COMMON TASKS

General Maintenance	
Task	**Command**
Check Service Status	so-status
Start/Stop/Restart All Services	so-start|stop|restart
Start/Stop/Restart Server Services	so-sguild-start|stop|restart
Start/Stop/Restart Sensor Services	so-sensor-start|stop|restart
Start/Stop/Restart Docker	docker start|stop|restart
Start/Stop/Restart All Docker Containers	so-elastic-start|stop|restart
Start/Stop Specific Component	so-<component>-<verb> (Ex: so-logstash-start)
Add Analyst (Sguil/Squert/Kibana) User	so-user-add
Change Analyst User Password	so-user-passwd
Add/View Firewall Rules (Analyst, Beats, Syslog, etc.)	so-allow so-allow-view
Update SO (packages and containers)	soup
Update Rules	rule-update
Generate SO Statistics	sostat
Check Redis Queue Length	so-redis-count

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

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

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

IMPORTANT FILES

Configuration Files	
Configuration	**File**
General Settings	/etc/nsm/securityonion.conf
Sensor Settings	/etc/nsm/<hostname-interface>/sensor.conf
Maintenance Scripts	/etc/cron.d, /usr/sbin
Snort	/etc/nsm/<hostname-interface>/snort.conf
Suricata	/etc/nsm/<hostname-interface>/suricata.yaml
Zeek/Bro	/opt/bro
Zeek/Bro Config	/opt/bro/etc/networks.cfg, node.cfg
Zeek/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/OSSEC	/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**
Zeek/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
Logstash	/var/log/logstash/logstash.log
Kibana	/var/log/kibana/kibana.log
Wazuh/OSSEC	/var/ossec/logs/ossec.log
Sensor Logs	/var/log/nsm/<hostname-interface>/snortu-n.log, barnyard2-n.log, suricata.log, netsniff-ng.log
Sguild	/var/log/nsm/securityonion/sguild.log

Performance Tuning	
Target	**Parameter/File**
Zeek/Bro	**lb_procs** in /opt/bro/etc/node.cfg
Snort/Suricata	**IDS_LB_PROCS** in /etc/nsm/<hostname-interface>/sensor.conf
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

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

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/OSSEC Rules	/var/ossec/rules/
Wazuh/OSSEC Rules (Custom)	/var/ossec/rules/local_rules.xml
Elastalert	/etc/elastalert/rules/

DATA

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

Originally Designed by: Chris Sanders
http://www.chrissanders.org - @chrissanders88

Updated by: Security Onion Solutions
https://securityonionsolutions.com - @securityonion

Security Onion Version: 16.04.6.4
Last Modified: 02.14.2020

Security Onion