Security Onion

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.conf
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
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
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.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

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
Component-Specific	/etc/nsm/<hostname-interface>/bpf-bro.conf, bpf-ids.conf, etc.

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
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

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 All Docker Containers	so-elastic-start|stop
Start/Stop Specific Container/Service	so-<noun>-verb Ex: so-logstash-start|stop
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 (and Ubuntu)	soup
Update Rules	rule-update
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