

Network Security Monitoring

INFO-6081 – Monitoring & Incident Response



FANSHAWE

Learning Outcomes

- Security Onion Components
- Analyst Tools
- Security Onion Deployment Types
- Security Onion Node Types
- Installing Security Onion
- QuickStart – Configuring Security Onion

Security Onion Core Components

Logstash

- A server-side data processing pipeline that processes data, transforms it, then sends it to a “stash”

Elasticsearch

- A distributed, RESTful search and analytics engine that can search many types of data (structured, unstructured, geo, metric)

Kibana

- Visualize Elasticsearch data and navigate the Elastic Stack

Security Onion Auxiliary Components

Curator

- Management for Elasticsearch indices and snapshots

ElastAlert

- Framework for alerting on anomalies, spikes, or other patterns of interest

FreqServer

- Detect randomness using character pair frequency analysis

DomainStats

- Performs mass domain analysis

Security Onion Analyst Tools – Kibana

Visualize Elasticsearch data and navigate the Elastic Stack



View pcap transcripts



Security Onion Analyst Tools – CyberChef

Manipulate data such with encoding like XOR, Base64, AES, etc...

Version 8.18.1sLast build: 19 days ago - New in v8: Automated encoding detection and simplified operation buildingOptionsAbout / Support?

Operations

Search...

Favourites★

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Recipe

From Hexdump

From Hex

DelimiterAuto

From Base64

AlphabetA-Za-z0-9+/=

☒ Remove non-alphabet chars

STEPBAKE!Auto Bake

Input

length: 1000
lines: 13

00000000 35 35 20 33 32 20 35 36 20 36 61 20 36 34 20 35 | 55 32 56 6a 64 5 |
00000010 38 20 34 61 20 37 30 20 36 34 20 34 38 20 36 62 | 18 4a 70 64 48 6b |
00000020 20 36 37 20 35 34 20 33 32 20 33 35 20 37 30 20 | 67 54 32 35 70 |
00000030 36 32 20 33 32 20 33 34 20 36 37 20 34 64 20 35 | 62 32 34 67 4d 5 |
00000040 34 20 35 39 20 37 35 20 34 64 20 34 34 20 35 31 | 4 59 75 4d 44 51 |
00000050 20 37 35 20 34 65 20 35 33 20 33 34 20 33 32 20 | 75 4e 53 34 32 |
00000060 34 39 20 34 37 20 36 63 20 37 35 20 35 39 20 33 | 49 47 6c 75 59 3 |
00000070 32 20 37 38 20 33 31 20 35 61 20 34 37 20 35 36 | 2 78 31 5a 47 56 |
00000080 20 37 61 20 34 39 20 34 35 20 34 65 20 33 35 20 | 7a 49 45 4e 35 |
00000090 35 39 20 36 64 20 35 36 20 37 39 20 35 31 20 33 | 59 6d 56 79 51 3 |
000000a0 32 20 36 38 20 36 63 20 35 61 20 36 39 20 34 31 | 2 68 6c 5a 69 41 |
000000b0 20 33 34 20 34 63 20 36 61 20 34 35 20 33 34 20 | 34 4c 6a 45 34 |
000000c0 34 63 20 36 61 20 34 35 20 36 38 | 4c 6a 45 68 |

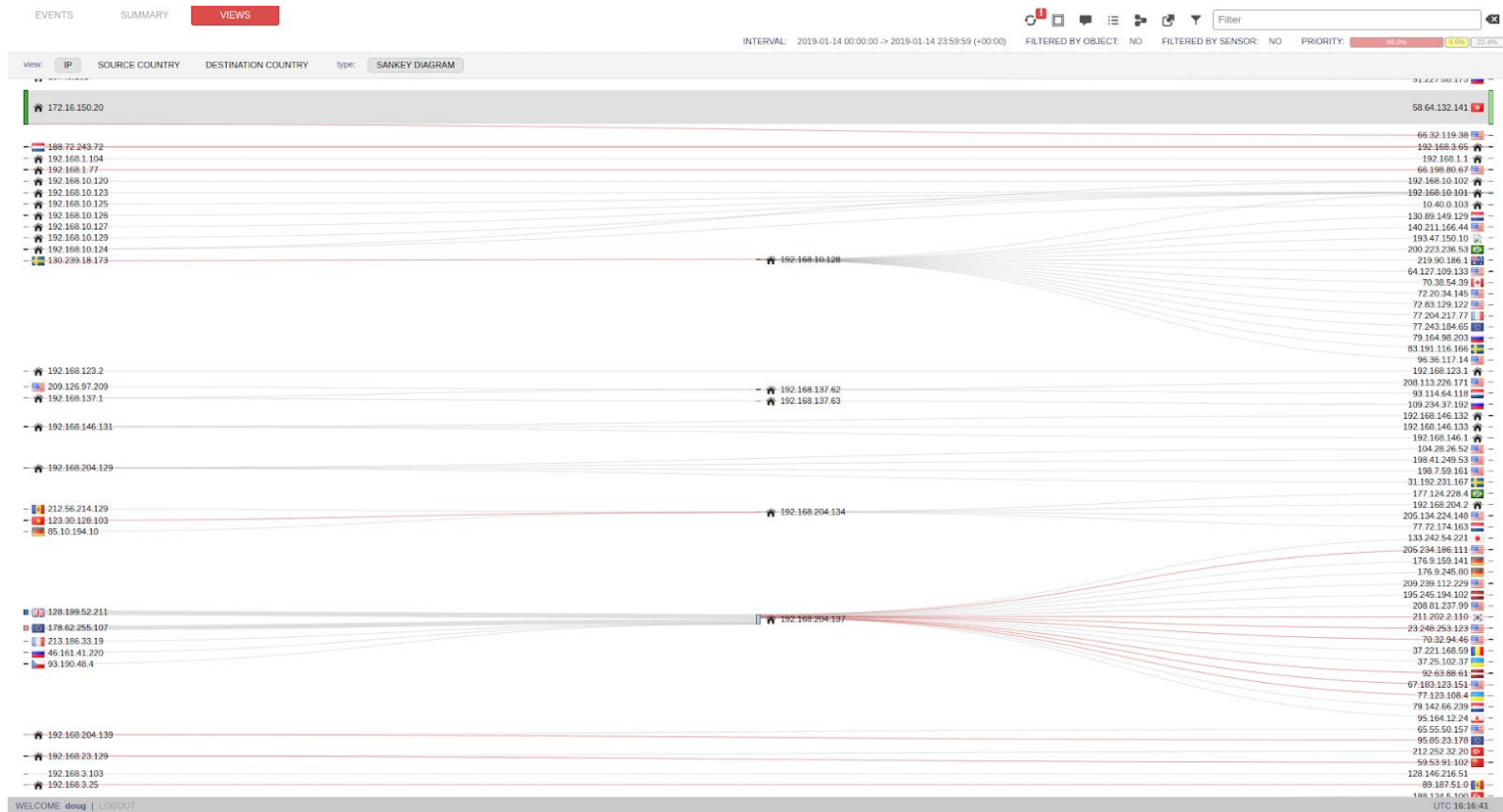
Output

start: 0time: 0ms
end: 61length: 61
length: 61lines: 1

Security Onion 16.04.5.6 includes CyberChef 8.18.1

Security Onion Analyst Tools – Squert

View event data from Sguil database (IDS alerts)



Security Onion Analyst Tools – Sguil

Access to realtime events, session data, and raw packet captures

File Query Reports Sound: Off ServerName: localhost UserName: doug UserID: 2 2019-01-10 12:41:00 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	securityonion-ens34-1	3.1941	2019-01-10 12:22:17	93.190.48.4	80	192.168.204.137	50086	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09
RT	1	securityonion-ens34-1	3.1942	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Landing Dec 29 2014
RT	12	securityonion-ens34-1	3.1943	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50088	6	ET CURRENT_EVENTS Nuclear EK Landing Jan 14 2014
RT	12	securityonion-ens34-1	3.1955	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50088	6	ET CURRENT_EVENTS Nuclear EK Landing Jan 06 2014
RT	12	securityonion-ens34-1	3.1967	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Landing Sep 29 2014
RT	12	securityonion-ens34-1	3.1979	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SWF
RT	12	securityonion-ens34-1	3.1991	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50088	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SWF M2
RT	45	securityonion-ens34-1	3.2003	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50089	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload
RT	6	securityonion-ens34-1	3.2022	2019-01-10 12:22:17	178.62.255.107	80	192.168.204.137	50089	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SilverLight M2
RT	2	securityonion-ens34-1	3.2054	2019-01-10 12:22:18	192.168.204.137	50091	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	8	securityonion-ens34-1	3.2056	2019-01-10 12:22:21	92.63.197.60	80	10.6.8.101	49203	6	ET INFO SUSPICIOUS Dotted Quad Host M2 Response
RT	8	securityonion-ens34-1	3.2057	2019-01-10 12:22:21	92.63.197.60	80	10.6.8.101	49203	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	securityonion-ens34-1	3.2058	2019-01-10 12:22:21	92.63.197.60	80	10.6.8.101	49203	6	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
RT	10	securityonion-ens34-1	3.2059	2019-01-10 12:22:21	10.6.8.101	49204	92.63.197.60	80	6	ET INFO Executable Download from dotted-quad host
RT	20	securityonion-ens34-1	3.2060	2019-01-10 12:22:21	10.6.8.101	49204	92.63.197.60	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
RT	16	securityonion-ens34-1	3.2061	2019-01-10 12:22:21	10.6.8.101	49204	92.63.197.60	80	6	ET TROJAN Single char EXE direct download likely trojan (multiple families)
RT	3	securityonion-ens34-1	3.2068	2019-01-10 12:22:21	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	1	securityonion-ens34-1	3.2101	2019-01-10 12:22:21	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	1	securityonion-ens34-1	3.2111	2019-01-10 12:22:21	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	1	securityonion-ens34-1	3.2121	2019-01-10 12:22:21	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	13	securityonion-ens34-1	3.2122	2019-01-10 12:22:17	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	13	securityonion-ens34-1	3.2123	2019-01-10 12:22:17	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	13	securityonion-ens34-1	3.2125	2019-01-10 12:22:17	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2
RT	13	securityonion-ens34-1	3.2126	2019-01-10 12:22:17	192.168.204.137	50089	176.9.159.141	80	6	ET TROJAN FarelPony Download Checkin 2

securityonion-ens34-1_2022

Reverse DNS: 178.62.255.107
Src Name: qadir.nodia.se
Dst IP: 192.168.204.137
Dst Name: Unknown

Whols Query: None • Src IP • Dst IP

% This is the RIPE Database query service.
% The objects are in RPSL format.
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, please use the --update flag.

% Information related to 178.62.128.0 - 178.62.128.255:
% Abuse contact for 178.62.128.0 - 178.62.128.255: DIGITALOCEAN-AMS-5

inetnum: 178.62.128.0 - 178.62.255.255
netname: DIGITALOCEAN-AMS-5
descr: DigitalOcean Amsterdam
country: NL
admin-c: PT7353-RIPE
tech-c: PT7353-RIPE
status: ASSIGNED

Search Abort Close

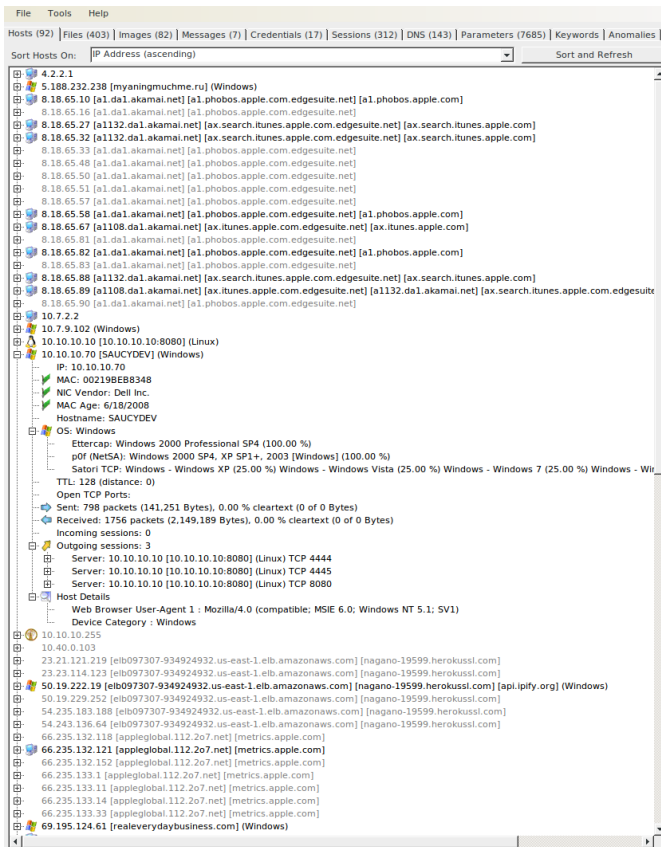
Debug Messages

192.168.204.137 and port 80 and port 50089 and proto 6) (vlan and host 178.62.255.107 and host 192.168.204.137 and port 80 and port 50089 and proto 6)
Receiving raw file from sensor.
Finished.

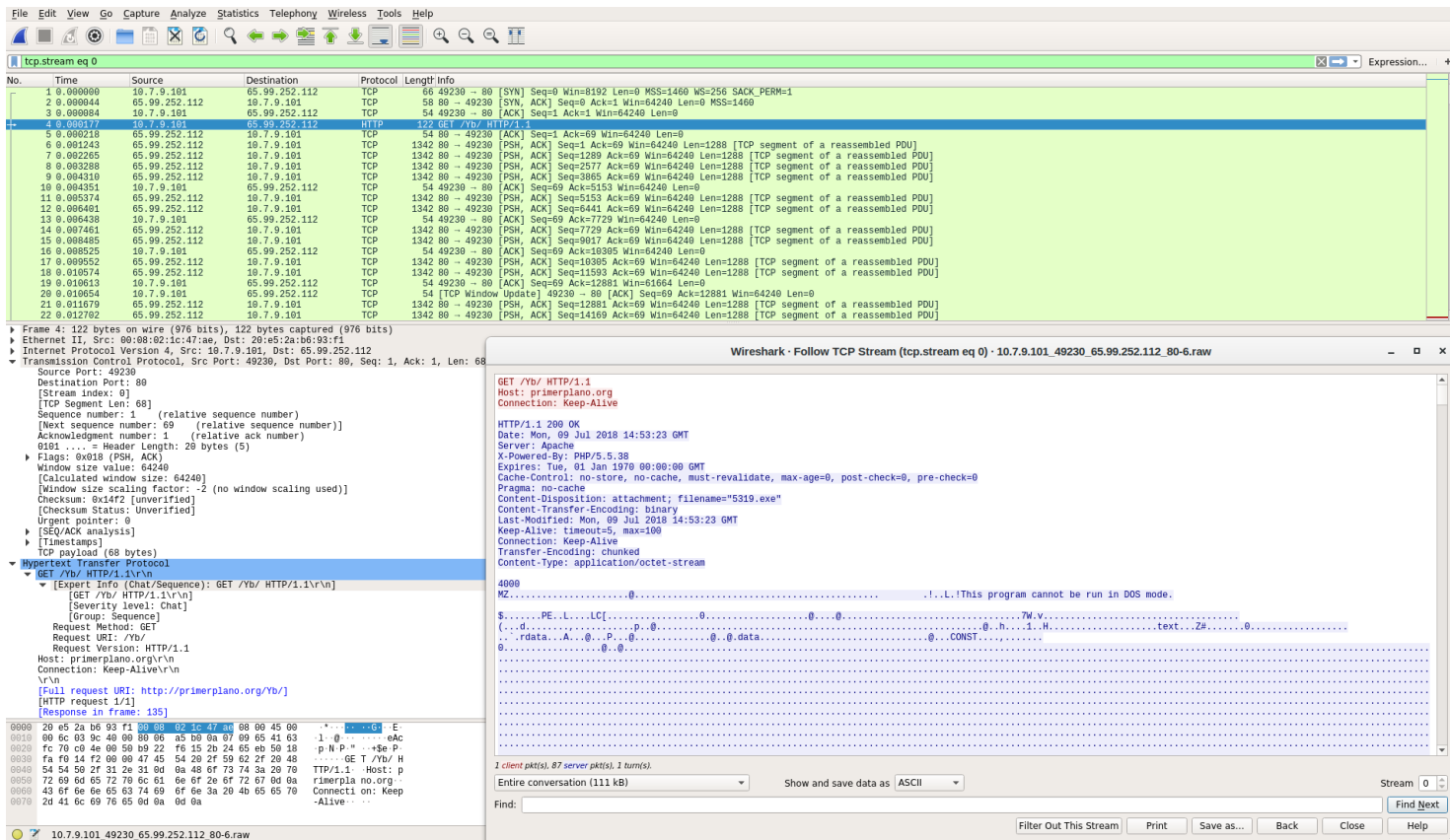
Search Packet Payload Hex Text NoCase

Security Onion Analyst Tools – NetworkMiner

off-line analysis and reassembly of transmitted files from pcap



Analyze network traffic in a network protocol analyzer



Security Onion Deployment Types

Stand Alone

- A self-contained, appliance style solution to collect and present data
- Often used in smaller deployments

Heavy Distributed

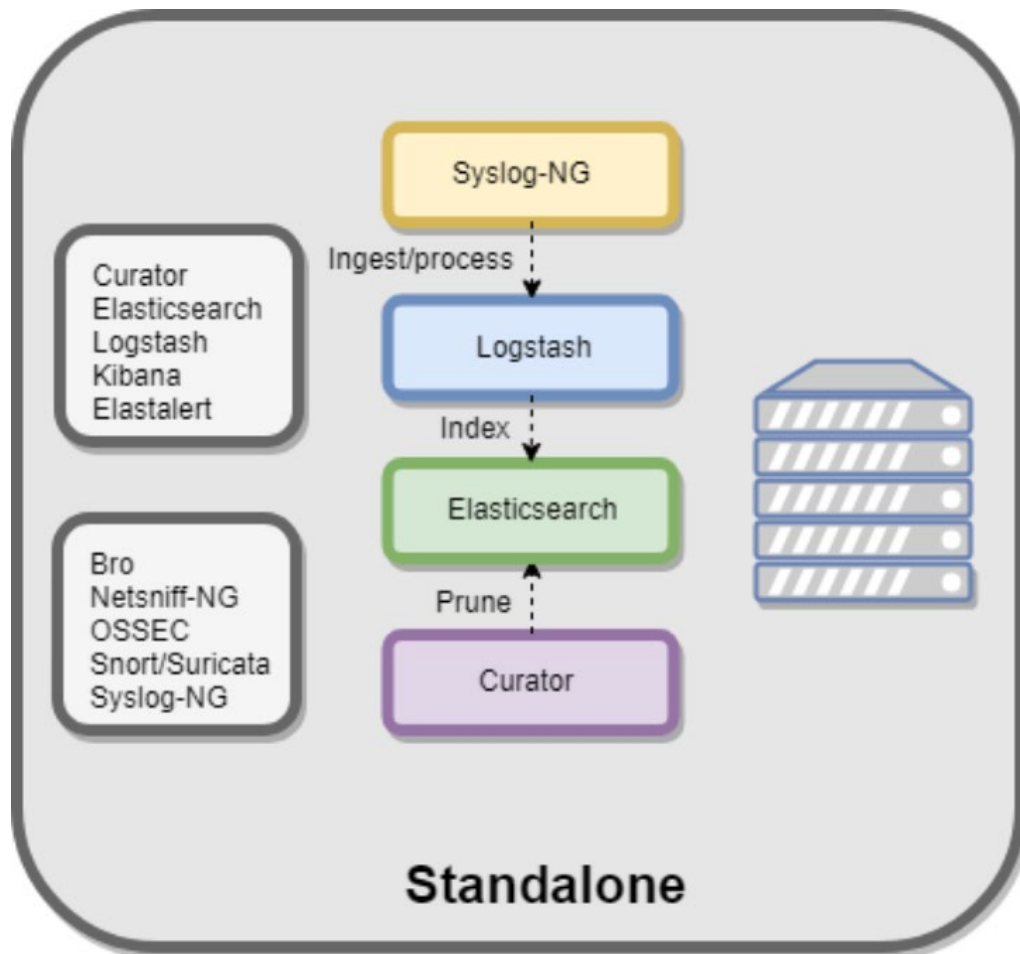
- A distributed platform, with multiple heavy nodes reporting to a master server
- Recommended only when a standard deployment is not possible

Security Onion Deployment Types

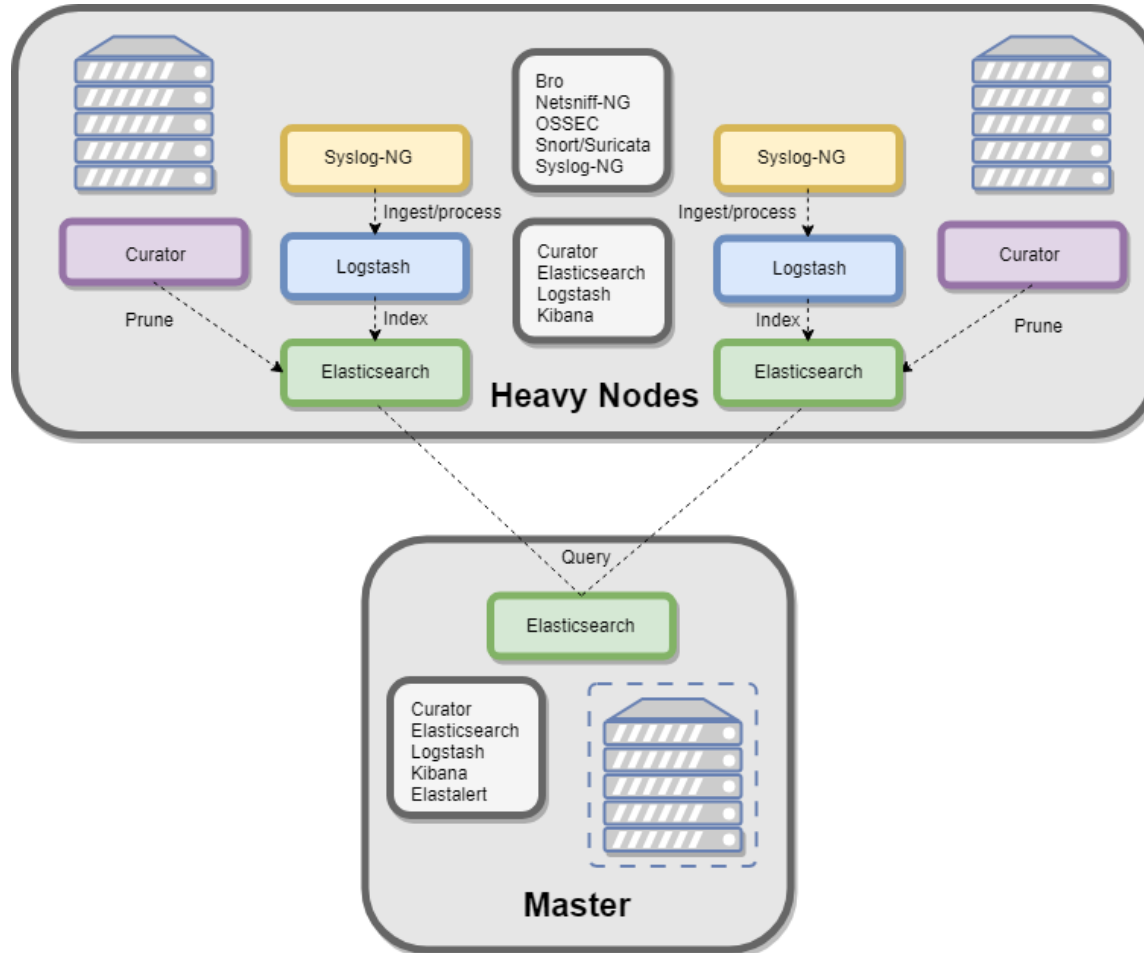
Distributed

- A distributed platform, with forward nodes collecting data, a master server aggregating and presenting the data to analysts, and storage nodes
- Preferred in environments where multiple sensors are required
- Sensors can be deployed globally, as long as they can connect to the central server

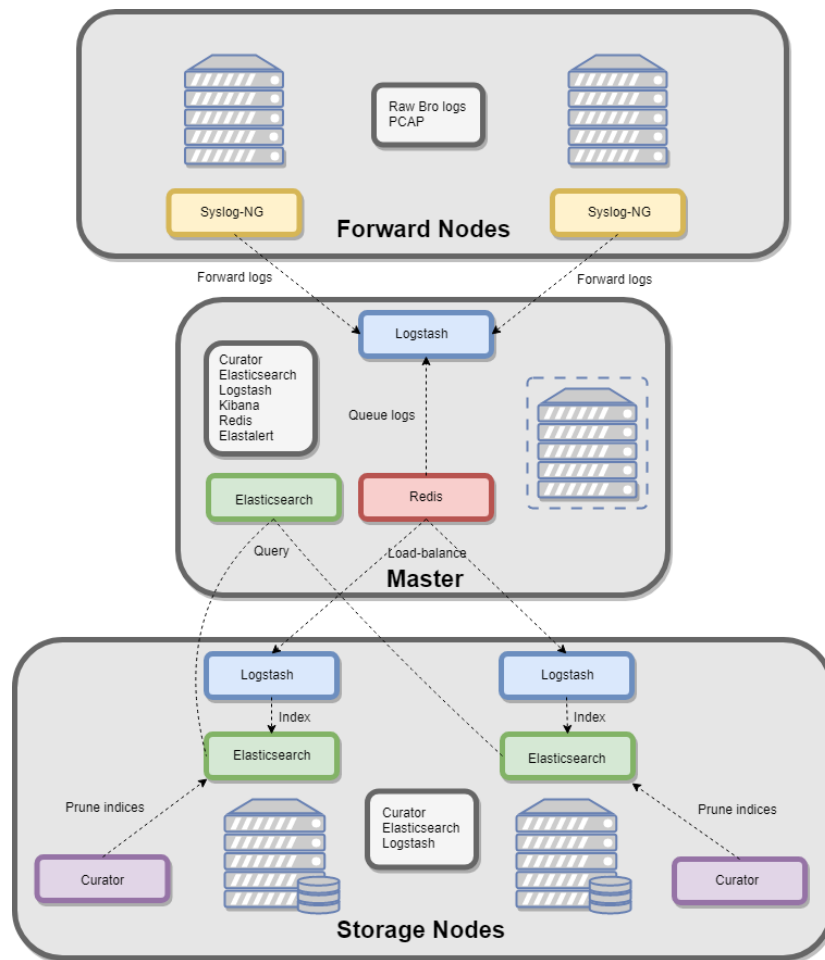
Stand Alone Example



Heavy Distributed Example



Distributed Example



Node Types – Master

- The master runs Elasticsearch, and manages cross-cluster search
- Analysts connect to perform queries and retrieve data
- The Master Node is comprised of:
 - Elasticsearch
 - Logstash
 - Kibana
 - Curator
 - Elastalert
 - Redis (Only if configured to output to a storage node)
 - OSSEC
 - Sguil

Node Types – Forward Node

- Forward nodes capture and forward all logs to the master via an autossh tunnel
- The master stores the forwarded data in Elasticsearch, or forwards the data to the storage nodes (if configured)
- The Forward Node is comprised of:
 - Zeek
 - Snort/Suricata
 - Netsniff-NG
 - OSSEC
 - Syslog-NG

Node Types – Heavy Node

- Heavy Nodes provide distributed deployments with Elasticsearch's cross-cluster search
- The Heavy Node is comprised of:
 - Elasticsearch
 - Logstash
 - Curator
 - Zeek
 - Snort/Suricata
 - Netsniff-NG
 - OSSEC
 - Syslog-NG (forwards logs locally to Logstash)

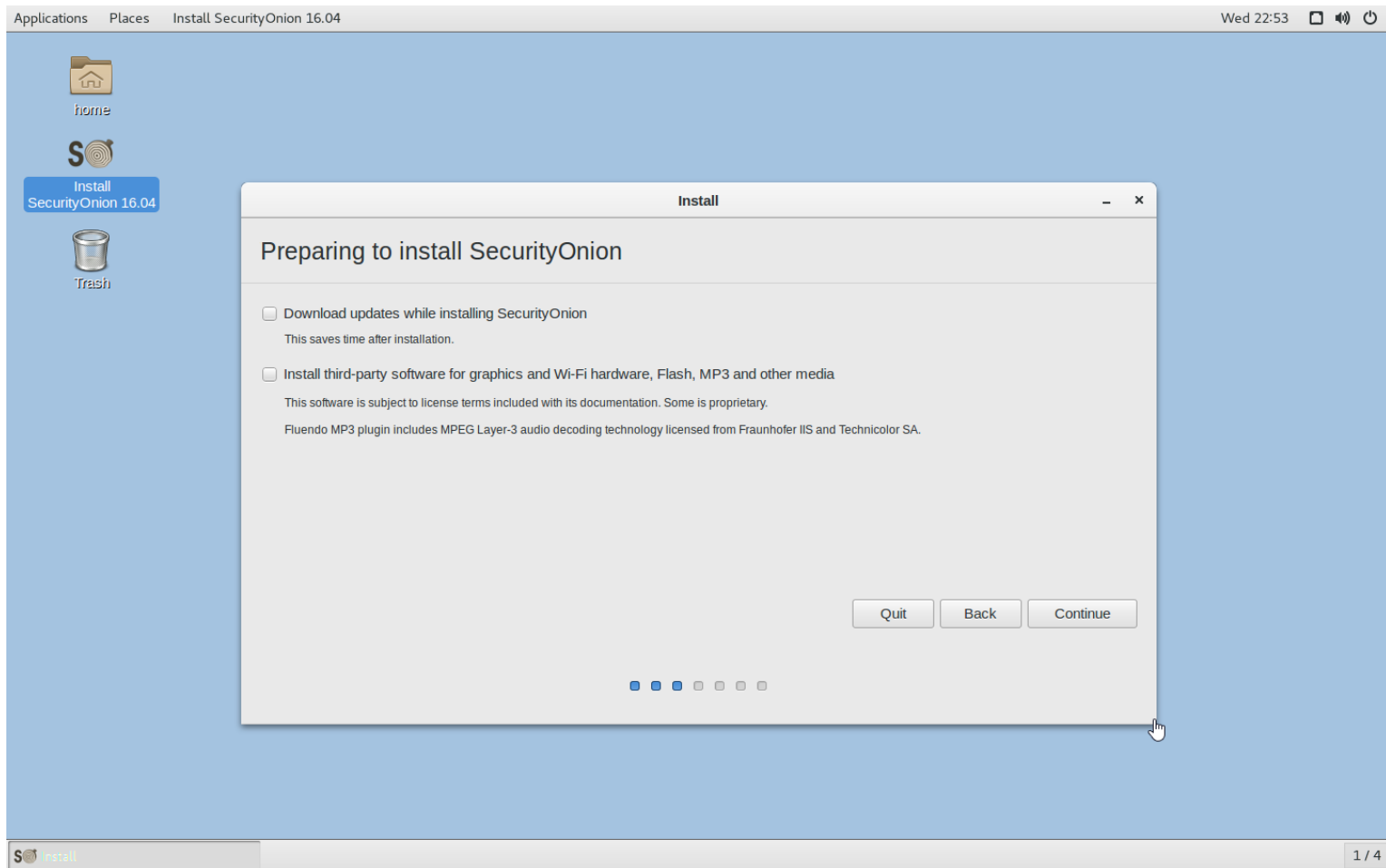
Node Types – Storage Node

- Storage nodes extend the processing and storage capabilities of the master node
- Any data residing on the storage node can be queried by the master via Elasticsearch
- The Heavy Node is comprised of:
 - Elasticsearch
 - Logstash
 - Curator
 - OSSEC

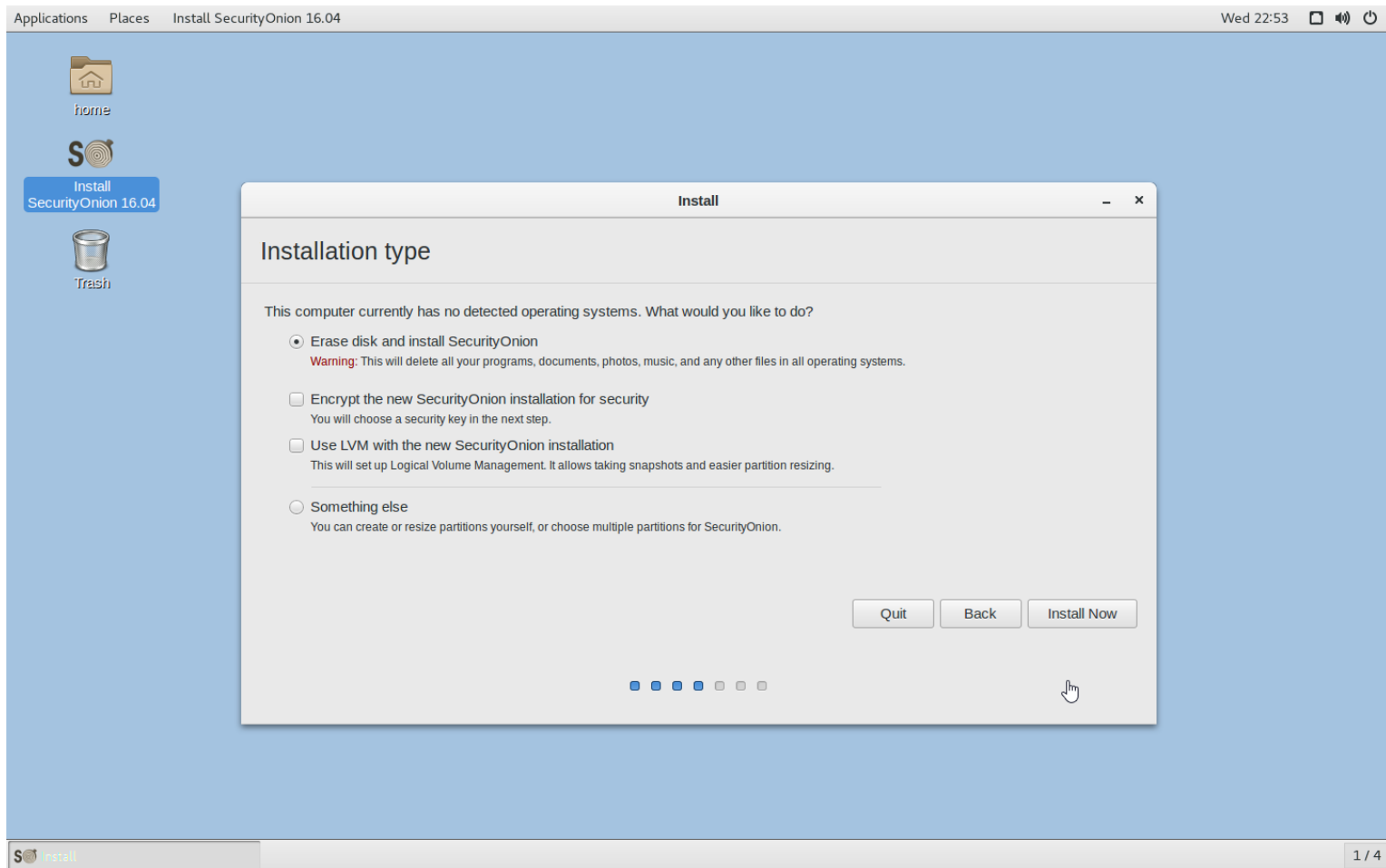
Installing Security Onion

- Security Onion is available as an iso from <https://securityonion.net/>
- Alternatively, SO can be added to an existing Ubuntu 16.04 machine by adding the SO PPA and packages
- The install iso can be used as a live system for troubleshooting installation issues, or installing SO to your hard drive (required for enterprise use)

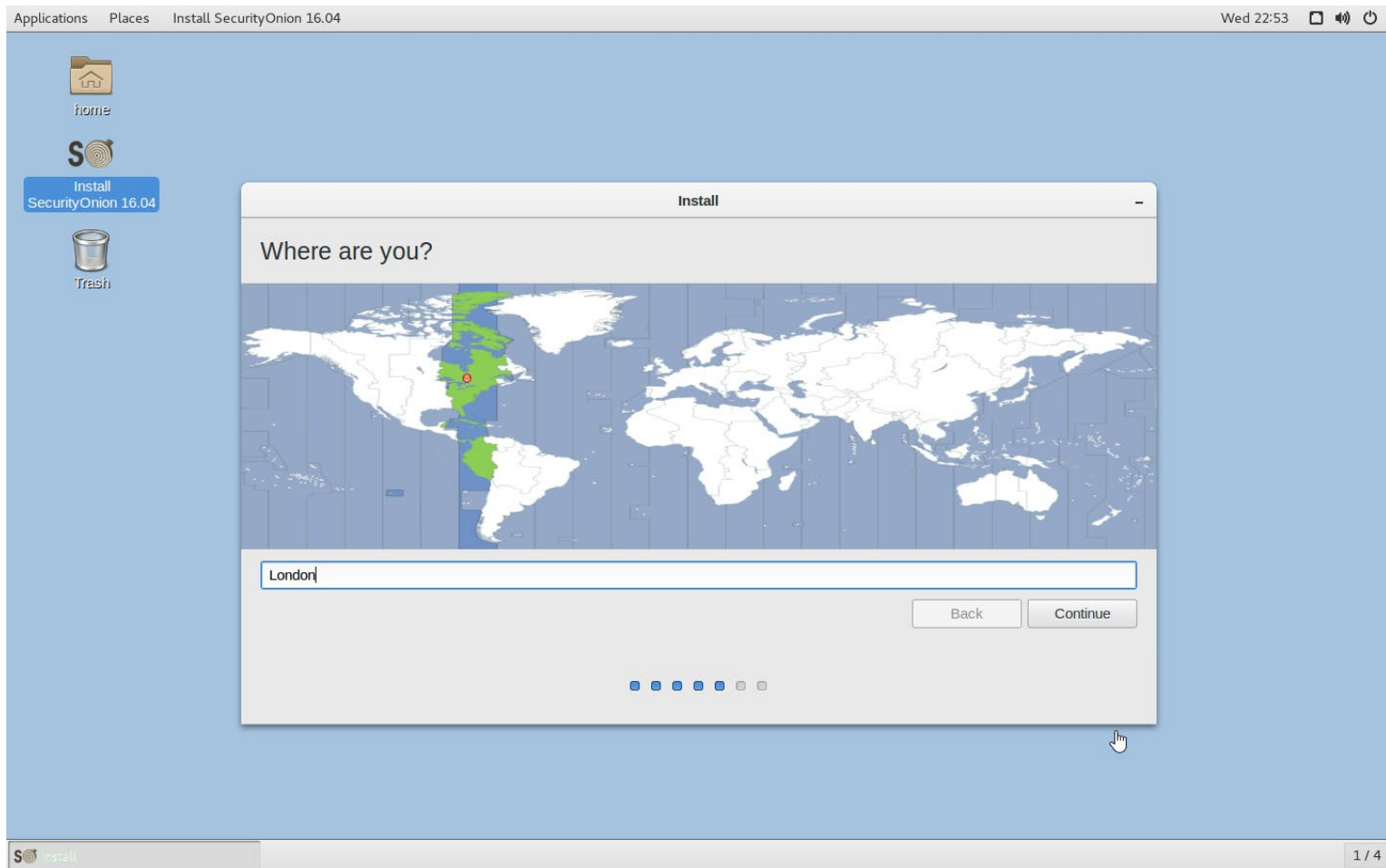
QuickStart – Configuring Security Onion



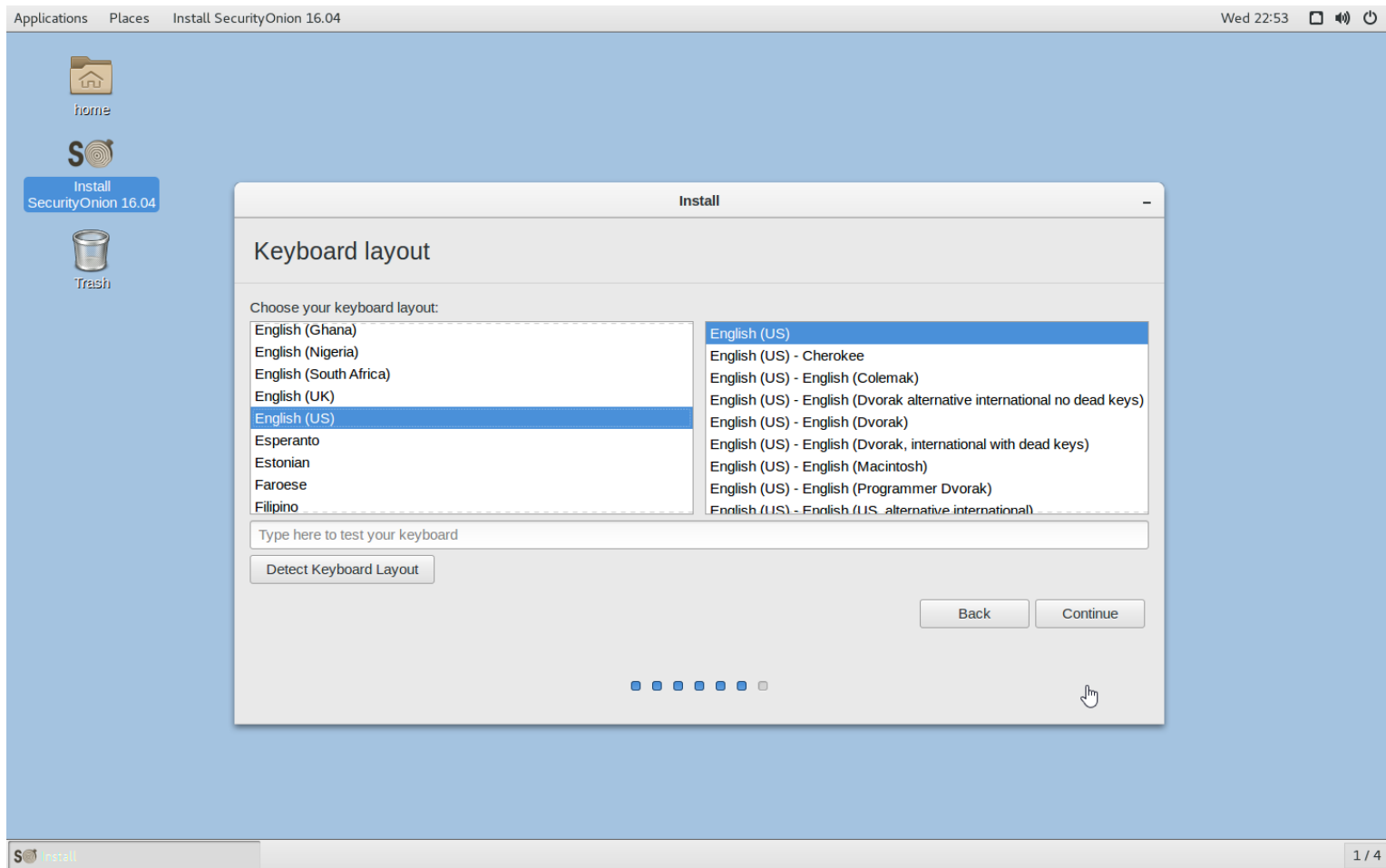
QuickStart – Configuring Security Onion



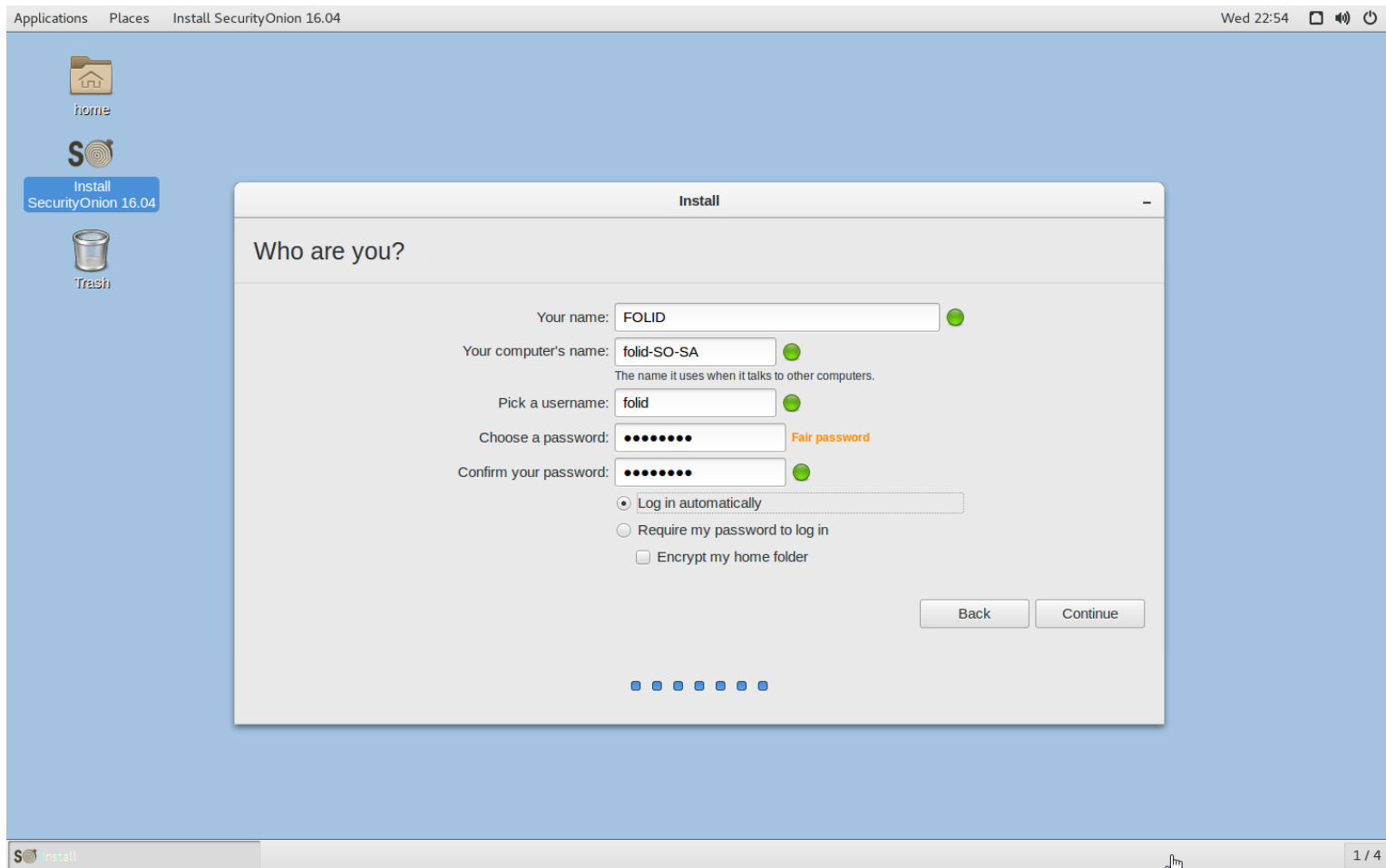
QuickStart – Configuring Security Onion



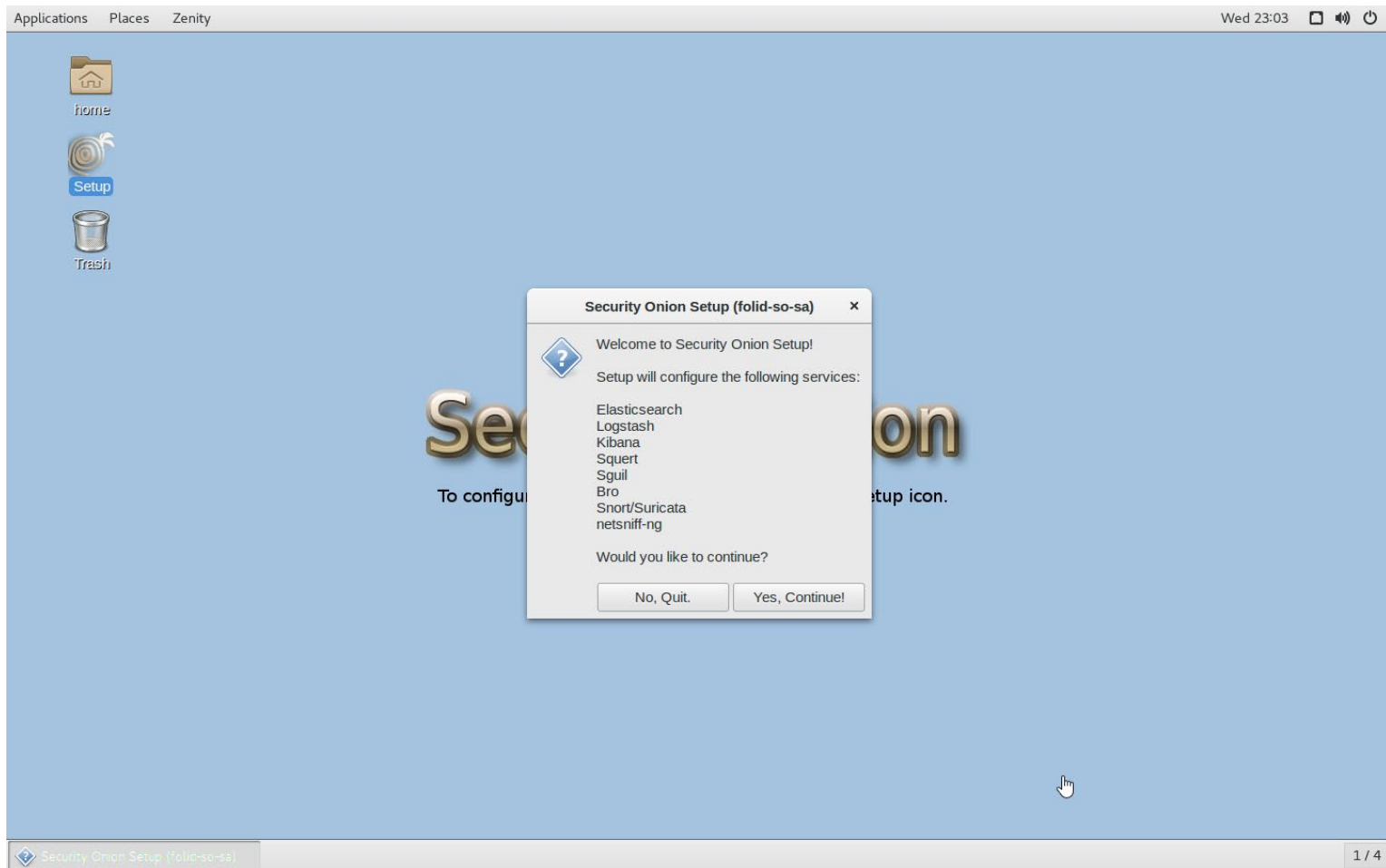
QuickStart – Configuring Security Onion



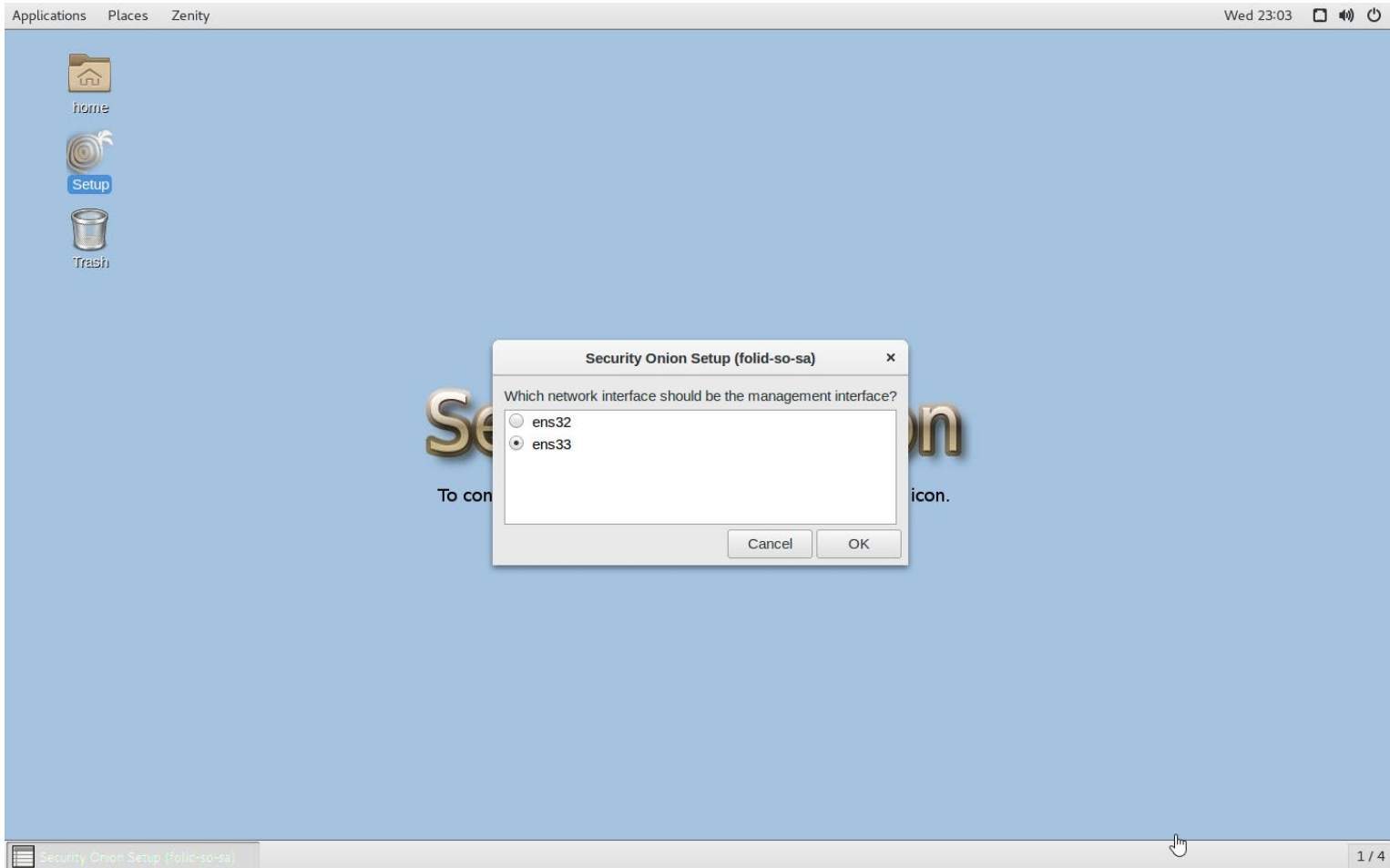
QuickStart – Configuring Security Onion



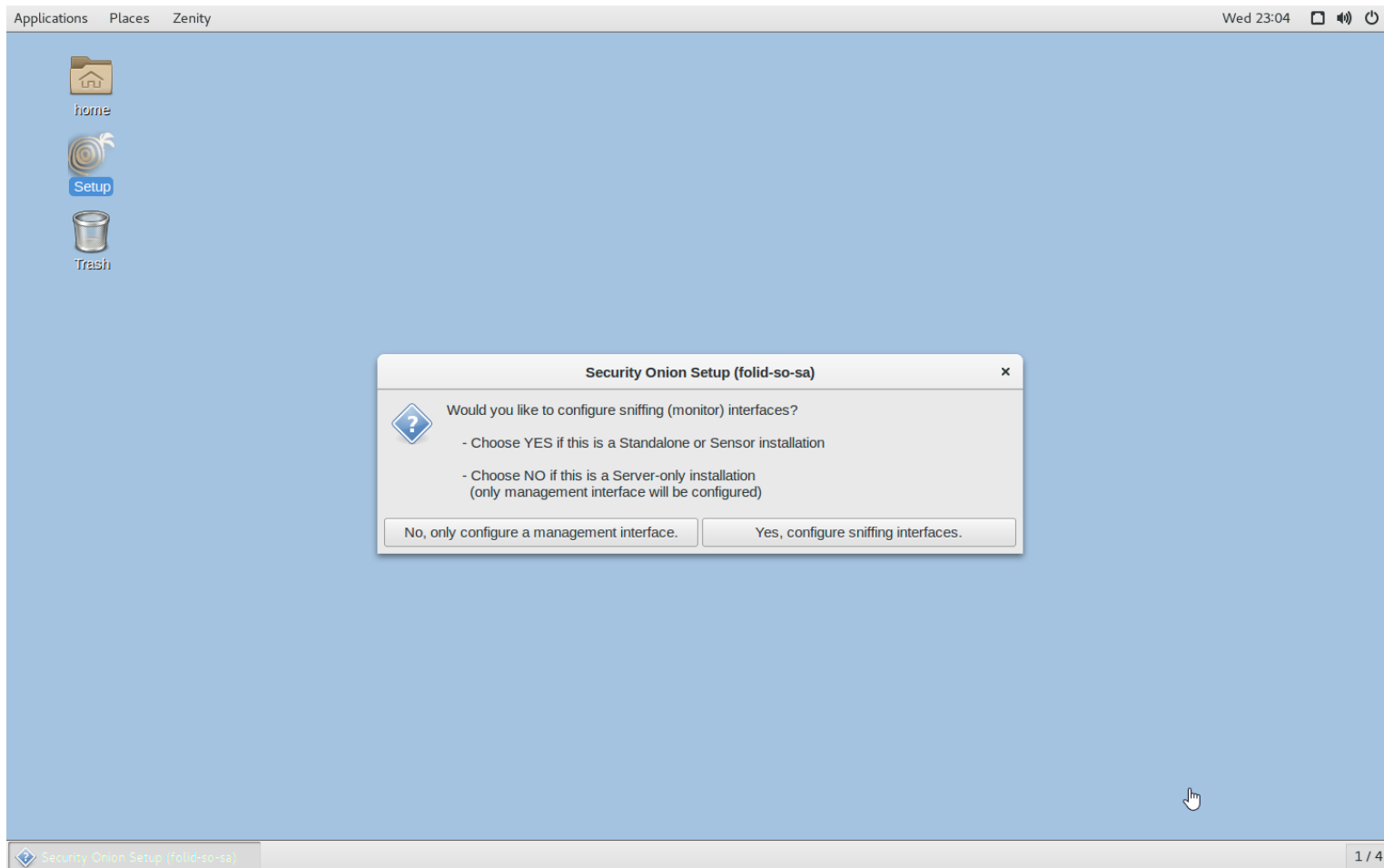
QuickStart – Configuring Security Onion



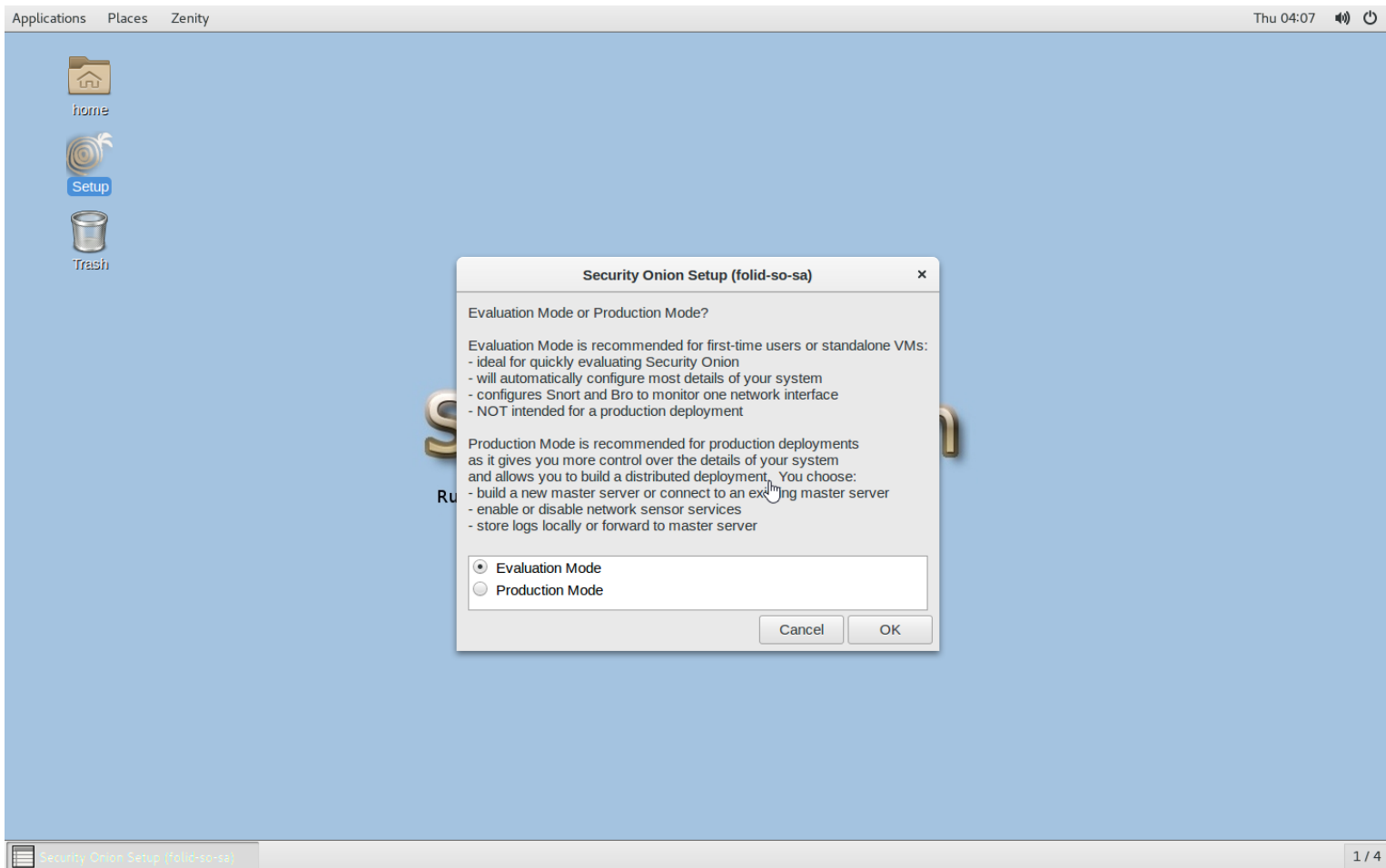
QuickStart – Configuring Security Onion



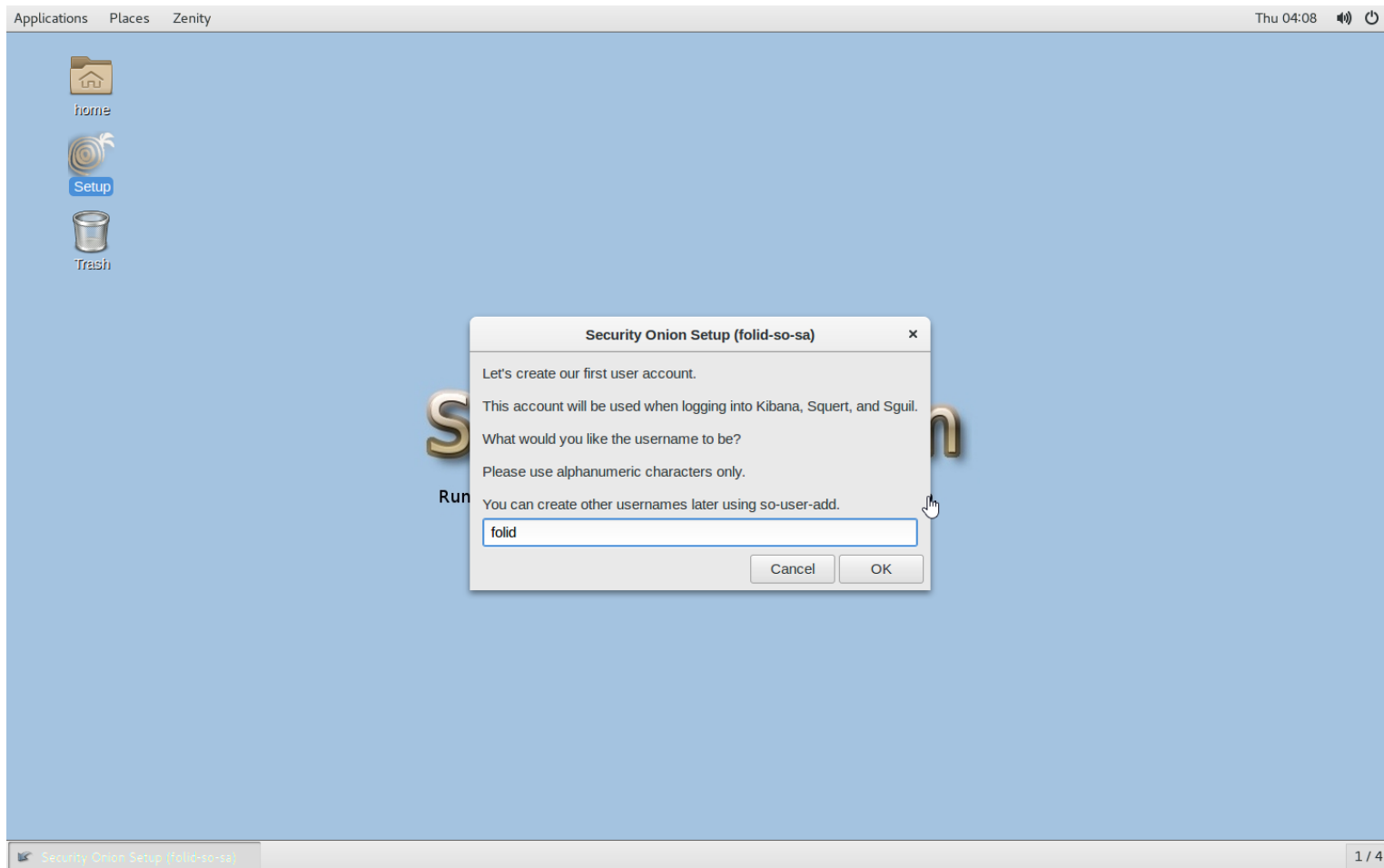
QuickStart – Configuring Security Onion



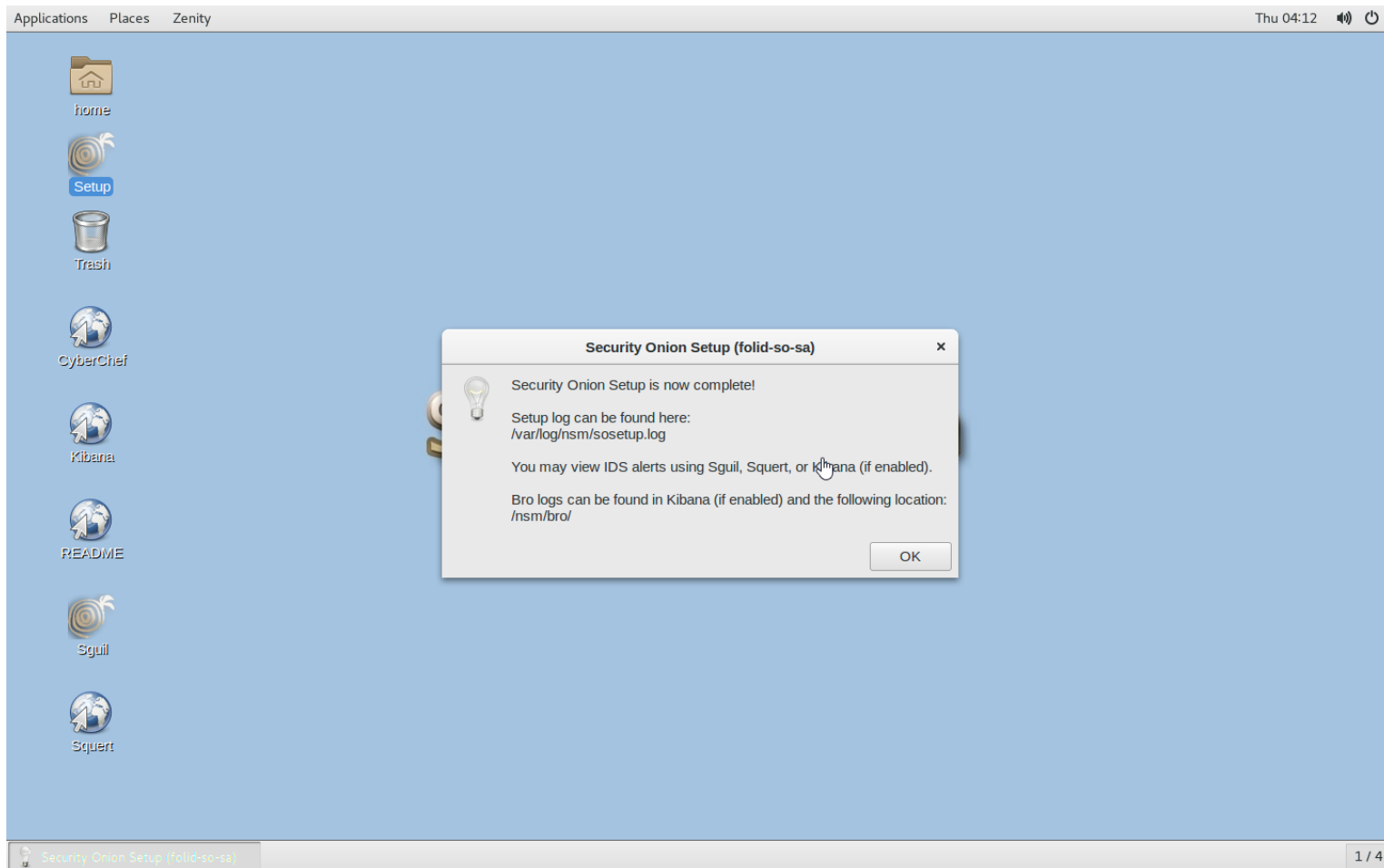
QuickStart – Configuring Security Onion



QuickStart – Configuring Security Onion



QuickStart – Configuring Security Onion



Summary

- Security Onion Core Components include Logstash, Elasticsearch and Kibana
- Analysts connect to tools such as Kibana, CapME, and Squert to analyze network traffic
- SO can be deployed in a number of different configurations, with distributed being the preferred configuration for enterprise environments
- SO node types include, master, forward, storage, heavy and stand-alone
- SO installs similarly to other Linux distributions, with a two-step configuration process required before use

References

- Bejtlich, R. (2013). Chapter 3: Stand-alone NSM Deployment and Installation. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.
- Security Onion Solutions. (2020). Security Onion: Security Onion Documentation. Evans, GA: Author.