COMMON TASKS

General Maintenance	
Task	**Command**
All Scripts	/usr/sbin/so*
Check Status of All Services	so-status
Start/Stop/Restart Individual Service	so-<service>-<verb>
Start/Stop/Restart Suricata	so-suricata-<verb>
Start/Stop/Restart Zeek	so-zeek-<verb>
Start/Stop/Restart Elasticsearch	so-elasticsearch-<verb>
Add SOC User (Manager)	so-user-add
List SOC users (Manager)	so-user-list
Disable SOC user (Manager)	so-user-disable EMAIL@DOMAIN
Update Rules (Manager)	so-rule-update
Check Redis Queue Length (Manager)	so-redis-count
Add Firewall Rules (Analyst, Beats, Syslog, etc.)	so-allow
Advanced Firewall Control	so-firewall
Security Onion Update	soup

Salt Commands (from Manager)	
Task	**Command**
Verify Nodes are Up	salt * test.ping
Execute Command on all Nodes	salt * cmd.run '<command>'
Sync all Nodes	salt * state.highstate
Check service status on all nodes	salt * so.status

Port/Protocols/Services (Distributed Deployment)	
Port/Protocol	**Service/Purpose**
22/tcp (node/Manager)	SSH access
4505-4506/tcp (Manager)	Salt communication from node(s) to Manager
443/tcp (Manager)	Security Onion Console (SOC) web interface

Support	
Blog	https://blog.securityonion.net
Docs	https://securityonion.net/docs
Community Support Forum	https://securityonion.net/discussions
Training, Professional Services, Hardware Appliances	https://securityonionsolutions.com

IMPORTANT DOCS AND LOCATIONS

Configuration	
Component	**Documentation**
Most configuration is done via web interface. More information at: https://securityonion.net/docs/administration	
Salt	https://securityonion.net/docs/salt.html
Suricata	https://securityonion.net/docs/suricata.html
Zeek	https://securityonion.net/docs/zeek.html
Elastic Agent	https://securityonion.net/docs/elastic-agent.html
Logstash	https://securityonion.net/docs/logstash.html
Redis	https://securityonion.net/docs/redis.html
Elasticsearch	https://securityonion.net/docs/elasticsearch.html
Not managed by web interface	
SSH	https://securityonion.net/docs/ssh.html

Diagnostic Logs	
Description	**File/Directory**
Suricata	/opt/so/log/suricata/suricata.log
Stenographer	/opt/so/log/stenographer/stenographer.log
Zeek Logs Directory	/nsm/zeek/logs/current/
Zeek Diag Logs	stderr.log, reporter.log, loaded_scripts.log
Strelka	/opt/so/log/strelka/
Logstash	/opt/so/log/logstash/logstash.log
Elasticsearch	/opt/so/log/elasticsearch/<hostname>.log
Elastalert	/opt/so/log/elastalert/elastalert.log
Kibana	/opt/so/log/kibana/kibana.log
InfluxDB	/opt/so/log/influxdb/
Other log files	/opt/so/log/

Performance Tuning	
Target	**Documentation**
Suricata Tuning	https://securityonion.net/docs/suricata.html
Zeek Tuning	https://securityonion.net/docs/zeek.html

Packet Filtering with BPF	
Description	**Documentation**
BPF Information	https://securityonion.net/docs/bpf.html

Rule and Alert Management	
Description	**Documentation**
Managing Rules	https://securityonion.net/docs/rules.html
Detections	https://securityonion.net/docs/detections.html
Alerts	https://securityonion.net/docs/alerts.html
Elastalert	https://securityonion.net/docs/elastalert.html

DATA

Data Directories	
Data	**Directory**
Packet Capture (Sensor)	/nsm/pcap/
Suricata Data (Sensor)	/nsm/suricata/
Zeek (Archived) (Sensor)	/nsm/zeek/logs/<yyyy-mm-dd>/
Zeek (Current Hour) (Sensor)	/nsm/zeek/logs/current/
Zeek Extracted Files (Sensor)	/nsm/zeek/extracted/complete/
Elasticsearch (Manager/Heavy/Search)	/nsm/elasticsearch/nodes/<x>/indices/
Docker Registry	/nsm/docker-registry/
Strelka analyzed files	/nsm/strelka/processed/
InfluxDB	/nsm/influxdb/
so-import-pcap	/nsm/import/
so-import-evtx	/nsm/import/

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

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

Security Onion Version: 2.4
Last Modified: 05.29.2024

Security Onion