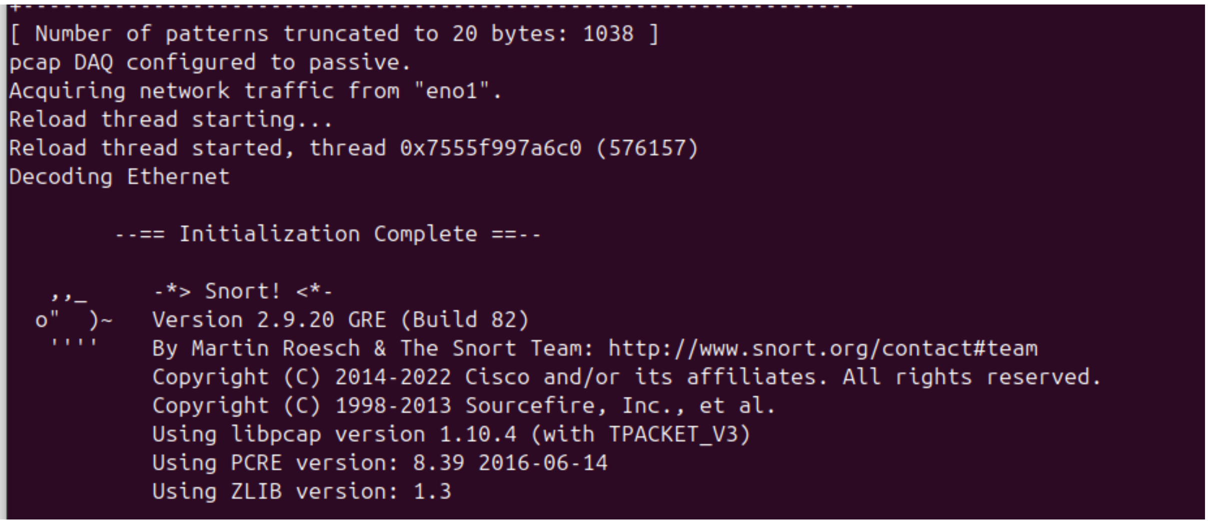
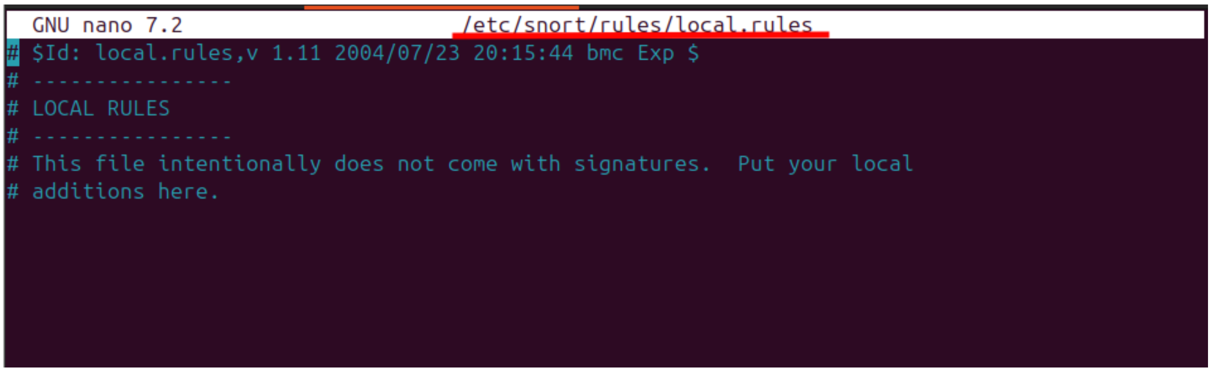
Brandon Gracy 19/12/2025

Our goal in this lab is to deploy snort in the same system running Elastic security, Configure custom detection rules to monitor network activity. Validate alerts by simulating and analyzing network threats. Integrate Snort with Elastic SIEM to centralize security logs.

Let's start to install the Snort.

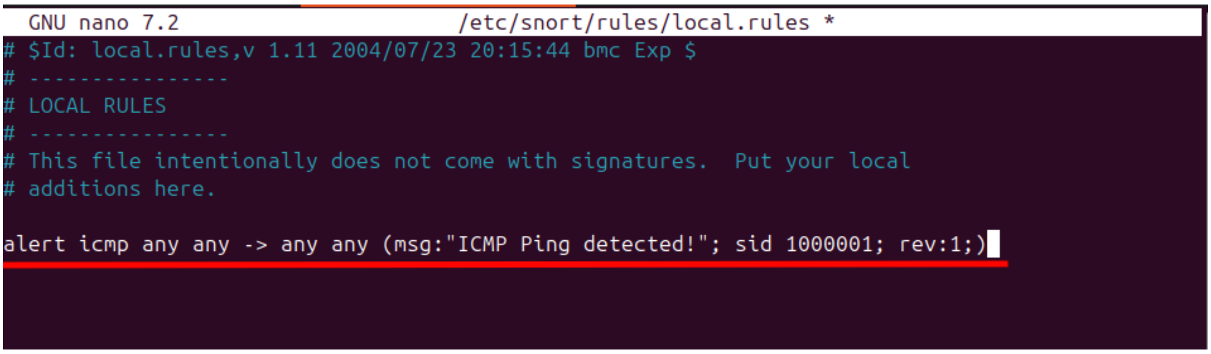


```
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eno1".
Reload thread starting...
Reload thread started, thread 0x7555f997a6c0 (576157)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3
```



```
  GNU nano 7.2                    /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

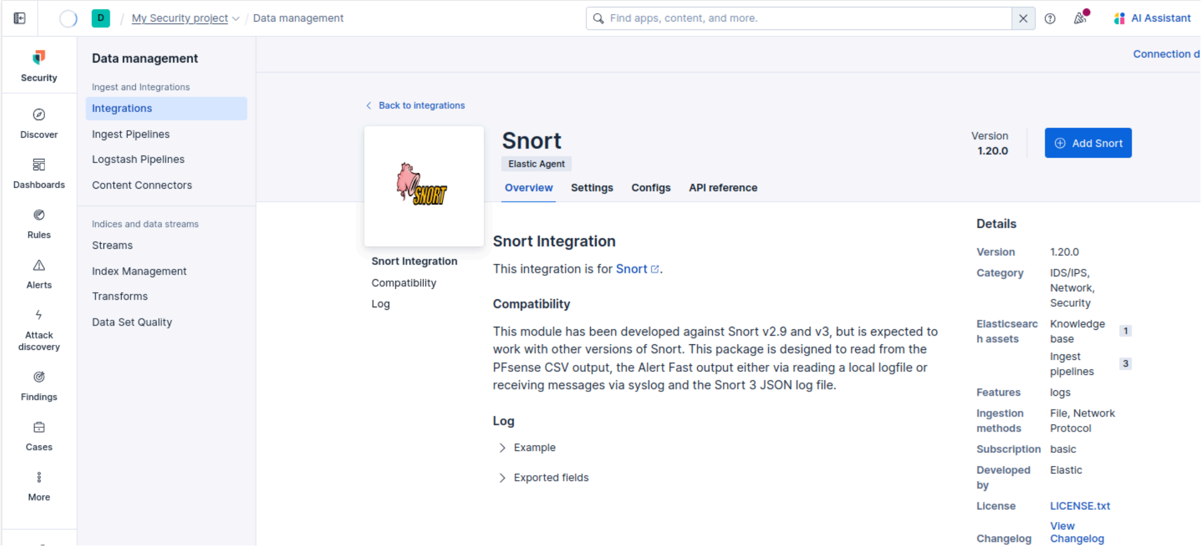
Let's create a new rule here that allow an alert.



```
  GNU nano 7.2                          /etc/snort/rules/local.rules *
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any -> any any (msg:"ICMP Ping detected!"; sid 1000001; rev:1;)
```

Here we have a rule that is an alert with the icmp that when somebody does a ping from any ip to any ip, and the message that will appear when this happens.

Now, we have to implement the snort integration on the elastic SIEM.



Version
1.20.0

Snort Integration

This integration is for Snort.

Compatibility

This module has been developed against Snort v2.9 and v3, but is expected to work with other versions of Snort. This package is designed to read from the PFsense CSV output, the Alert Fast output either via reading a local logfile or receiving messages via syslog and the Snort 3 JSON log file.

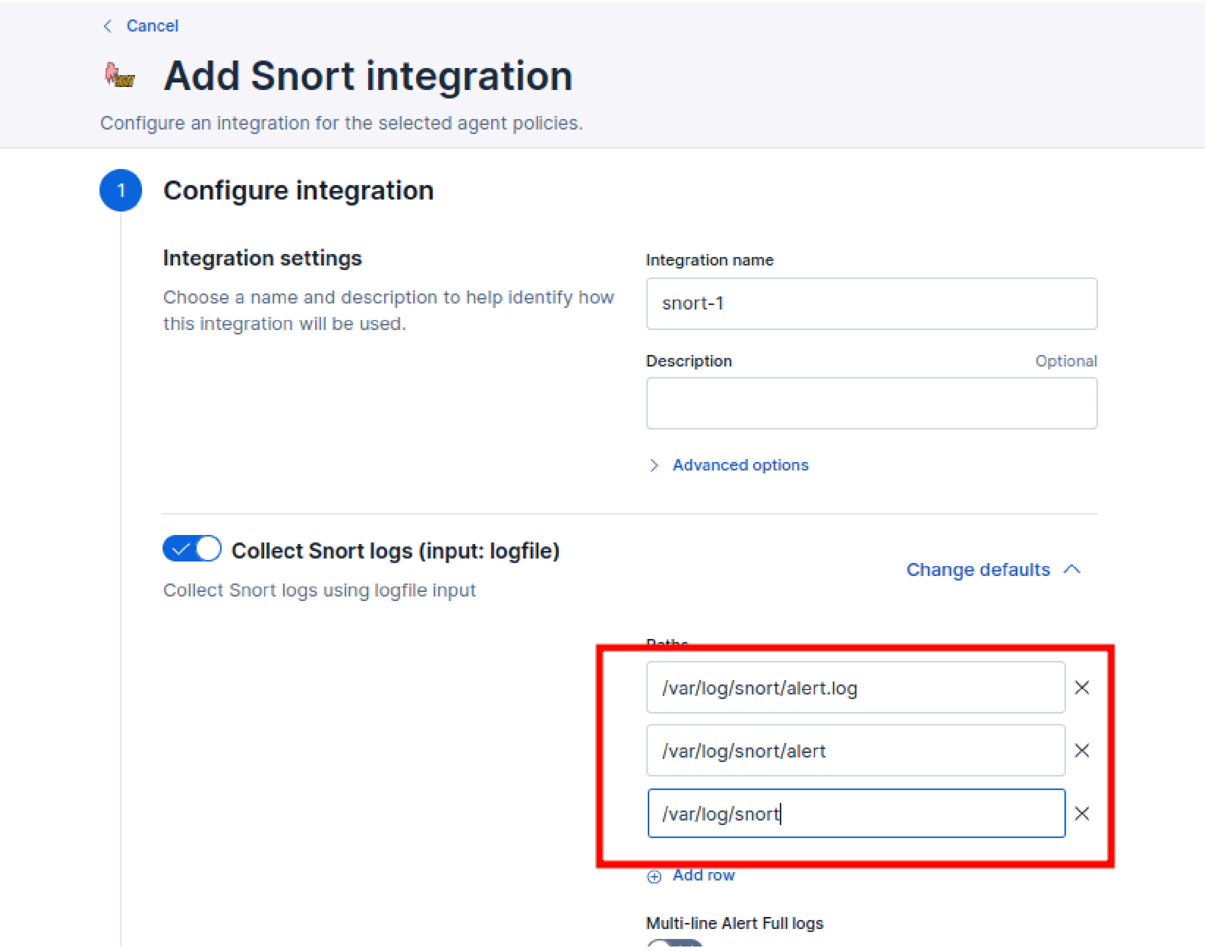
Log

› Example

› Exported fields

Details

Version	1.20.0	
Category	IDS/IPS, Network, Security	
Elasticsearch assets	Knowledge base	1
	Ingest pipelines	3
Features	logs	
Ingestion methods	File, Network Protocol	
Subscription	basic	
Developed by	Elastic	
License	LICENSE.txt	
Changelog	View Changelog	



< Cancel

Add Snort integration

Configure an integration for the selected agent policies.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: snort-1

Description (Optional):

> Advanced options

Collect Snort logs (input: logfile)

Collect Snort logs using logfile input

Change defaults ^

Paths

/var/log/snort/alert.log ×

/var/log/snort/alert ×

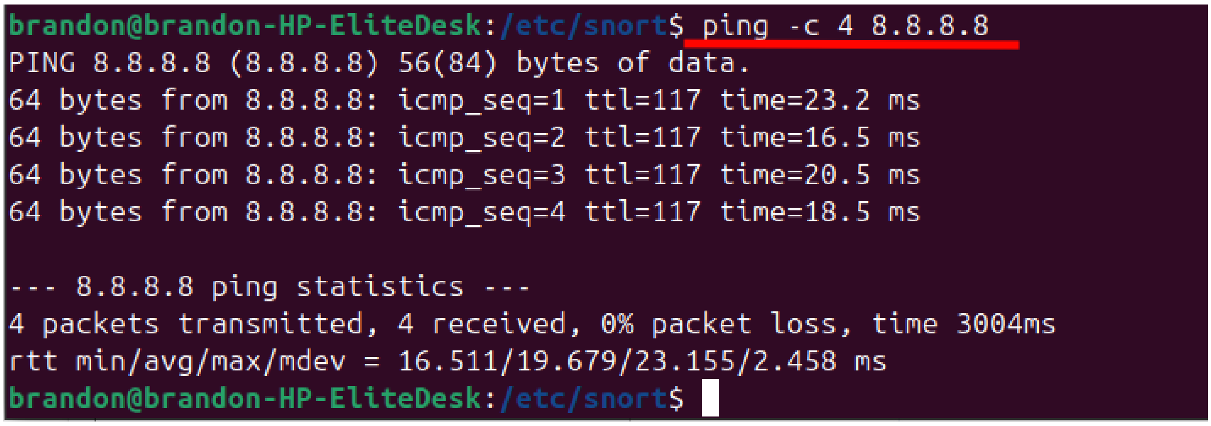
/var/log/snort ×

⊕ Add row

Multi-line Alert Full logs

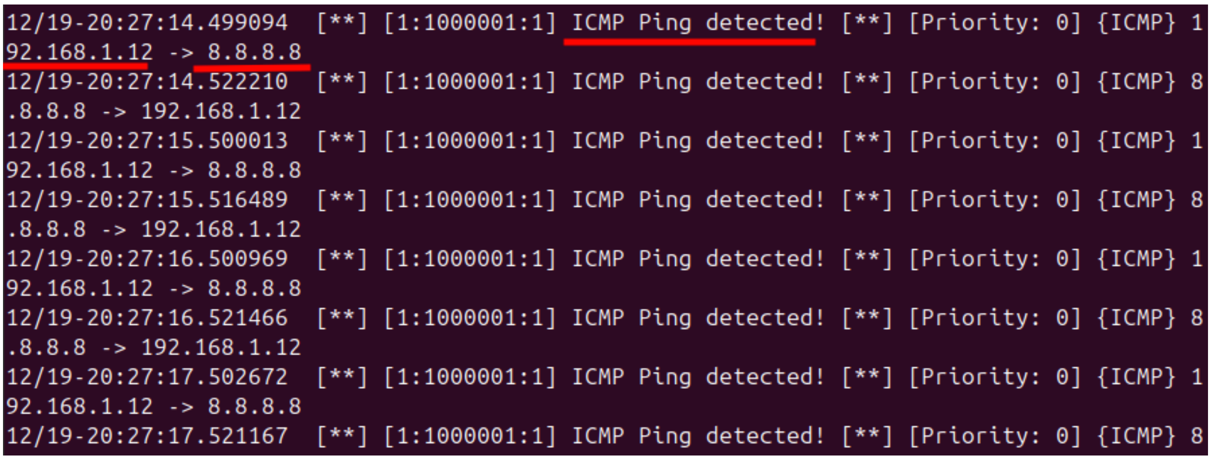
In the Snort Integration settings, configure log collection by adding these three paths.

Now let's see what happened when we did a ping.



```
brandon@brandon-HP-EliteDesk:/etc/snort$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=23.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=20.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=18.5 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 16.511/19.679/23.155/2.458 ms
brandon@brandon-HP-EliteDesk:/etc/snort$ 
```

Here we did a ping to google.



```
12/19-20:27:14.499094  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 1
92.168.1.12 -> 8.8.8.8
12/19-20:27:14.522210  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 8
.8.8.8 -> 192.168.1.12
12/19-20:27:15.500013  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 1
92.168.1.12 -> 8.8.8.8
12/19-20:27:15.516489  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 8
.8.8.8 -> 192.168.1.12
12/19-20:27:16.500969  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 1
92.168.1.12 -> 8.8.8.8
12/19-20:27:16.521466  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 8
.8.8.8 -> 192.168.1.12
12/19-20:27:17.502672  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 1
92.168.1.12 -> 8.8.8.8
12/19-20:27:17.521167  [**] [1:1000001:1] ICMP Ping detected! [**] [Priority: 0] {ICMP} 8
```

Here we can check that snort did alert us, and we can see what happened with the message.