Innovate!

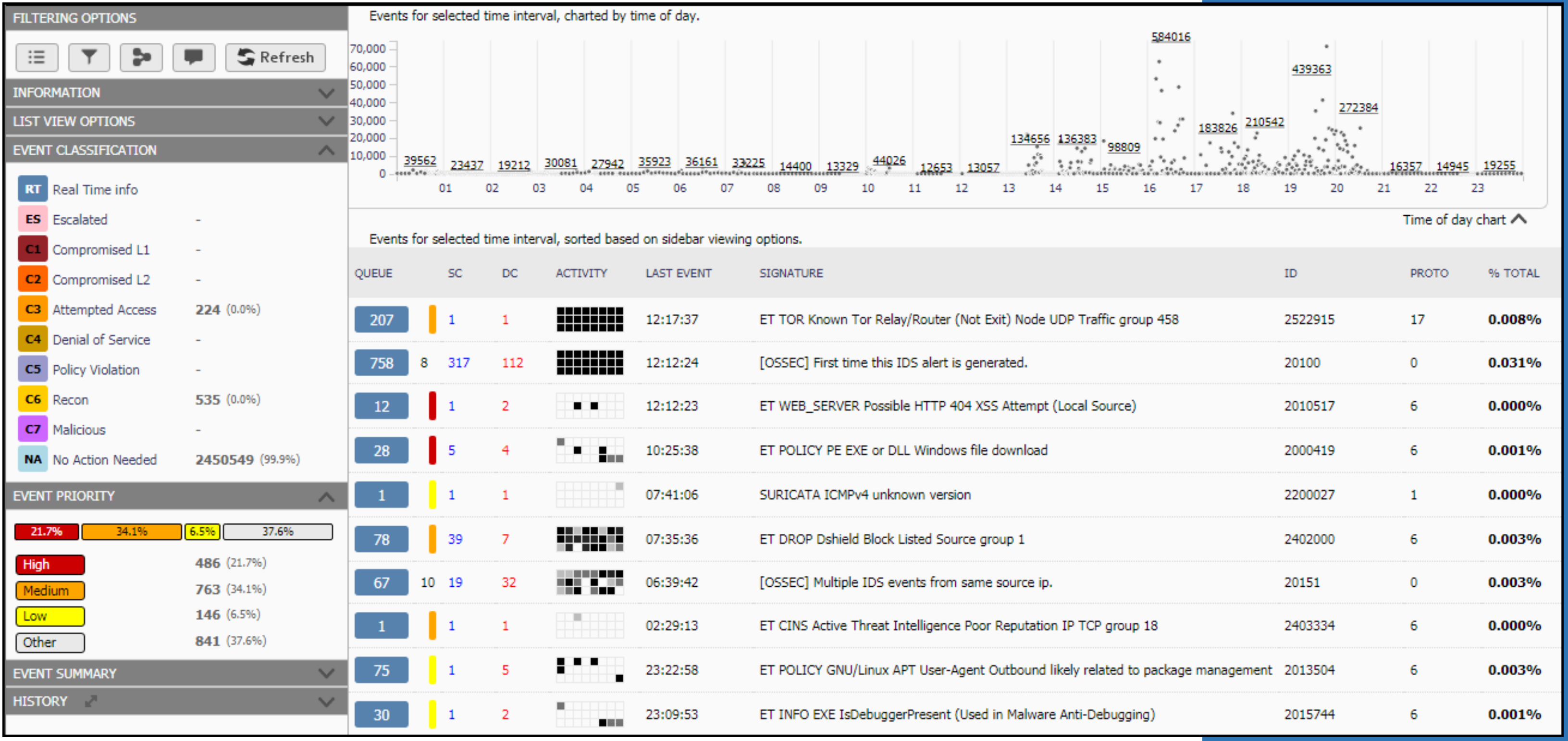
Security Onion

WHAT

Security Onion is a **Network Security Monitoring** (NSM) system that allows an analyst to peel back the layers of a network to see what's happening inside. It can be installed on a standalone server, incorporated into a VM environment, or distributed into a network with sensors linked to a master server. It combines multiple data gathering tools with multiple analysis tools to enable a human analyst high visibility to the traffic that is flowing on the network. It is not an automated protection system, it is a monitoring system that will provide visibility into network traffic as well as context around alerts and anomalous events. It requires human analysts to review alerts and investigate network activity for anomalies.

CAPABILITIES

- Open-Source
- Simple Setup
- Full Packet Capture
- Intrusion Detection
- Analysis Tools
- Packet Level Visibility
- Traffic Forensics
- Scalable



EVENT CLASSIFICATION

RT	Real Time info	
ES	Escalated	-
C1	Compromised L1	-
C2	Compromised L2	-
C3	Attempted Access	224 (0.0%)
C4	Denial of Service	-
C5	Policy Violation	-
C6	Recon	535 (0.0%)
C7	Malicious	-
NA	No Action Needed	2450549 (99.9%)

EVENT PRIORITY

21.7% 34.1% 6.5% 37.6%

High	486 (21.7%)
Medium	763 (34.1%)
Low	146 (6.5%)
Other	841 (37.6%)

Events for selected time interval, sorted based on sidebar viewing options.

QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
207	🟧	1	1		12:17:37	ET TOR Known Tor Relay/Router (Not Exit) Node UDP Traffic group 458	2522915	17	0.008%
758	8	317	112		12:12:24	[OSSEC] First time this IDS alert is generated.	20100	0	0.031%
12	🟥	1	2		12:12:23	ET WEB_SERVER Possible HTTP 404 XSS Attempt (Local Source)	2010517	6	0.000%
28	🟥	5	4		10:25:38	ET POLICY PE EXE or DLL Windows file download	2000419	6	0.001%
1	🟨	1	1		07:41:06	SURICATA ICMPv4 unknown version	2200027	1	0.000%
78	🟧	39	7		07:35:36	ET DROP Dshield Block Listed Source group 1	2402000	6	0.003%
67	10	19	32		06:39:42	[OSSEC] Multiple IDS events from same source ip.	20151	0	0.003%
1	🟧	1	1		02:29:13	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 18	2403334	6	0.000%
75	🟨	1	5		23:22:58	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	2013504	6	0.003%
30	🟨	1	2		23:09:53	ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	2015744	6	0.001%

Innovate! is an 8(a), woman- and minority-owned consulting firm focused on driving measurable business value, making a difference in the world, empowering our employees, and exploring the boundaries of what's possible with our clients.

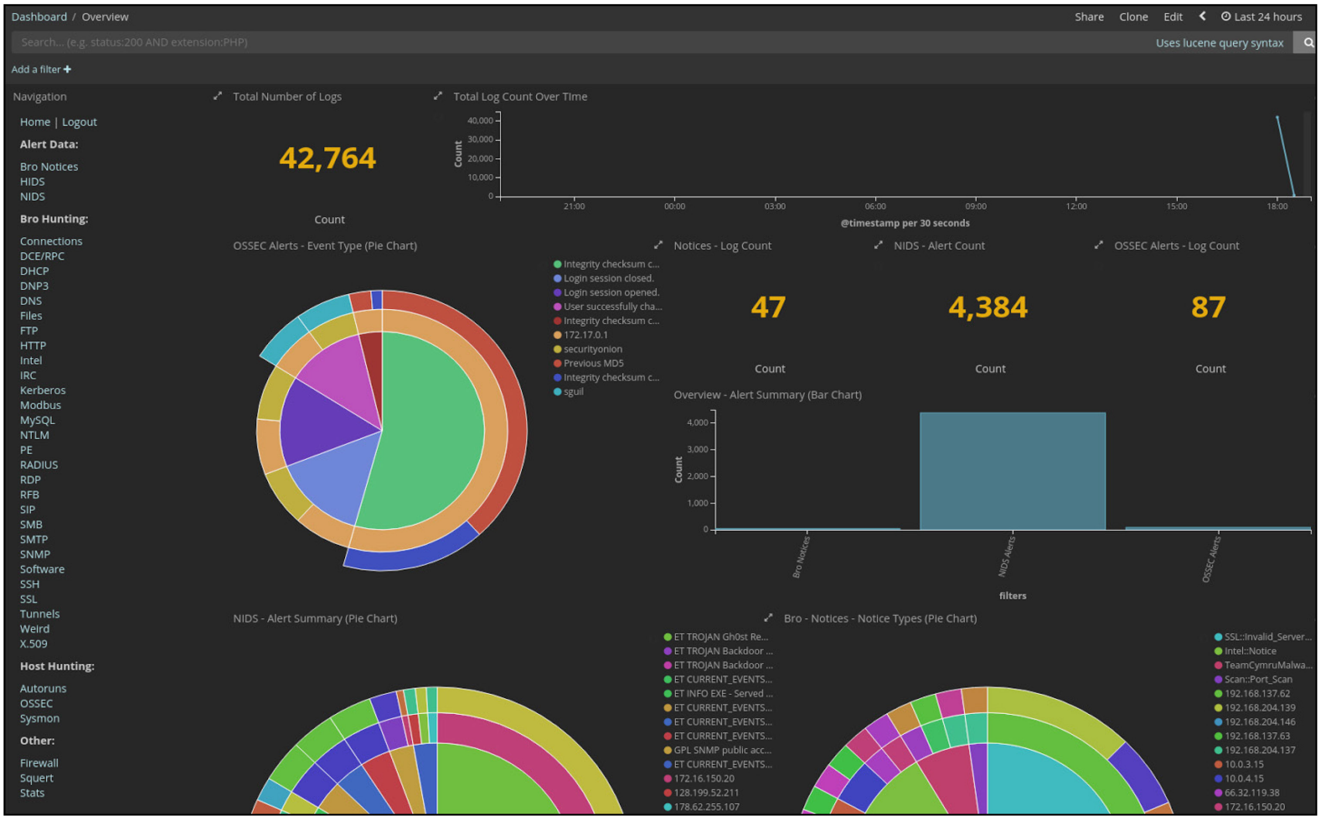
For more information on how Innovate! can support you, contact Frank Roberts (208) 699-2712

Security Onion combines Full Packet Capture with both rule-driven NIDS (Network Intrusion Detection System) using either ‘Snort’ or ‘Suricata’, and analysis-driven NIDS using ‘Bro IDS’.

- Rule-driven systems look at network traffic for fingerprints and identifiers that match known malicious, anomalous or otherwise suspicious data.
- Analysis-driven systems looks at all the data as a whole and correlates it into a framework that provides context for the events that can then be used as a trail to follow when investigating and analyzing activities.

Security Onion integrates multiple analysis tools to enable an analyst to make sense of the daunting amount of data collected.

- Sguil provides a single GUI that allows an analyst full visibility of the alerts as well as the individual packet data that can be correlated with associated traffic to investigate activities.
- ELSA (Enterprise Log Search & Archive) is a web-based query interface that allows analysts to easily search and chart syslog data.
- Squert is the current web interface (shown on the previous page) to the Sguil database that is much more user-friendly for quickly analyzing and reporting events.
- CapMe is a simple web interface enabling easy downloading of packet-capture data.
- Kibana is the next generation web interface giving advanced reporting with charts/graphs and visualization tools to better sort and filter the data for human consumption. Here is an example of the new interface coming soon.



WHY

The ability to view, analyze, and report on network traffic is essential to securing any systems or networks connected to the internet. Many networks rely solely on a combination of automated firewalls and end-point security software. Firewalls and/or Intrusion Detection Systems (IDS) are necessary but they are not designed for in-depth packet analysis/storage, nor is anyone monitoring them in real-time. End-point security is also necessary but it cannot be relied upon as the only means of protection either because it does not see the traffic that is flowing on the rest of the network. A separate system is needed to monitor and 'sniff' all the traffic that is flowing in and out of a network to give an analyst the visibility and tools needed to discover anomalies and investigate exploits or breaches in real-time as well as historically if a security issue has occurred. Security Onion is that system.

BARRIERS

The primary barrier to Network Security Monitoring is not the lack of data collection or automated tools that provide fancy interfaces, it is the lack of understanding that there is no replacement for the human analyst that must be monitoring and reviewing the alerts and network activity to not only protect the system from real-time intrusions but also investigate historical events. A Network Analyst is a combination of a security guard and detective. A broad range of networking and systems understanding is needed to decipher and make decisions on the vast and detailed information that Security Onion un-peels.

WHERE

Innovate! has been using Security Onion to monitor the traffic on its internal development VM servers for quite some time. The information gathered when first activating it were enlightening and resulted in multiple system security measures being implemented.

Innovate! is also actively designing and testing standalone plug-and-play systems that can quickly be inserted into client networks.

Interested in peeling back the layers of your network? Innovate! offers the monitoring appliances, installation, setup, and monitoring staff to give businesses the visibility they need to protect their assets and data from the ever-growing hurricane of malicious attacks. Contact us today for more information.