

Preparing For The Hunt

Gathering Security Telemetry With Free And Open Tools

Matthew Gracie
Senior Engineer
Security Onion Solutions

The background is a solid blue color with several overlapping, semi-transparent, curved shapes in various shades of blue. These shapes create a layered, geometric effect, resembling stylized waves or abstract architectural elements. The text is centered horizontally and vertically on the page.

Who Am I And What Am I Talking About?

Threat Hunting

vs.

Alert Investigation

vs.

Detection Engineering

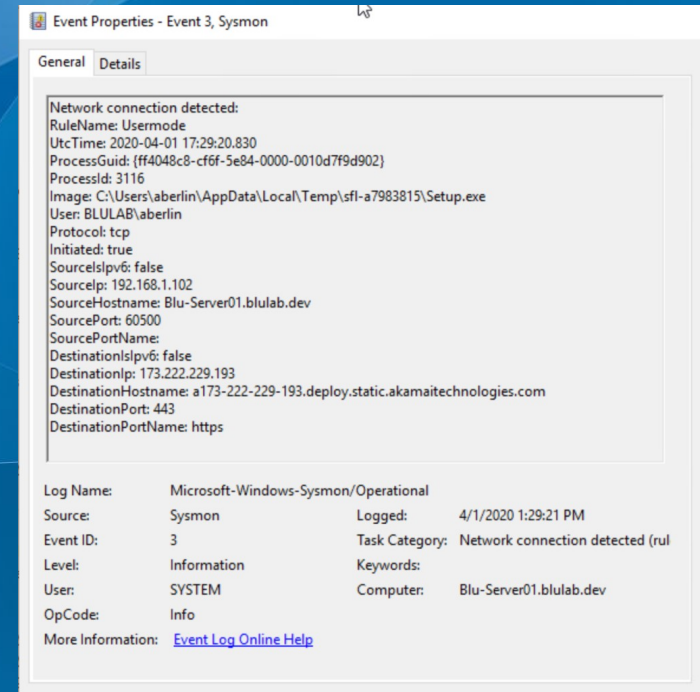
Network Traffic Telemetry

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

```
{  
  "ts": 1678462332.230685,  
  "uid": "Cjws4Uly0jJK7TMK3l",  
  "id.orig_h": "192.168.10.54",  
  "id.orig_p": 44356,  
  "id.resp_h": "52.4.89.81",  
  "id.resp_p": 80,  
  "trans_depth": 1,  
  "method": "GET",  
  "host": "firetv.captiveportal.com",  
  "uri": "/generate_204",  
  "version": "1.1",  
  "user_agent": "Dalvik/2.1.0 (Linux; U; Android",  
  "request_body_len": 0,  
  "response_body_len": 0,  
  "status_code": 204,  
  "status_msg": "No Content",  
  "tags": []  
}
```

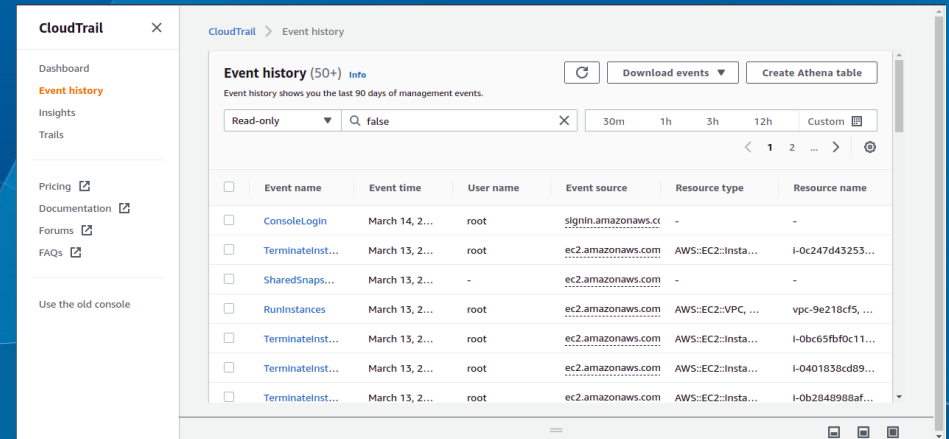
Endpoint Telemetry

- 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

corelight/**community-id-spec**



An open standard for hashing network flows into identifiers, a.k.a "Community IDs".



6

Contributors



9

Issues



140

Stars



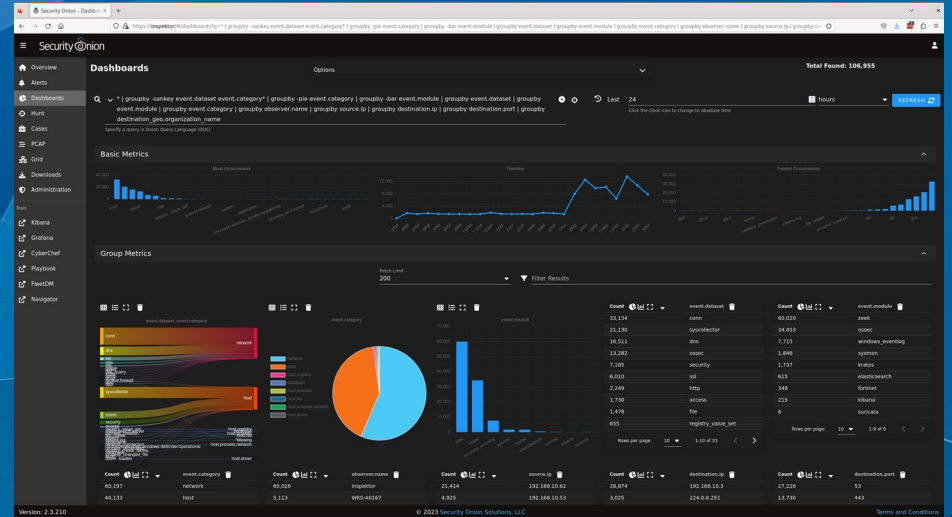
23

Forks



Query Interface

- Elastic Kibana
- SOC Hunt / Dashboards



Demonstration

Questions?



@InfosecGoon



infosecgoon@roadflares.org



<https://github.com/InfosecGoon>