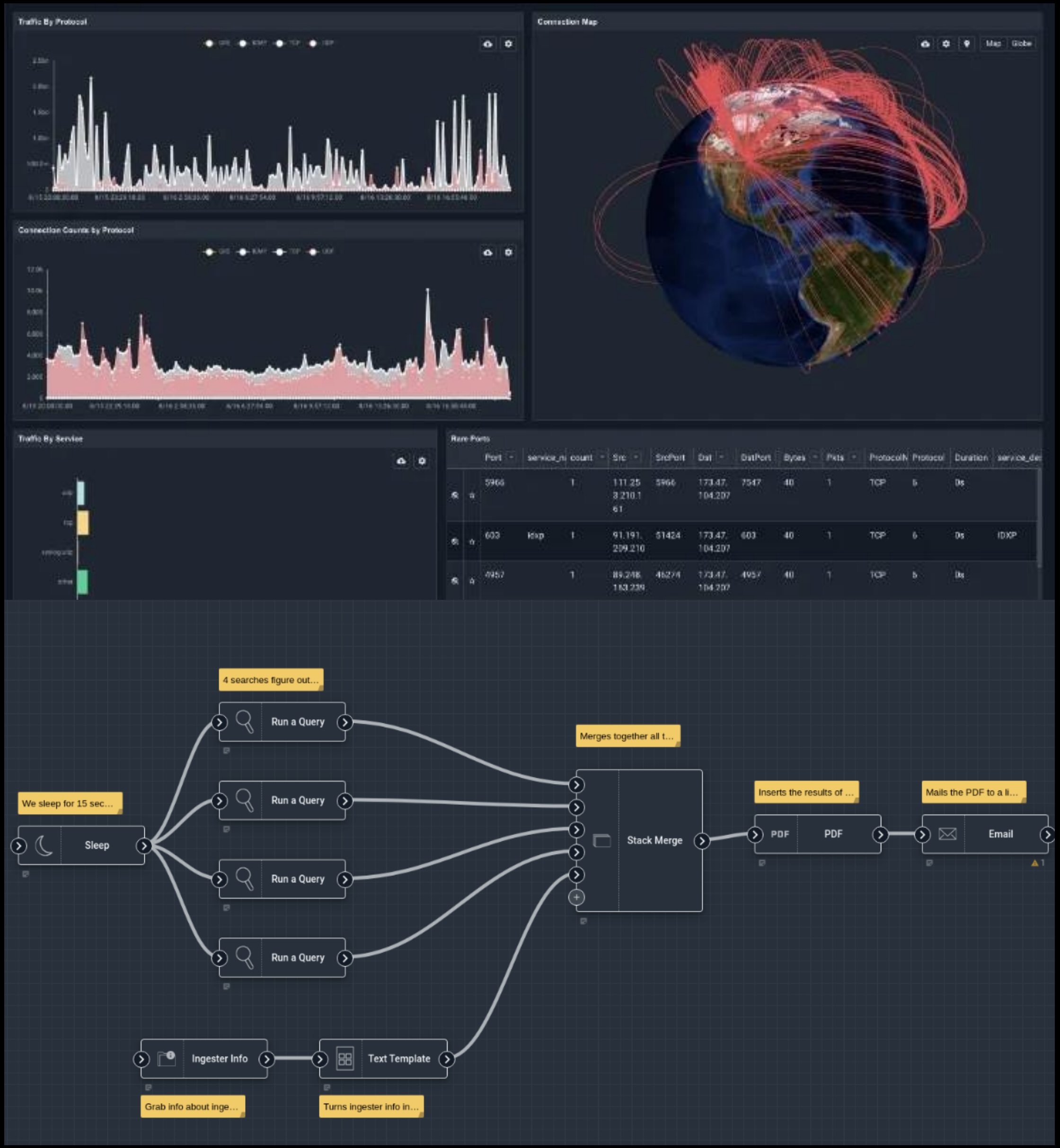
Software Assessment: Gravell | Splunk |Swimlane | SecurityOnion

Group 29: Grid-SIEM

Gravwell

- What it offers
  - Automation
    - Flow diagram
    - Query syntax based on linux cmd line
  - Kits
    - Linux syslog, threatblockr, netflow, ipfix
  - Easy to implement and configure
    - Designed around being able to set it up in minutes
  - Compiles incident timelines
  - Various dashboards
    - Automation, DNS, IP Netflow, Processes
- Licenses
  - Free community edition
    - 13.9GB/day data ingestion
    - Configurable data retention age-out
    - Scriptable searches
    - No single sign on
    - No cloud storage
    - Two user "seats"
  - Other licenses very expensive

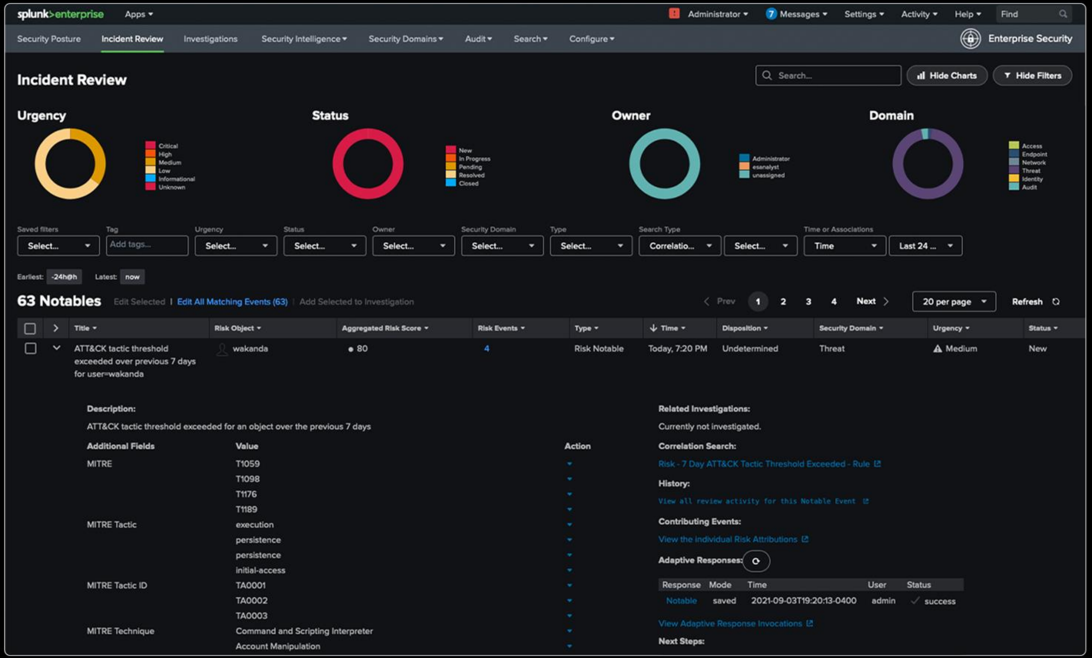


Rare Ports

Port	service_n	count	Src	SrcPort	Dst	DstPort	Bytes	Pkts	ProtocolN	Protocol	Duration	service_de
5966		1	111.25 3.210.1 61	5966	173.47. 104.207	7547	40	1	TCP	6	0s	
603	idxp	1	91.191. 209.210	51424	173.47. 104.207	603	40	1	TCP	6	0s	IDXP
4957		1	89.248. 163.239	46274	173.47. 104.207	4957	40	1	TCP	6	0s	

Splunk

- What is it? And who uses it?
  - Data analytics platform. SecurityOnion-like. Security teams for threat detection, incident response.
- How can it help us accomplish our project goals?
  - Offers real-time threat detection, can process log data from various nodes within PowerCyber architecture.
  - Offers advanced analytics capabilities to identify patterns and anomalies that may indicate a security threat.
- What does the free-tier offer?
  - Splunk Enterprise Free allows users to index and search up to 500 MB of data per day. There may be restrictions on features and data retention in the free version.
- Common problems working with this software?
  - Complex platform with many capabilities. Not intuitive. Could be expensive if we decide to move past free-tier.
- How easy is it to use?
  - Many resources for training. Especially useful to understand complex searches, data parsing and connecting to data sources.



Incident Review

Earliest: -24h@h Latest: now

63 Notables

Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status
ATT&CK tactic threshold exceeded over previous 7 days for user=wakanda	wakanda	● 80	4	Risk Notable	Today, 7:20 PM	Undetermined	Threat	⚠ Medium	New

Description:

ATT&CK tactic threshold exceeded for an object over the previous 7 days

Additional Fields	Value	Action
MITRE	T1059	
	T1098	
	T1176	
	T1189	
MITRE Tactic	execution	
	persistence	
	persistence	
	initial-access	
MITRE Tactic ID	TA0001	
	TA0002	
	TA0003	
MITRE Technique	Command and Scripting Interpreter	
	Account Manipulation	

Related Investigations:

Currently not investigated.

Correlation Search:

Risk - 7 Day ATT&CK Tactic Threshold Exceeded - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View the individual Risk Attributions

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2021-09-03T19:20:13-0400	admin	✓ success

View Adaptive Response Invocations

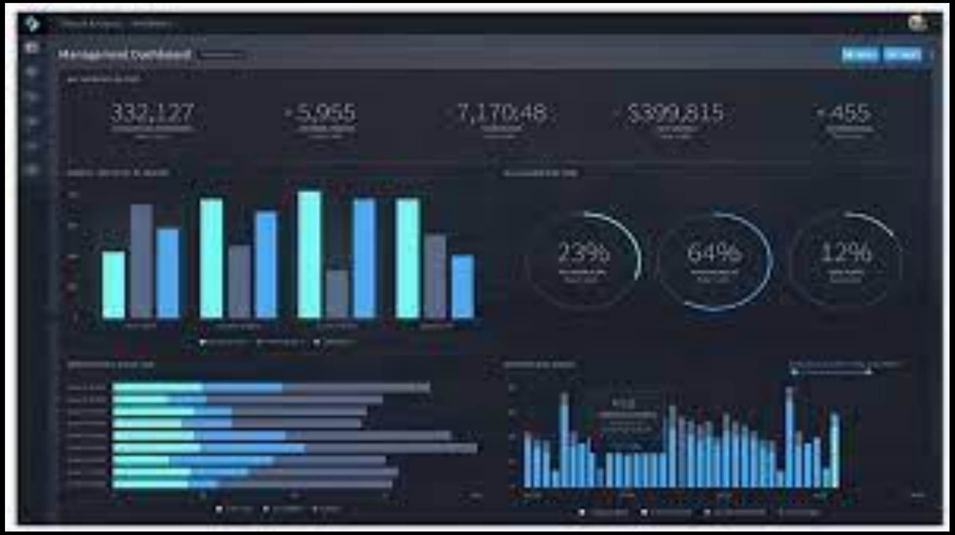
Next Steps:

Splunk vs Gravwell

- Splunk: Has been around for longer. Lots of resources and a supportive community of users. Could be more expensive and more difficult to work with since it has many features. Splunk's capabilities and solutions do not focus entirely on security.
- Gravwell: Attempts to address issues with Splunk. It is a newer platform known for its ease of use and flexibility. Security focused.

Swimlane

- Security Orchestration, Automation, and Response (SOAR) platform
  - Meant to streamline security operations
- Orchestrate workflows
  - Visual playbooks – users can create playbooks for different security processes
- Case management feature
  - Helps manage and track security incidents
- Dashboard for visualization of threat management
- Commercial product that has licensing costs

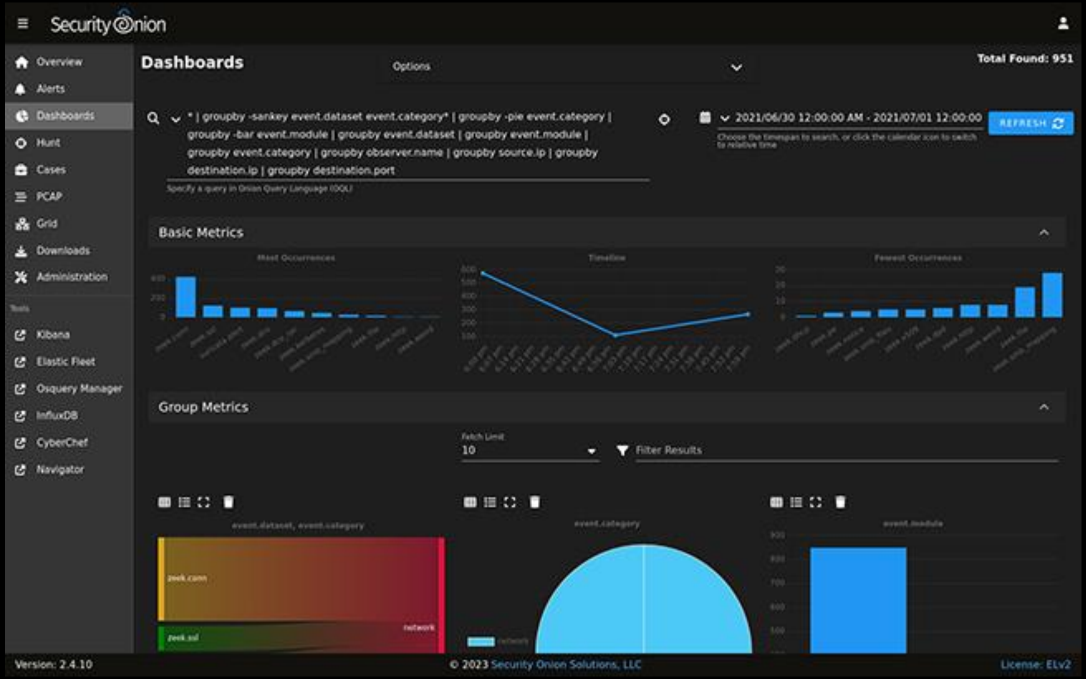


Swimlane vs SecurityOnion

- SecurityOnion
  - SIEM – real time analysis of security incidents
    - Alerting and analysis of possible incidents
  - Open source
  - monitoring, log management, intrusion detection
- Swimlane
  - SOAR – automate responses to collected threat-related data
    - Automated response to provided incidents
  - Commercial license required
  - Playbook automation, manage and track security incidents, automation of common security tasks

Security Onion

- Security Onion is an open source SIEM tool that primarily manages logs, monitoring, and intrusion detection.
- Security Onion has dashboards for system diagnostics that can be configured to display relevant information depending on the need.
- There are many tools that Security Onion can interface with and are included in the Security Onion Console
    - Kibana, Elastic Fleet, CyberChef, Playbook, and ATT&CK Manager.



```
* | groupby -sankey event.dataset event.category* | groupby -pie event.category | groupby -bar event.module | groupby event.dataset | groupby event.module | groupby event.category | groupby observer.name | groupby source.ip | groupby destination.ip | groupby destination.port
```

2021/06/30 12:00:00 AM - 2021/07/01 12:00:00

Total Found: 951

Fetch Limit: 10

Security Onion vs other options

- Security Onion does not have pricing plans or upgraded versions.
    - This could be good because the features that will be added are by the user's constraints and all of the features are available to all users
- Security Onion's machine learning capabilities are behind Splunk, Gravwell, and Swimlane.
    - For our project it could be useful because we will be doing the primary coding of a machine learning tool.
    - It could also take too much time to create a machine learning tool and it could be more efficient for us to focus training an already implemented machine learning tool.
- Security Onion fits the size of our project while giving it some of the tools that enterprise level SIEMs have.