IMPORTANT FILES

	Configuration Files
Configuration	File
General Settings	/etc/nsm/securityonion.conf
Sensor Settings	/etc/nsm/ <hostname-interface>/sensor.conf</hostname-interface>
Maintenance Scripts	/etc/cron.d, /usr/sbin
Snort	/etc/nsm/ <hostname-interface>/snort.conf</hostname-interface>
Suricata	/etc/nsm/ <hostname-interface>/suricata.conf</hostname-interface>
Bro	/opt/bro
Bro Config	/opt/bro/etc/networks.cfg, node.cfg
Bro Local Policy/Scripts/Intel	/opt/bro/share/bro/site/local.bro (config) /opt/bro/share/bro/policy (scripts) /opt/bro/share/bro/intel/intel.dat (intel)
Elasticsearch Config	/etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/jvm.options (heap size)
Logstash Config	/etc/logstash/logstash.yml /etc/logstash/jvm.options (heap size) /etc/logstash/conf.d (standard pipeline config) /etc/logstash/custom (custom pipeline config and custom templates)
Kibana Config	/etc/kibana/kibana.yml
Curator Config	/etc/curator/config/curator.yml
Syslog-NG	/etc/syslog-ng/syslog-ng.conf
Wazuh	/var/ossec/etc/ossec.conf
Sguil (Server)	/etc/nsm/securityonion/sguild.conf
Sguil (Client)	/etc/sguil/sguil.conf
Sguil (Email)	/etc/nsm/securityonion/sguild.email
Onionsalt	/opt/onionsalt

	Log Files
Scope	File
Bro	/nsm/bro/logs/current/stderr.log (errors), reporter.log (errors/warnings), loaded_scripts.log (loaded scripts)
Elastalert	/var/log/elastalert/elastalert_stderr.log
Elasticsearch	/var/log/elasticsearch/ <hostname>.log</hostname>
Logstash	/var/log/logstash/logstash.log
Kibana	/var/log/kibana/kibana.log
OSSEC	/var/ossec/logs/ossec.log
Sensor Logs	/var/log/nsm/ <hostname-interface>/snortu-n.log, barnyard2-n.log, suricata.log, netsniff-ng.log</hostname-interface>
Sguild	/var/log/nsm/securityonion/sguild.log

Performance Tuning	
Target Parameter/File	
Bro	lb_procs in /opt/bro/etc/node.cfg
Snort/Suricata	IDS_LB_PROCS in /etc/nsm/ <hostname-interface>/sensor.</hostname-interface>
PF_RING	min_num_slots in /etc/modprobe.d/pf_ring.conf
Netsniff-NG	PCAP_OPTIONS, PCAP_SIZE, PCAP_RING_SIZE in /etc/nsm/ <hostname-interface>/sensor.conf</hostname-interface>

Security Onion

Rule Management	
Configuration	File
IDS Rules (Downloaded)	/etc/nsm/rules/downloaded.rules
IDS Rules (Custom)	/etc/nsm/rules/local.rules
Rule Thresholds	/etc/nsm/rules/threshold.conf
Disabled Rules	/etc/nsm/pulledpork/disablesid.conf
Modified Rules	/etc/nsm/pulledpork/modifysid.conf
PulledPork Config	/etc/nsm/pulledpork/pulledpork.conf
Wazuh Rules	/var/ossec/rules
Wazuh Rules (Custom)	/var/ossec/rules/local_rules.xml
Elastalert	/etc/elastalert/rules

Packet Filtering	
Scope File	
Server (Entire Deployment)	/etc/nsm/rules/bpf.conf
Sensor-Specific	/etc/nsm/ <hostname-interface>/bpf.conf</hostname-interface>
Component-Specific	/etc/nsm/ <hostname-interface>/bpf-bro.conf, bpf-ids.conf, etc.</hostname-interface>

DATA

	Data Directories
Data	Directory
Packet Capture (Sensor)	/nsm/sensor_data/ <hostname-interface>/dailylogs</hostname-interface>
Alert Data (Sensor)	/nsm/sensor_data/ <hostname-interface></hostname-interface>
Alert Data (Master)	/var/lib/mysql/securityonion_db
Bro (Archived) (Sensor)	/nsm/bro/logs/yyyy-mm-dd
Bro (Current Hr) (Sensor)	/nsm/bro/logs/current
Bro Extracted Files (Sensor)	/nsm/bro/extracted (only EXEs extracted, by default)
Elasticsearch (Master/Heavy/Storage)	/nsm/elasticsearch/nodes/x/indices

Originally Designed by: Chris Sanders - http://www.chrissanders.org - @chrissanders88
Updated by: Security Onion Solutions - https://securityonion.net - @securityonion
Security Onion Version: 16.04.6.1
Last Modified: 04.17.2019

COMMON TASKS

Task Command Check Service Status so-status Start/Stop/Restart All Services so-start stop restart Start/Stop/Restart Server Services Start/Stop/Restart Sensor so-sensor-start stop restart Start/Stop/Restart Docker docker start stop restart Start/Stop All Docker containers Start/Stop Specific so- <noun>-verb Ex: so-logstash-start stop Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) soup Update Rules Generate SO Statistics sostat Check Redis Queue Length redis-cli 'llen logstash-redis'</noun>		
Check Service Status Start/Stop/Restart All Services Start/Stop/Restart Server Services Start/Stop/Restart Sensor Services Start/Stop/Restart Docker Start/Stop/Restart Docker Start/Stop All Docker Containers Start/Stop Specific Container/Service Ex: so-logstash-start stop Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics so-start stop restart so-sensor-start stop restart so-losterstart stop restart so-sensor-start stop	General Maintenance	
Start/Stop/Restart Server Services Start/Stop/Restart Sensor Services Start/Stop/Restart Docker Services Start/Stop/Restart Docker Start/Stop All Docker Containers Start/Stop Specific Container/Service Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics so-squild-start stop restart so-sensor-start stop restart	Task	Command
Start/Stop/Restart Server Services Start/Stop/Restart Sensor Services Start/Stop/Restart Docker Start/Stop All Docker Containers Start/Stop Specific Container/Service Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics so-sensor-start stop restart so-sensor-start stop so-elastic-start stop so-elastic-start stop so-elastic-start stop so-elastic-start stop so-unou-verb Ex: so-logstash-start stop so-user-add so-user-passwd so-user-passwd so-allow so-allow so-allow-view ule-update Generate SO Statistics	Check Service Status	so-status
Services So-sguild-start stop restart Start/Stop/Restart Sensor So-sensor-start stop restart Start/Stop/Restart Docker docker start stop restart Start/Stop All Docker So-elastic-start stop Containers So-elastic-start stop Start/Stop Specific So- <noun>-verb Ex: so-logstash-start stop So-user-add So-user-add So-user-add So-user-passwd So-user-passwd Add/View Firewall Rules So-user-passwd Add/View Firewall Rules So-allow So-allow-view Update SO (and Ubuntu) Soup Update Rules rule-update Generate SO Statistics Sostat</noun>	Start/Stop/Restart All Services	so-start stop restart
Services So-sensor-start stop restart docker start stop restart Start/Stop All Docker Containers Start/Stop Specific Container/Service Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics So-elastic-start stop So-elastic-start stop So-user-bestart so-user-add So-user-passwd So-user-passwd So-user-passwd So-allow so-allow so-allow-view Update SO (and Ubuntu) Soup Update SO (sand Ubuntu) Soup		so-sguild-start stop restart
Start/Stop All Docker Containers Start/Stop Specific Container/Service Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics so-elastic-start stop so-vnoun>-verb Ex: so-logstash-start stop so-user-add so-user-passwd so-allow so-allow so-allow view ule-update sostat		so-sensor-start stop restart
Containers So-elastic-start stop Start/Stop Specific	Start/Stop/Restart Docker	docker start stop restart
Container/Service Ex: so-logstash-start stop Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password so-user-passwd Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) so-allow Update SO (and Ubuntu) soup Update Rules rule-update Generate SO Statistics sostat		so-elastic-start stop
Add Analyst (Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics so-user-passwd		
(Sguil/Squert/Kibana) User Change Analyst User Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics So-user-passwd so-user-passwd so-allow so-allow so-allow-view vule-update sostat	Container/Service	Ex: so-logstash-start stop
Password Add/View Firewall Rules (Analyst, Beats, Syslog, etc.) Update SO (and Ubuntu) Update Rules Generate SO Statistics so-allow so-allow-view rule-update sostat	•	so-user-add
(Analyst, Beats, Syslog, etc.) so-allow-view Update SO (and Ubuntu) soup Update Rules rule-update Generate SO Statistics sostat		so-user-passwd
Update Rules rule-update Generate SO Statistics sostat	•	30 401
Generate SO Statistics sostat	Update SO (and Ubuntu)	soup
	Update Rules	rule-update
Check Redis Queue Length redis-cli 'llen logstash-redis'	Generate SO Statistics	sostat
	Check Redis Queue Length	redis-cli 'llen logstash-redis'

Salt Commands (from Master Server)	
Task Command	
Execute Command	salt '*' cmd.run ' <command/> '
Verify Sensors Up	salt '*' test.ping
Update Minions	salt '*' state.highstate
Update Sensors	soup && salt '*' cmd.run 'soup -y'

Port/Protocols/Services (Distributed Deployment)	
Port/Protocol	Service/Purpose
22/tcp (Sensor/Master)	SSH access/AutoSSH tunnel from sensor(s) to Master
4505-4506/tcp (Master)	Salt comm from sensor(s) to Master
7736/tcp (Master)	Sguild comm from sensor(s) to Master

Support
Mailing List https://securityonion.net/docs/mailinglists
Reddit
https://www.reddit.com/r/securityonion/
Docs
https://securityonion.net/docs
Blog
https://blog.securityonion.net
Training, Professional Services, Hardware Appliances https://securityonionsolutions.com