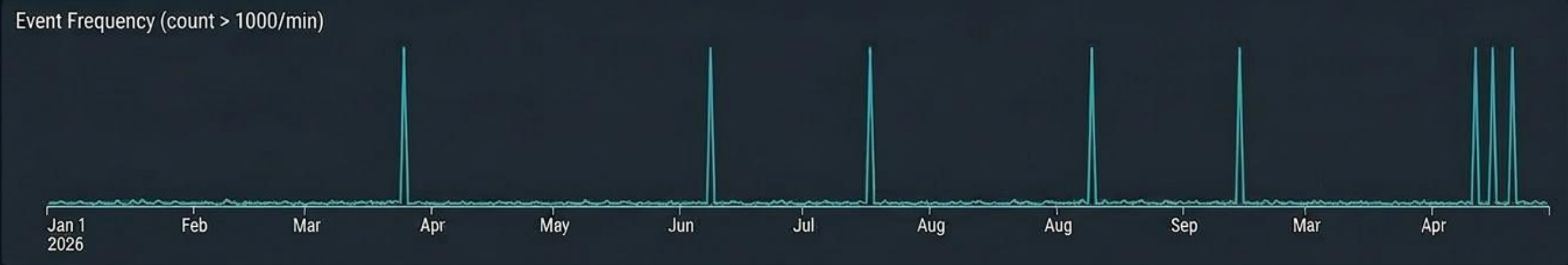
Search

Time range: All time ▼

Event Timeline

All Time

Battjewebs



Query Results (Unsorted)

_time ↕	src_ip ↕	count ↕
Mar 05, 2026, 03:15:00 PM	192.168.1.50	7100
Jan 20, 2026, 08:45:11 AM	10.0.0.101	1450
Feb 12, 2026, 11:30:00 PM	172.16.0.22	5800
Apr 01, 2026, 06:10:05 AM	192.168.1.50	6900
Mar 15, 2026, 01:22:33 AM	203.0.113.88	7950
Jan 05, 2026, 04:00:00 PM	10.0.0.101	2100
Apr 10, 2026, 10:59:59 PM	192.168.1.50	7300
Feb 28, 2026, 07:14:00 AM	172.16.0.22	4100
Mar 30, 2026, 09:01:22 PM	198.51.100.44	6200
Jan 28, 2026, 02:30:15 AM	10.0.0.101	3500

index=security_events sourcetype=auth_logs ("sudo" OR "su") action=failure | stats count BY user, src_host | where count>=3

All time



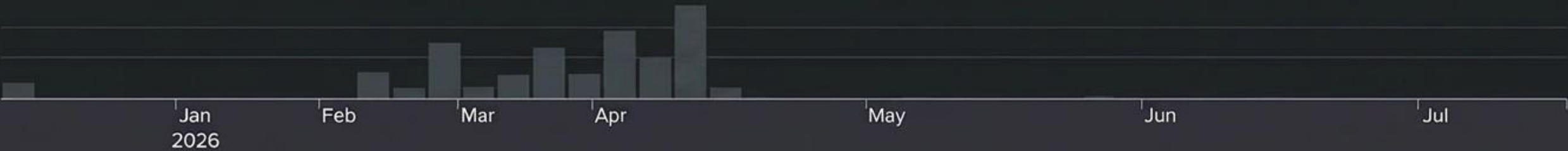
_time ↕	user ↕	src_host ↕	count ↕
2026-02-15	admin	pi-lab01	4
2026-04-03	analyst	server-02	13
2026-01-20	root	ubuntu-siem	7
2026-03-29	devops	audit-node-01	15
2026-02-01	iot-admin	pi-lab01	3
2026-04-10	root	server-02	9
2026-03-11	analyst	audit-node-01	11
2026-01-05	devops	ubuntu-siem	6
2026-02-22	admin	pi-lab01	14
2026-04-12	iot-admin	server-02	12

index=security_events sourcetype=proxy_logs direction=outbound ("SSN" OR "credit card" OR "confidential")
| stats count BY src_ip, dest_domain

All time ▾



All ▾ Es ID t↓ Event times ▾



Time

_time ↕	src_ip ↕	dest_domain ↕	count ↕
2026-02-15 10:15:30 EST	192.168.1.100	fileshare.example.com	15
2026-01-08 21:00:15 EST	10.0.0.50	dropbox.example.net	1
2026-04-03 14:45:00 EST	172.16.10.12	personal-mail.example.org	20
2026-03-22 08:30:12 EST	192.168.100.22	cloudsync.example.io	5
2026-01-20 05:10:05 EST	10.10.10.10	wetransfer.example.com	2
2026-03-01 12:00:00 EST	192.168.10.5	cloudsync.example.io	18
2026-01-30 09:55:55 EST	10.1.2.33	dropbox.example.net	1
2026-04-01 19:01:02 EST	172.16.58.12	wetransfer.example.com	11
2026-02-28 23:59:59 EST	192.168.1.100	fileshare.example.com	3

index=security_events sourcetype=web_logs uri_query=""' OR 1=1" OR uri_query="UNION SELECT" | stats count BY src_ip, uri_query

Q

All time ▾

Events Timeline



Statistics Results

_time	src_ip	uri_query	count
2026-02-14 03:33:10	192.168.10.11	id=1' OR 1=1 --	15
2026-01-15 10:11:55	10.1.20.5	q=-UNION SELECT password FROM users	28
2026-04-12 18:05:30	172.16.5.99	category_id=10 OR 'a'='a'	4
2026-01-28 09:20:15	192.168.10.11	q=UNION SELECT username, email FROM admin	22
2026-03-21 15:10:45	172.16.5.99	product_id=5'; waitfor delay '0:0:15' --	7
2026-04-01 01:40:01	203.0.113.15	user=admin'; DROP TABLE logs; --	12
2026-02-25 12:55:00	8.8.8.8	order_id=2 OR 1=1 --	3
2026-03-11 08:15:20	172.16.5.99	q=';exec master..xp_cmdshell 'net user'	19
2026-04-10 16:35:11	203.0.113.15	id=3 UNION SELECT 1,2,3 --	26
2026-01-05 17:55:00	192.168.10.11	user=root'; --	11

index=security_events sourcetype=firewall action=blocked dest_port IN (22,3389,5900,8080) | stats count BY src_ip, dest_port | where count>=5

All time ▾

🔍

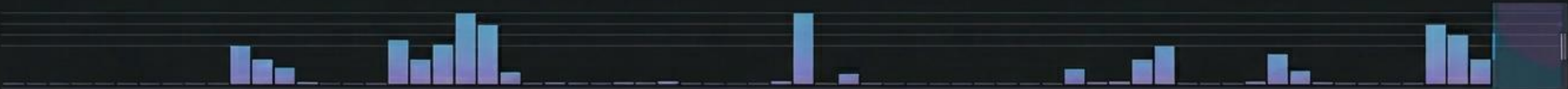


_time ↕	src_ip ↕	dest_port ↕	count ↕
2026-01-01 00:00:00	203.0.113.44	22	35
2026-03-15 10:01:01	198.51.100.9	3389	40
2026-04-13 18:30:00	192.0.2.88	5900	7
2026-01-01 18:15:33	192.0.2.88	8080	22
2026-04-12 21:58:33	192.0.13.23	22	18
2026-02-14 14:00:01	203.0.113.44	3389	25
2026-04-13 11:30:10	192.0.2.88	5900	10
2026-03-22 03:03:03	198.51.100.9	8080	20
2026-04-13 06:15:55	192.0.13.23	5900	15
2026-01-01 19:03:01	203.0.113.44	8080	5

```
index=security_events sourcetype=netflow direction=outbound | lookup known_ports port AS dest_port OUTPUTNEW category
| where isnull(category) | stats count BY src_ip, dest_port
```

All time ▾ ▾

Events Timeline



10 unsorted rows

	_time ↕	src_ip ↕	dest_port ↕	count ↕
1	2026-04-13 11:23:45	10.0.1.55	31337	5
2	2026-03-01 08:12:01	192.168.20.12	49152	1
3	2026-01-10 16:55:30	10.10.5.101	51515	18
4	2026-04-05 23:40:11	10.0.3.77	60001	12
5	2026-02-28 09:33:01	192.168.10.50	49200	25
7	2026-01-22 04:11:11	10.50.60.200	31337	2
8	2026-04-13 14:02:22	192.168.5.6	49152	9
9	2026-02-05 22:15:33	10.10.10.10	60001	3
11	2026-04-12 11:11:11	192.168.5.55	31337	15
12	2026-03-10 09:33:00	10.0.3.3	51515	6

index=security_events sourcetype=web_logs (uri_query="<script>" OR uri_query="javascript:") | stats count BY src_ip, uri_query

All time ▾

🔍

✓ 5 connected

Search (SPL)

Hot complite

Chure Inain data

All ▾

m

🔍

id

1/

⋮

Time staping ▾

Events timeline

Random events

With activity



4 | sowts

All rows

K4 counts

_time ▾	src_ip ▾	uri_query ▾	count ▾
2026-01-12 12:30:00.00	192.20.88.3	<script>alert('xss')</script>	8
2026-01-12 18:30:33.00	192.10.57.38	g=javascript:alert(1)	9
2026-01-12 12:37:59.00	192.10.57.35	comment=<script src=evil.js>	12
2026-04-12 18:02:49.00	192.10.57.36	comment=<script src=evil.js>	5
2026-01-12 18:00:20.00	192.10.58.79	q=javascript:alert(1)	6
2026-01-12 18:59:09.00	192.20.83.44	comment=<script *alert(:evil.js</script>	6
2026-01-12 18:52:09.00	192.10.57.32	comment=<script alert-:ircle=inervet=evil.js>	9
2026-01-12 18:09:03.00	192.10.57.33	q=javascript:alert(1)	13
2026-04-12 18:41:39.00	192.10.58.2	<script>alert('xss')</script>	15
2026-04-12 18:42:27.00	192.10.53.93	<script>alert('xss')</script>	15

XSS Attack Pattern Detected