Preparing For The Hunt

Gathering Security Telemetry With Free And Open Tools

Matthew Gracie
Senior Engineer
Security Onion Solutions

Who Am I And What Am I Talking About?

Threat Hunting

vs.

Alert Investigation

vs.

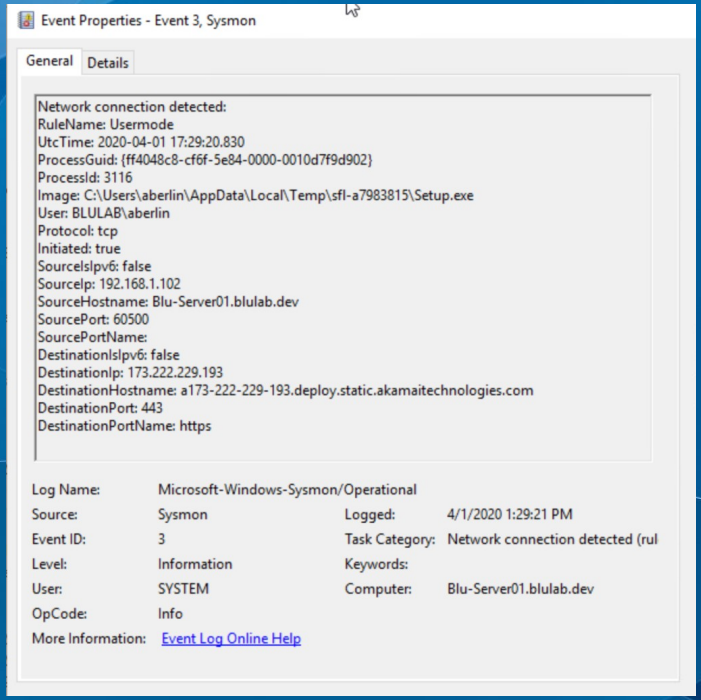
Detection Engineering

Network Traffic Telemetry

- Gathered via network tap or SPAN ports
- Metadata – Zeek
- Full Packet Capture

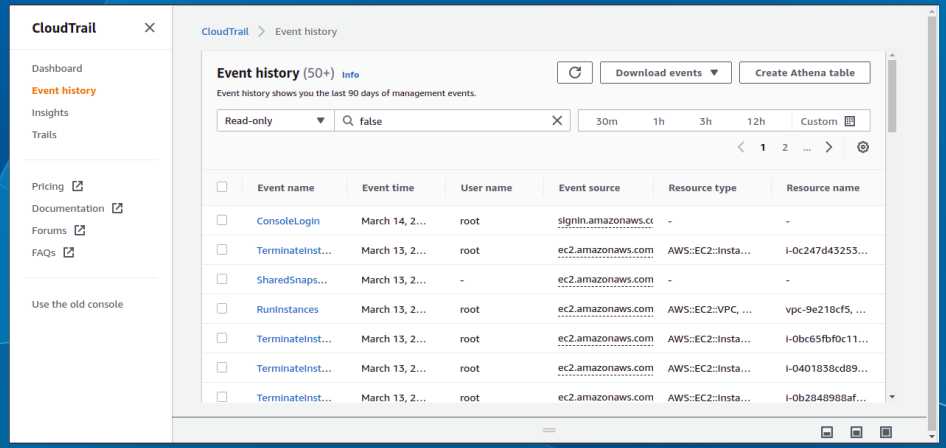
Endpoint Telemetry

- Windows Event Logs
- Sysmon Logs
- EDR / AV Logs
- Linux / MacOS Logs
- Network Device Logs



Cloud Telemetry

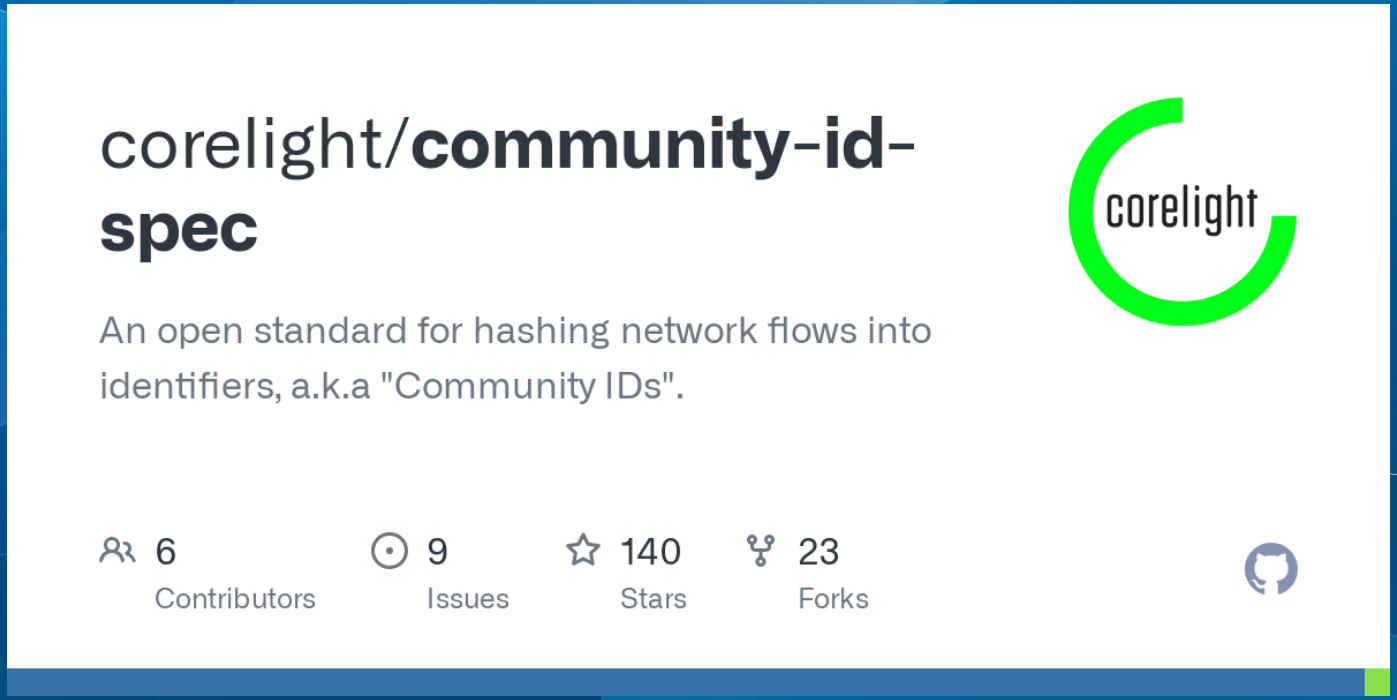
- AWS Cloudtrail
- Azure / O365
- Google Workspaces



Storage Backend

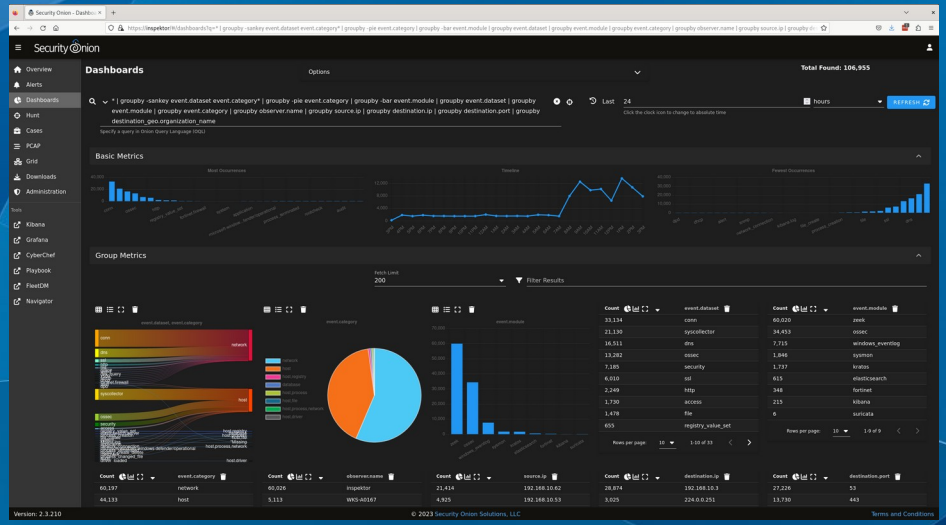
- Elasticsearch for parsing and storage
- Filebeat / Elastic Agent for transport and ingestion
- Elastic Common Schema (ECS) for normalization
- Enrichment pipelines for things like geography and ASN
- Clusters and scales horizontally

Community ID



Query Interface

- Elastic Kibana
- SOC Hunt / Dashboards



Demonstration

Questions?


@InfosecGoon


infosecgoon@roadflares.org


https://github.com/InfosecGoon