Threat Hunting Workshop

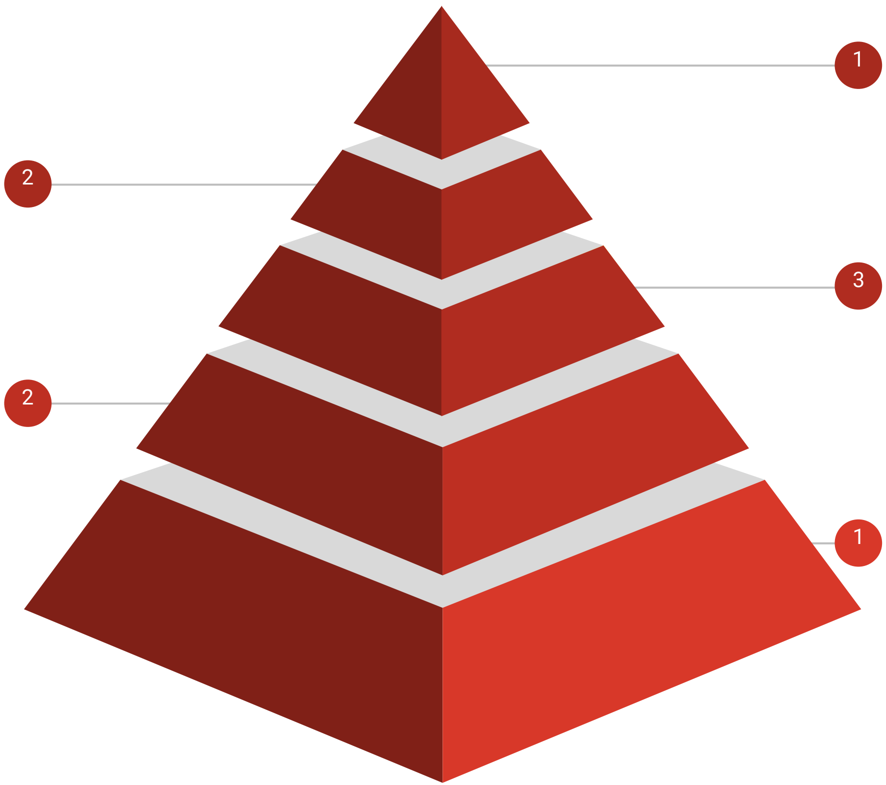
Getting started at Threat Hunting

Modules

1. Hunting Theory
2. Hunting Skills
3. Pre Hunt
4. After Hunt

Hunting Theory

Before we talk about Hunting...



Advanced Security
Threat Hunting, Threat Intelligence, Red Teaming

Security Operations
SIEM, Forensics, Incident Response, SOC, CERT

Security Baseline
Hardening, Antivirus, Firewall, IDS/IPS, Logging, Netflow, Vulnerability management

Operations & Engineering
Architecture, System standardization, Update & Patching, Backup/Restore

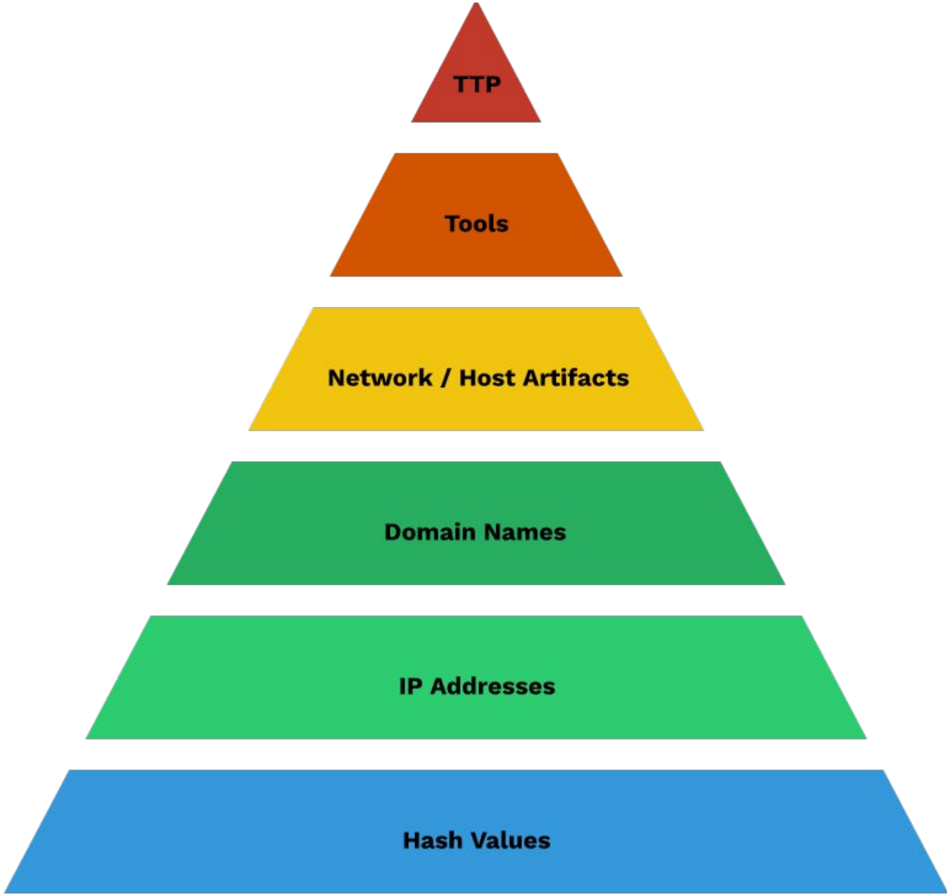
Organization & Procedures
Resources (Financial and Manpower), Processes, Permission and Intention

What is Threat Hunting

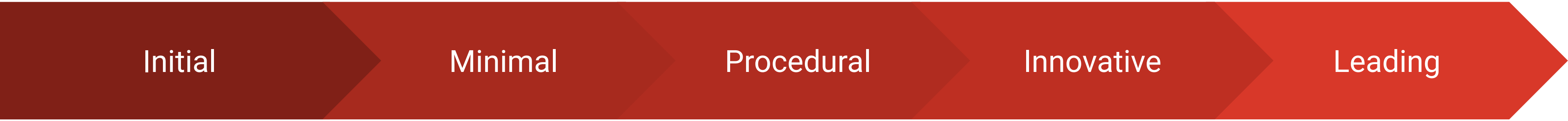
- Human centric
- Active defense measure
- Validate state of the network
- Search advanced threats
- Search for what traditional security system miss

Why Threat Hunting?

Catch the tactics,
techniques and procedures.



When To Hunt



Initial

- Little or no data collection
- Automatic alerts
- SIEM / IDS

Minimal

- Moderate data collection from key points (firewall, IDS)
- Threat Intelligence
- Splunk / ELK
- Domains, URL, Hashes
- Basic searches

Procedural

- High data collection throughout the infrastructure
- Develops hypothesis
- Histograms
- Existing hunting procedures
- Trends
- Hunting on regular basis

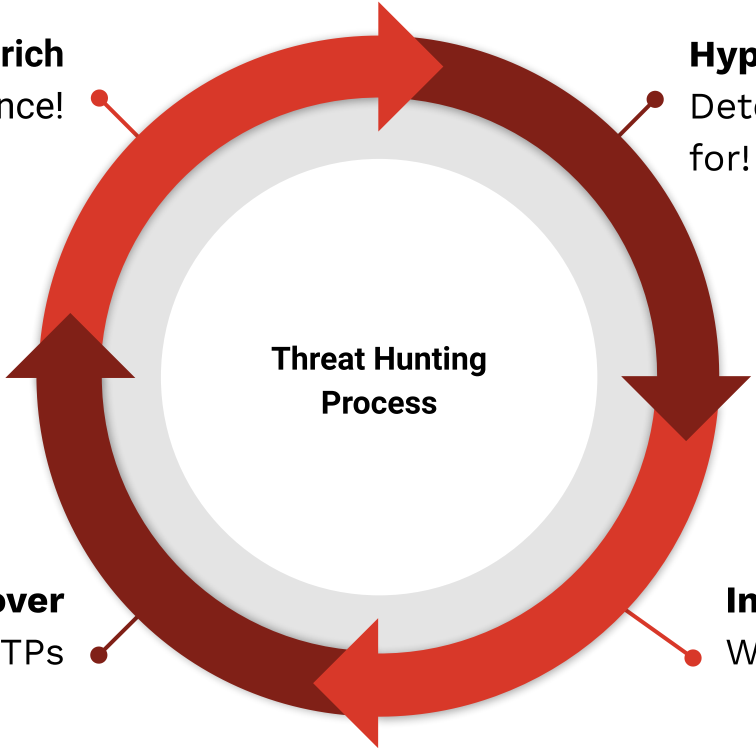
Innovative

- Risk scoring of threat intel
- Visualization and graphs
- Develops hunting procedures
- TTPs
- Builds library
- Data science

Leading

- Publishes and automates hunting procedures
- Complex ATPs
- Campaign tracking
- Sharing of IOCs
- Continuously improve capabilities

How To Hunt



Threat Hunting Process

Hypothesis
Determine what you hunt for!

Investigate
With tools and techniques

Uncover
New patterns and TTPs

Inform and Enrich
Hunt once!

Hunting Methodologies

- Attack Driven
- Data Driven
- Intelligence Driven

The Hunter

- Hunter only
- Alongside other security teams
- Curious and passionate
- Innovative and fast learning
- Not necessarily experienced

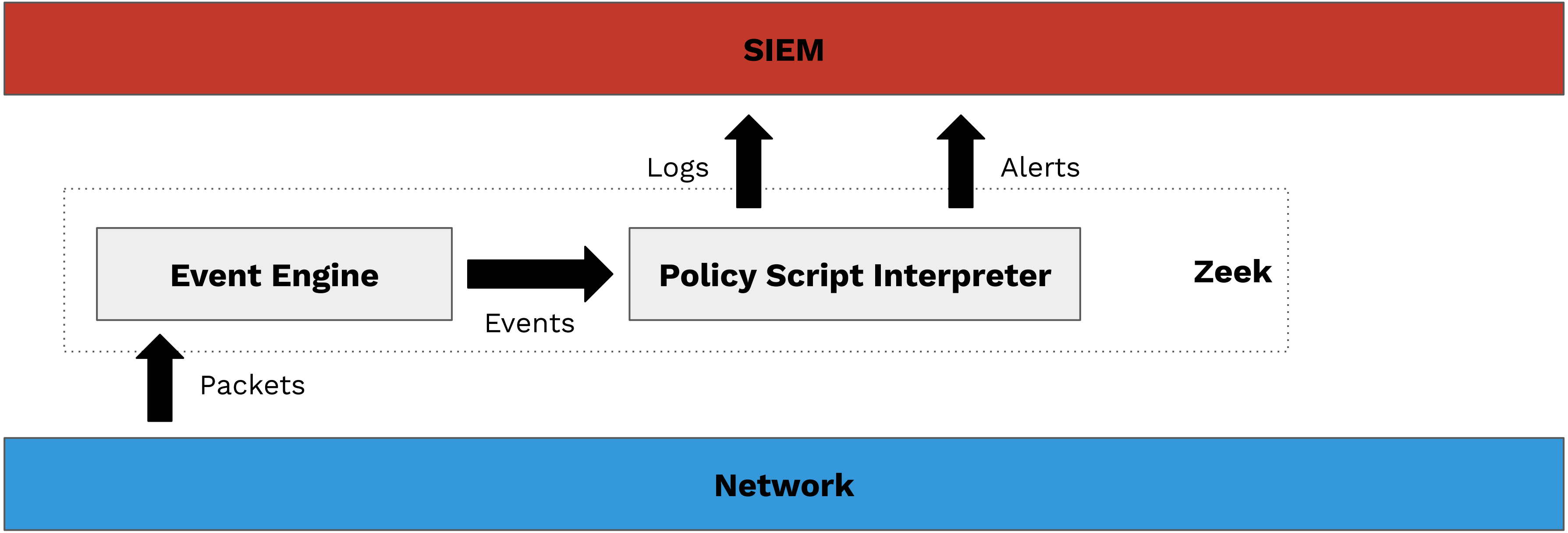
Hunting Skills

Skills Overview

- Zeek
- Suricata
- Host Logging
- Elastic Stack
- Facebook OSQuery & Kolide Fleet
- Google Rapid Response
- YARA

Zeek

Netflow on steroids.



Zeek

Use Cases

- Network monitoring and statistics
- Custom alerts
- Signature matching
- Anomaly detection
- IDS

Projects

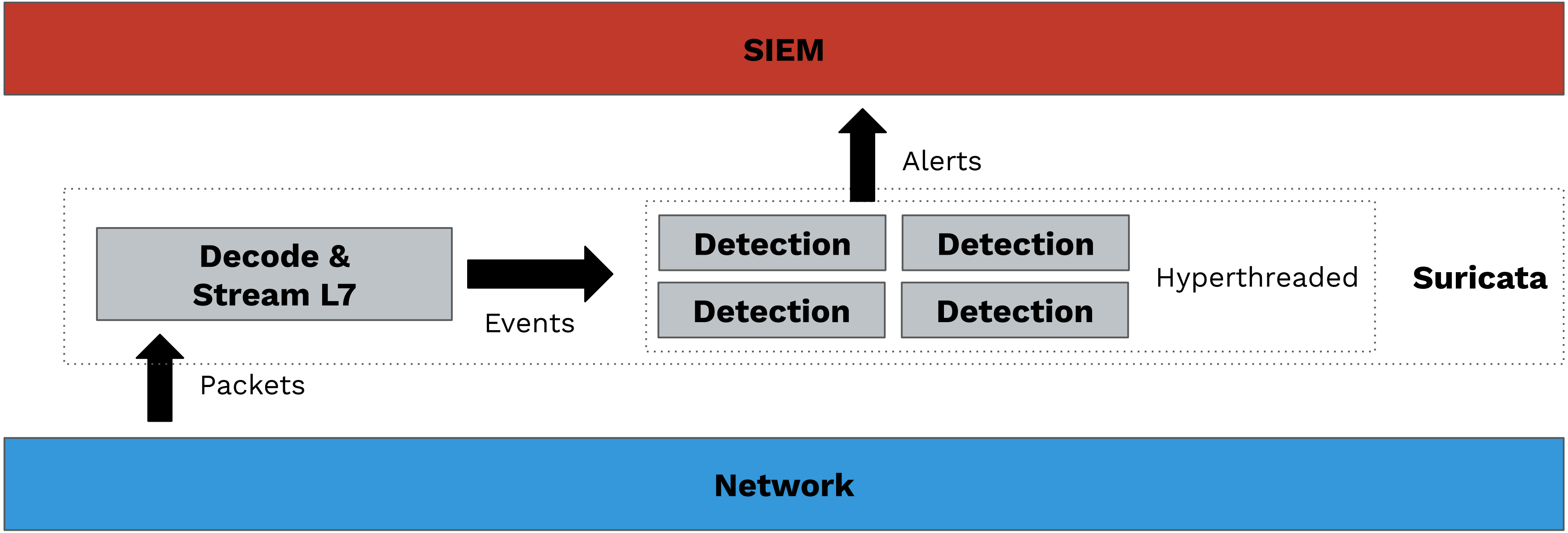
- OwlH
- RITA
- BZAR

MITRE ATT&CK Coverage

Initial Access	Execution	Persistance	Privilege Escalation	Defense Evasion	Credential Access
🟩 Discovery	🟩 Lateral Movement	Collection	🟩 Command and Control	🟩 Exfiltration	Impact

Suricata

Protocol aware and hyperthreaded Snort.



Suricata

Use Cases

- Signature matching
- IDS
- File extraction
- Layer 7 logging

Projects

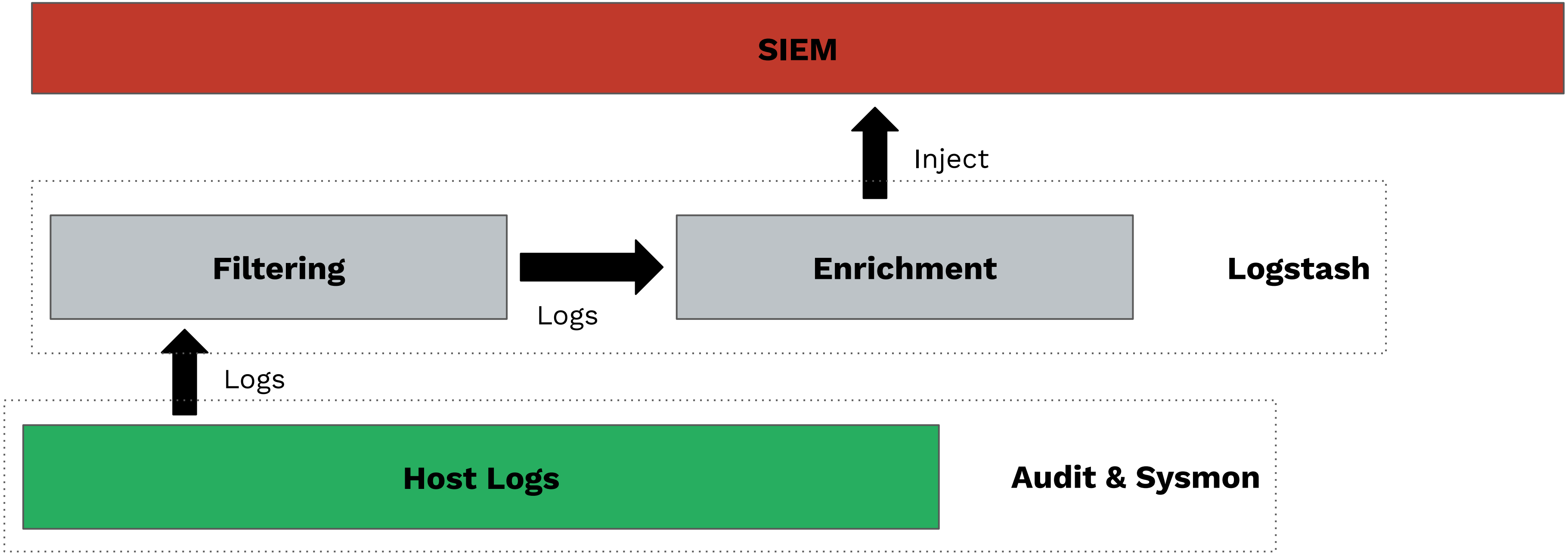
- Packet Fence
- OwlH
- Security Onion
- SELKS

MITRE ATT&CK Coverage

🟩 Initial Access	⬜ Execution	⬜ Persistance	🟩 Privilege Escalation	⬜ Defense Evasion	⬜ Credential Access
🟩 Discovery	🟩 Lateral Movement	⬜ Collection	🟩 Command and Control	🟩 Exfiltration	⬜ Impact

Host Logging

Crucial visibility on the endpoints.



Host Logging

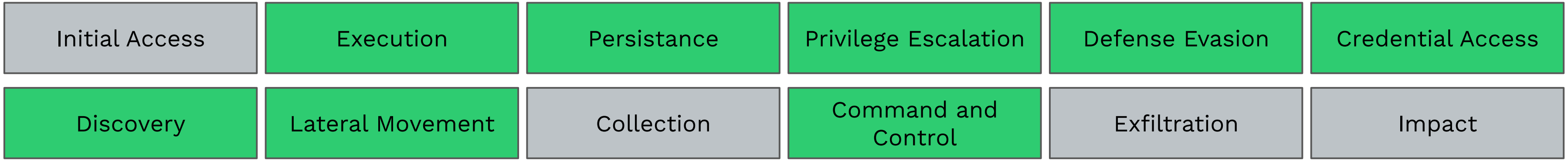
Use Cases

- Get visibility on endpoints
- Detect malicious behavior

Projects

- Sysmon
- sysmon-modular
- sysmon-config
- AuditD
- auditd-attack
- HELK

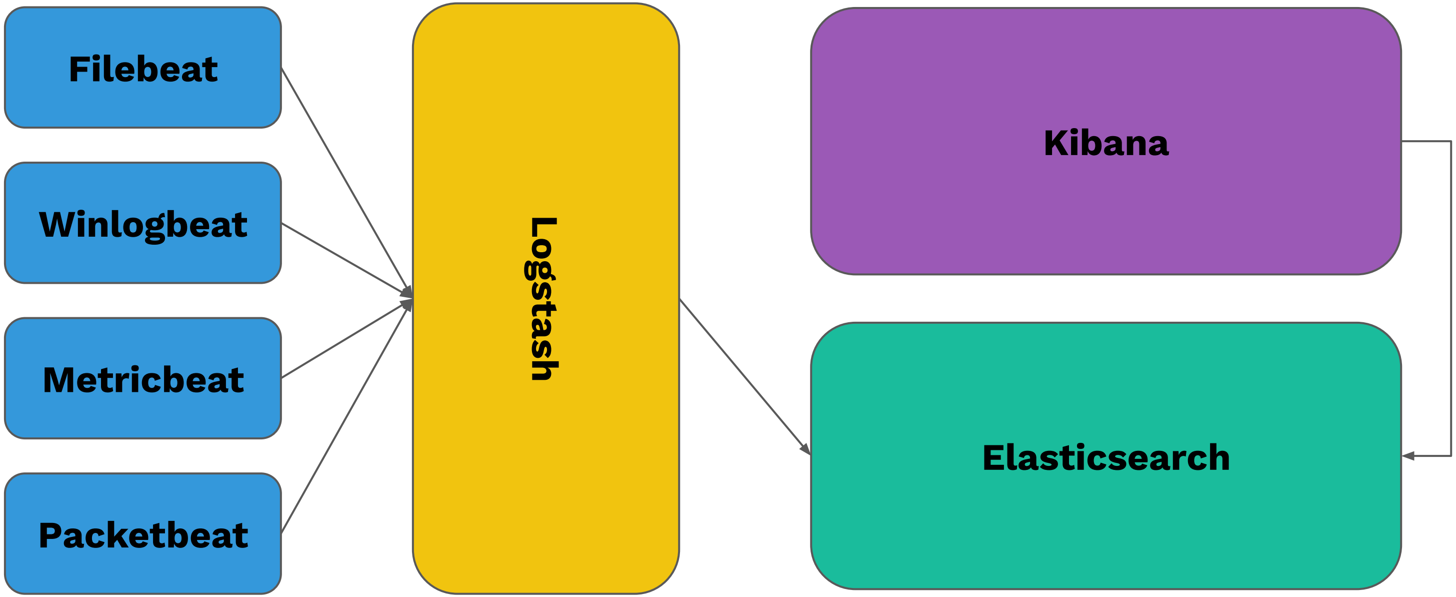
MITRE ATT&CK Coverage



Initial Access	Execution	Persistance	Privilege Escalation	Defense Evasion	Credential Access
Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact

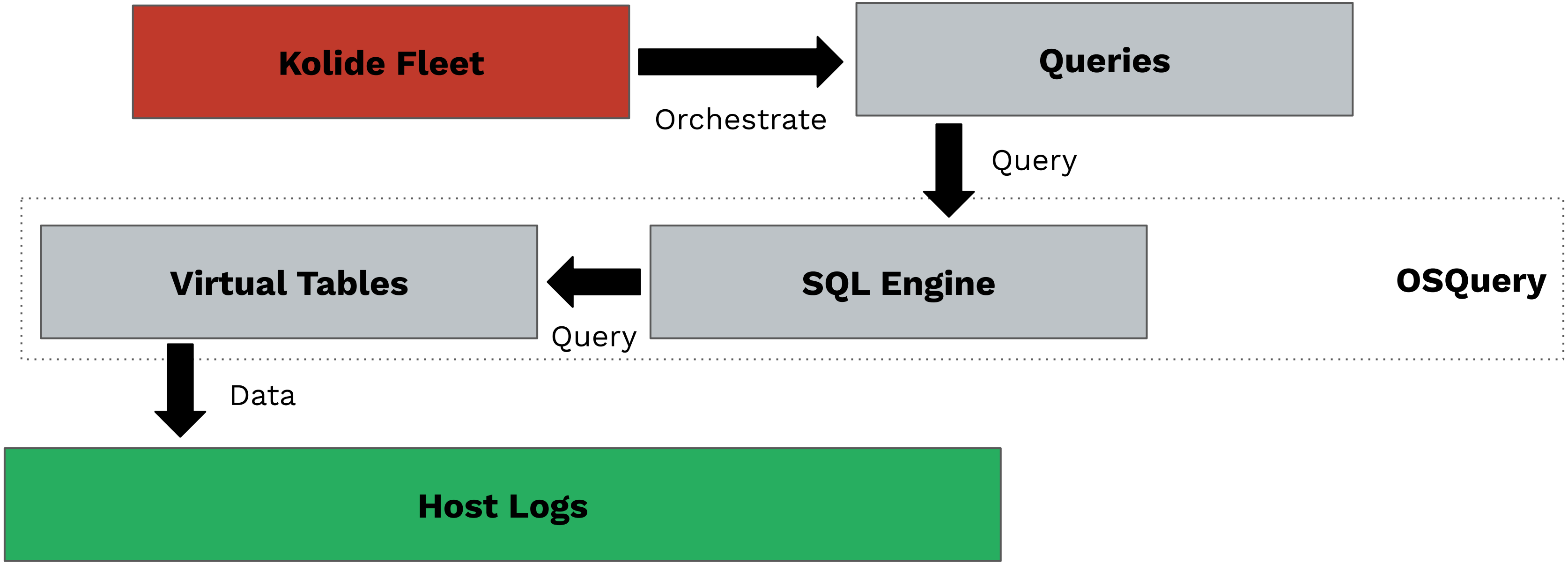
Elastic Stack

Open Source search and analytics.



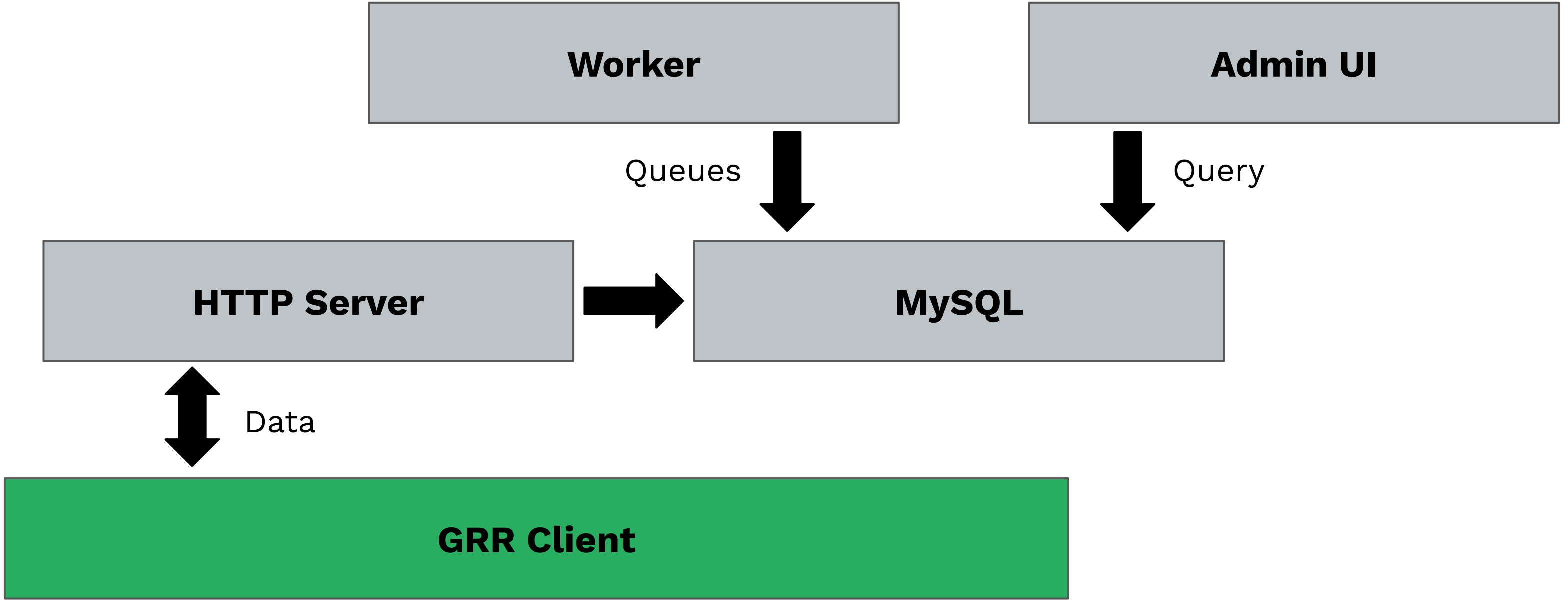
OSQuery and Fleet

SQL queries for endpoints.



Google Rapid Response

Remote live forensics for incident response.



YARA

Binary pattern matching made easy.

Meta

Strings

Condition

```
rule demo
{
     meta:
          author = “Stefan Seiler”

     strings:
          $hex_string = { E2 34 ?? C8 A? FB }
          $my_text_string = "text here"

     condition:
          $my_text_string and $my_hex_string
}
```

Pre Hunt Tasks

Modul Overview

- Know your environment
- Data governance
- Get visibility
- Threat Intelligence
- Develop hypothesis

Environment

- Core Services
- Classification
- Where

Data Governance

Documentation

Build a data dictionary for every eventlog collected in the environment. Document each field and what information it holds.

Standardization

Standardize and clean up the data with an schema. To easily search data across multiple sources.

Modeling

Identify relations between the logs and document them is vital to recreate and trace actions in logs.

Visibility

Write Playbook

- What do I look for?
- What data do I need to prove the thesis?

After Hunting

Modul Overview

- Review
- Improve
- Automate

Review

- Hunt Procedure
- Findings
- Share MISP

Improve

- Lack visibility?
- Lack skills?

Automate

- SIGMA Rules
- YARA Rules
- Zeek script
- OSQuery queries