Lab-to-SOC: Building an Open-Source Detection Pipeline

Suricata + ELK + Filebeat — From Install to Alert

Jan Rosas Ortiz · Douglass Brown

Networks Don't Tell You When They're Under Attack.

47% — **Credential Attacks**
Breaches starting with compromised credentials (Verizon DBIR)

16d — **Average Dwell Time**
Mean time before detection (IBM 2024)

80% — **Visibility Gap**
Organizations lacking centralized log visibility

Our Open-Source Detection Stack

Ubuntu
Operating System

Suricata
IDS

Elastic
Search · Viz

Filebeat
Log Shipper

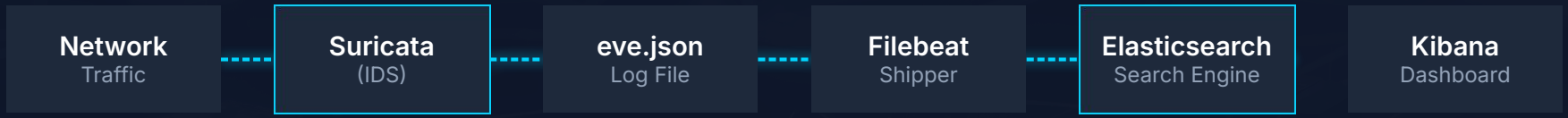
Jan Rosas Ortiz · Douglass Brown

Why Suricata?

	Snort (Legacy)	Suricata (Modern)
Threading	Single-threaded	Native Multi-threading
Output Format	Unified2 / PCAP	Native JSON (EVE)
Performance	CPU Bottlenecks	High-Speed Scalability
Modern Tooling	External conversion	ELK-Ready Out-of-the-Box

Jan Rosas Ortiz · Douglass Brown

The Pipeline



Jan Rosas Ortiz · Douglass Brown

Tuning for the Lab — Loopback Interface

```
af-packet:
- interface: lo # was eth0
cluster-id: 99
cluster-type: cluster_flow
```

"Without this, our internal attacks would be invisible."

Jan Rosas Ortiz · Douglass Brown

Three Custom Detection Rules

SSH Brute Force

Auth Failure Thresholds

Suspicious DNS

Non-Standard TLD Queries

Nmap SYN Scan

Stealth Port Discovery

`Local rules → /etc/suricata/rules/local.rules`

Jan Rosas Ortiz · Douglass Brown

Rule Anatomy

```
alert tcp any any → $ETH0 any (msg:"SSH Brute Force"; flags:S; threshold: type both, track by_src, count 5, seconds 60; sid:100001;)
```

Threshold: 5 attempts / 60 seconds

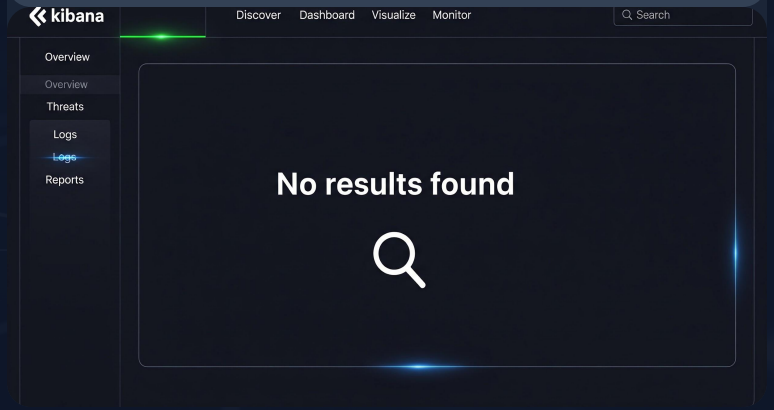
```
alert udp any any → any 53 (msg:"Suspicious DNS Query"; content:".bit"; nocase; sid:100002; rev:1;)
```

```
alert tcp any any → $HOME_NET any (msg:"Nmap SYN Scan"; flags:S; window:1024; sid:100003;)
```

Jan Rosas Ortiz · Douglass Brown

The Fix That Made It All Work

🚫 BEFORE



Empty Kibana Dashboard

✅ AFTER

Alerts Flowing

```
suricata.yml:
- module: suricata
    eve: enabled: true, var.paths: ["/var/log/suricata/eve.json"]
```

"Filebeat needed explicit eve.json path."

Jan Rosas Ortiz · Douglass Brown


Now we hunt.
From build — to validation
Jan Rosas Ortiz · Douglass Brown

Red Team Playbook

Nmap Port Scan
Reconnaissance Phase

SSH Brute (6x)
Credential Stuffing

DNS Lookup
C2 / Exfiltration Test

Simulation Commands

```
# SYN Stealth Scan
nmap -sS -T4 127.0.0.1
```

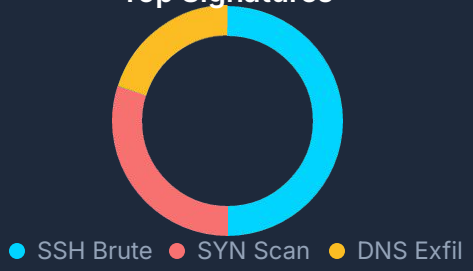
```
# Brute Force Loop
for i in {1..6}; do ssh user@127.0.0.1; done
```

Jan Rosas Ortiz · Douglass Brown

What Kibana Saw

Alerts Over Time

Top Signatures

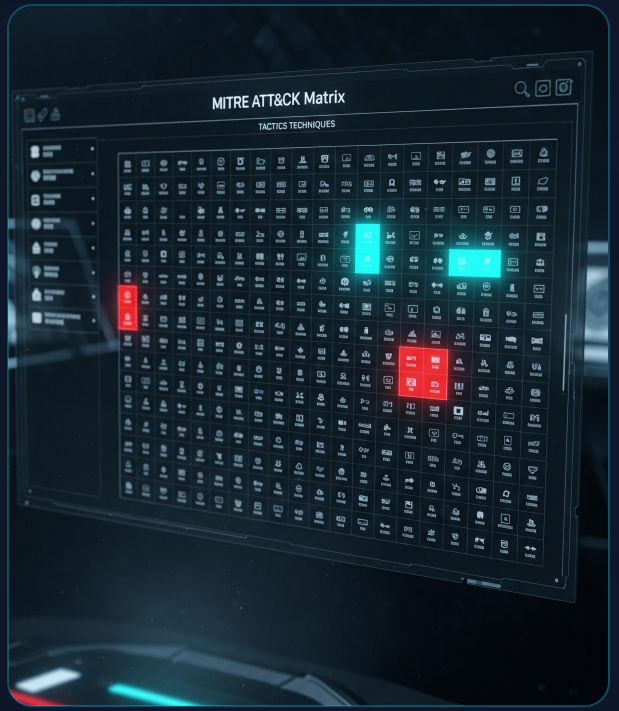


Timestamp	Signature	Source IP
2026-05-29 17:04:12	SSH Brute Force Attempt	192.168.1.45
2026-05-29 17:04:10	Nmap SYN Stealth Scan	192.168.1.45
2026-05-29 17:03:55	Suspicious DNS Query (.bit)	192.168.1.12

Jan Rosas Ortiz · Douglass Brown

Our Lab Maps to Real Attacker Tradecraft

Our Rule	MITRE Tactic	Real-World Example
`Nmap SYN`	TA0043 Recon	Conti ransomware
`SSH Brute`	TA0006 Cred Access	Credential stuffing
`Suspicious DNS`	TA0011 C2	Cobalt Strike beacons



Jan Rosas Ortiz · Douglass Brown

Honest After-Action

✅ What Worked

- All 3 attacks detected within seconds
- Filebeat module shipped clean JSON
- Dashboard usable for novice analyst

❌ What Didn't

- No real-time alerting (poll-based viz)
- Single-host lab — no lateral movement
- Rules need tuning to reduce false positives

Jan Rosas Ortiz · Douglass Brown

If This Were Production, We'd...

Re-enable Elasticsearch security
Enable authentication and encryption using `xpack.security`

Pipe alerts to Slack/PagerDuty
Automate incident response notifications via Elastalert integrations

Add Sigma rules + threat intel feeds
Leverage community standards and feeds like MISP or AlienVault OTX

Run Suricata in IPS mode
Transition from passive detection to active blocking of malicious traffic

Tune rules against known-good baseline
Continuous refinement to minimize false positives and alert fatigue

Three Takeaways

Visibility is not detection. Detection is not response.

Capturing data is only step one; actionable alerting and defined playbooks are the true goal.

Open-source can match commercial — IF you tune it.

ELK and Suricata provide enterprise-grade power but require hands-on configuration to perform.

The hardest part isn't the install. It's the rule design.

Infrastructure is easy; logic that separates signal from noise is where the real security work happens.

Jan Rosas Ortiz · Douglass Brown