PASSIVE FINGERPRINTING WITH SURICATA

PRESENTED BY:

JEREMY GROVE

WHO AM I

- Security Engineer at Quadrant Information Security
- Quadrant is an MSSP
- Role is to improve to support functions
- Just finished my Masters in Cyber Security and Information Assurance
  - WINK WINK ^^^^^ LOOK HERE!! ^^^^^ WINK WINK

WHAT IS FINGERPRINTING?

- **Fingerprinting** is the use of information to correlate data sets in order to identify **network** services, operating system number and version, software applications, databases, configurations and more.

REASONS TO USE SURICATA

- Other programs
  - Require another tool to watch
  - No control of signatures
  - Depends on developer for updates
- Suricata
  - Integrates with current tool set and workflow
  - Low cost
  - Customizable

WHY FINGERPRINT?

- Greater environmental intelligence
- Improved signal to noise ratio
- Faster research and response
- Confidence in triage decisions

SYSTEM COMPONENTS

- Signatures
- Data Management

SIGNATURE CONTENT

- User Agents
  - Mozilla/5.0 (Linux; Android 9; SM-G965U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.62 Mobile Safari/537.36
- Ports
  - 80 HTTP
  - 445 SMB
- Many more
  - Server Response, Broadcast IP used, etc.

SIGNATURE KEYWORDS

- Located in Metadata
- Fingerprint_os
  - Free form for any OS
- Fingerprint_type
  - Server or Client
- Fingerprint_expire
  - Set to timeframe in seconds

EXAMPLE SIGNATURE

```
alert http $HOME_NET any -> any any (msg:"Samsung Galaxy S10"; flow:established,to_server; content:"User-Agent|3a| "; nocase; http_header; content:"SM-G973"; nocase; threshold: type limit, track by_src, seconds 3600, count 1; target: src_ip; metadata: fingerprint_os android, fingerprint_type client, fingerprint_expire 86400; classtype:fingerprint; sid:xxxxxxxxx; rev:1;)
```

DHCP

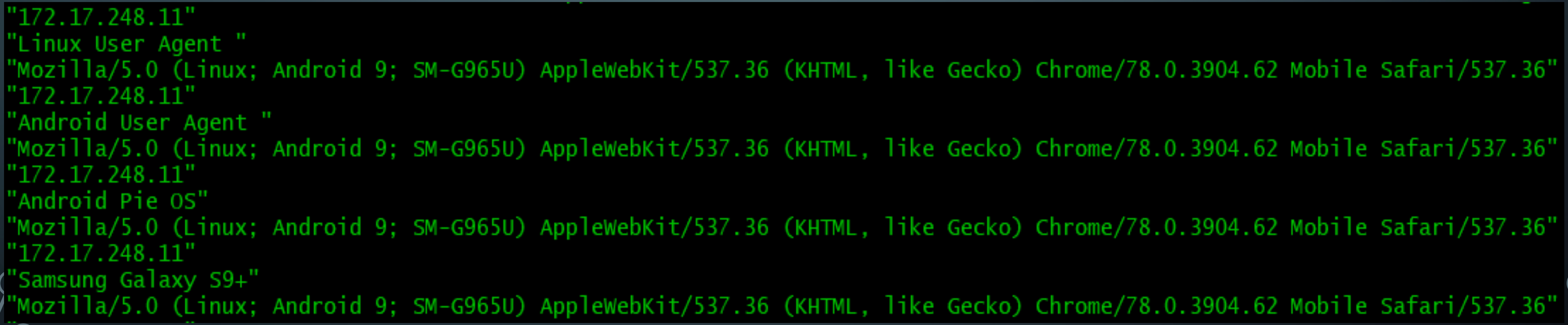
- Provides MAC address
  - Allows you tie the IP to a specific device
- Moved into the alert file for ingestion
  - Allows you keep a historical record of the MAC to IP relationship

DATA MANAGEMENT

- Process Flow
- Redis
- Elasticsearch

PROCESS FLOW

- Fingerprint alert created

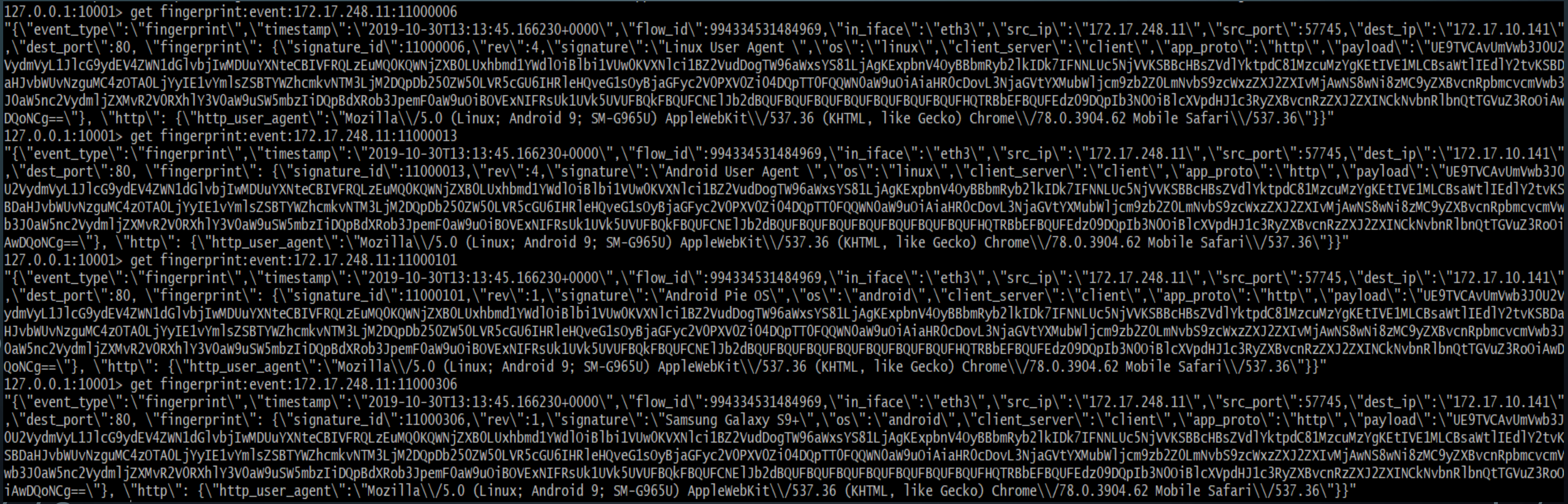


```
"172.17.248.11"
"Linux User Agent "
"Mozilla/5.0 (Linux; Android 9; SM-G965U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.62 Mobile Safari/537.36"
"172.17.248.11"
"Android User Agent "
"Mozilla/5.0 (Linux; Android 9; SM-G965U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.62 Mobile Safari/537.36"
"172.17.248.11"
"Android Pie OS"
"Mozilla/5.0 (Linux; Android 9; SM-G965U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.62 Mobile Safari/537.36"
"172.17.248.11"
"Samsung Galaxy S9+"
"Mozilla/5.0 (Linux; Android 9; SM-G965U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.62 Mobile Safari/537.36"
```

PROCESS FLOW CONT.

- Data inserted into Redis
  - fingerprint:event:172.17.248.11:11000006
  - fingerprint:event:172.17.248.11:11000013
  - fingerprint:event:172.17.248.11:11000101
  - fingerprint:event:172.17.248.11:11000306

PROCESS FLOW CONT.



```
127.0.0.1:10001> get fingerprint:event:172.17.248.11:11000006
"{\"event_type\":\"fingerprint\",\"timestamp\":\"2019-10-30T13:13:45.166230+0000\",\"flow_id\":994334531484969,\"in_iface\":\"eth3\",\"src_ip\":\"172.17.248.11\",\"src_port\":57745,\"dest_ip\":\"172.17.10.141\"
,\"dest_port\":80, \"fingerprint\": {\"signature_id\":11000006,\"rev\":4,\"signature\":\"Linux User Agent \",\"os\":\"linux\",\"client_server\":\"client\",\"app_proto\":\"http\",\"payload\":\"UE9TVCAvUmVwb3J0U2
VydmVyL1JlcG9ydEV4ZWN1dGlvbjIwMDUuYXNteCBIVFRQLzEuMQ0KQWNjZXB0LUxhbmd1YWdlOiBlbi1VUw0KVXNlci1BZ2VudDogTW96aWxsYS81LjAgKExpbnV4OyBBbmRyb2lkIDk7IFNNLUc5NjVVKSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvKSBD
aHJvbWUvNzguMC4zOTA0LjYyIE1vYmlsZSBTYWZhcmkvNTM3LjM2DQpDb250ZW50LVR5cGU6IHRleHQveG1sOyBjaGFyc2V0PXV0Zi04DQpTT0FQQWN0aW9uOiAiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS9zcWxzZXJ2ZXIvMjAwNS8wNi8zMC9yZXBvcnRpbmcvcmVwb3
J0aW5nc2VydmljZXMvR2V0RXhlY3V0aW9uSW5mbzIiDQpBdXRob3JpemF0aW9uOiBOVExNIFRsUk1UVk5UVUFBQkFBQUFCNElJb2dBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFHQTRBbEFBQUFEdz09DQpIb3N0OiBlcXVpdHJ1c3RyZXBvcnRzZXJ2ZXINCkNvbnRlbnQtTGVuZ3RoOiAw
DQoNCg==\"}, \"http\": {\"http_user_agent\":\"Mozilla\\/5.0 (Linux; Android 9; SM-G965U) AppleWebKit\\/537.36 (KHTML, like Gecko) Chrome\\/78.0.3904.62 Mobile Safari\\/537.36\"}}"
127.0.0.1:10001> get fingerprint:event:172.17.248.11:11000013
"{\"event_type\":\"fingerprint\",\"timestamp\":\"2019-10-30T13:13:45.166230+0000\",\"flow_id\":994334531484969,\"in_iface\":\"eth3\",\"src_ip\":\"172.17.248.11\",\"src_port\":57745,\"dest_ip\":\"172.17.10.141\"
,\"dest_port\":80, \"fingerprint\": {\"signature_id\":11000013,\"rev\":4,\"signature\":\"Android User Agent \",\"os\":\"linux\",\"client_server\":\"client\",\"app_proto\":\"http\",\"payload\":\"UE9TVCAvUmVwb3J0
U2VydmVyL1JlcG9ydEV4ZWN1dGlvbjIwMDUuYXNteCBIVFRQLzEuMQ0KQWNjZXB0LUxhbmd1YWdlOiBlbi1VUw0KVXNlci1BZ2VudDogTW96aWxsYS81LjAgKExpbnV4OyBBbmRyb2lkIDk7IFNNLUc5NjVVKSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvKS
BDaHJvbWUvNzguMC4zOTA0LjYyIE1vYmlsZSBTYWZhcmkvNTM3LjM2DQpDb250ZW50LVR5cGU6IHRleHQveG1sOyBjaGFyc2V0PXV0Zi04DQpTT0FQQWN0aW9uOiAiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS9zcWxzZXJ2ZXIvMjAwNS8wNi8zMC9yZXBvcnRpbmcvcmVw
b3J0aW5nc2VydmljZXMvR2V0RXhlY3V0aW9uSW5mbzIiDQpBdXRob3JpemF0aW9uOiBOVExNIFRsUk1UVk5UVUFBQkFBQUFCNElJb2dBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFHQTRBbEFBQUFEdz09DQpIb3N0OiBlcXVpdHJ1c3RyZXBvcnRzZXJ2ZXINCkNvbnRlbnQtTGVuZ3RoOi
AwDQoNCg==\"}, \"http\": {\"http_user_agent\":\"Mozilla\\/5.0 (Linux; Android 9; SM-G965U) AppleWebKit\\/537.36 (KHTML, like Gecko) Chrome\\/78.0.3904.62 Mobile Safari\\/537.36\"}}"
127.0.0.1:10001> get fingerprint:event:172.17.248.11:11000101
"{\"event_type\":\"fingerprint\",\"timestamp\":\"2019-10-30T13:13:45.166230+0000\",\"flow_id\":994334531484969,\"in_iface\":\"eth3\",\"src_ip\":\"172.17.248.11\",\"src_port\":57745,\"dest_ip\":\"172.17.10.141\"
,\"dest_port\":80, \"fingerprint\": {\"signature_id\":11000101,\"rev\":1,\"signature\":\"Android Pie OS\",\"os\":\"android\",\"client_server\":\"client\",\"app_proto\":\"http\",\"payload\":\"UE9TVCAvUmVwb3J0U2V
ydmVyL1JlcG9ydEV4ZWN1dGlvbjIwMDUuYXNteCBIVFRQLzEuMQ0KQWNjZXB0LUxhbmd1YWdlOiBlbi1VUw0KVXNlci1BZ2VudDogTW96aWxsYS81LjAgKExpbnV4OyBBbmRyb2lkIDk7IFNNLUc5NjVVKSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvKSBDa
HJvbWUvNzguMC4zOTA0LjYyIE1vYmlsZSBTYWZhcmkvNTM3LjM2DQpDb250ZW50LVR5cGU6IHRleHQveG1sOyBjaGFyc2V0PXV0Zi04DQpTT0FQQWN0aW9uOiAiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS9zcWxzZXJ2ZXIvMjAwNS8wNi8zMC9yZXBvcnRpbmcvcmVwb3J
0aW5nc2VydmljZXMvR2V0RXhlY3V0aW9uSW5mbzIiDQpBdXRob3JpemF0aW9uOiBOVExNIFRsUk1UVk5UVUFBQkFBQUFCNElJb2dBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFHQTRBbEFBQUFEdz09DQpIb3N0OiBlcXVpdHJ1c3RyZXBvcnRzZXJ2ZXINCkNvbnRlbnQtTGVuZ3RoOiAwD
QoNCg==\"}, \"http\": {\"http_user_agent\":\"Mozilla\\/5.0 (Linux; Android 9; SM-G965U) AppleWebKit\\/537.36 (KHTML, like Gecko) Chrome\\/78.0.3904.62 Mobile Safari\\/537.36\"}}"
127.0.0.1:10001> get fingerprint:event:172.17.248.11:11000306
"{\"event_type\":\"fingerprint\",\"timestamp\":\"2019-10-30T13:13:45.166230+0000\",\"flow_id\":994334531484969,\"in_iface\":\"eth3\",\"src_ip\":\"172.17.248.11\",\"src_port\":57745,\"dest_ip\":\"172.17.10.141\"
,\"dest_port\":80, \"fingerprint\": {\"signature_id\":11000306,\"rev\":1,\"signature\":\"Samsung Galaxy S9+\",\"os\":\"android\",\"client_server\":\"client\",\"app_proto\":\"http\",\"payload\":\"UE9TVCAvUmVwb3J
0U2VydmVyL1JlcG9ydEV4ZWN1dGlvbjIwMDUuYXNteCBIVFRQLzEuMQ0KQWNjZXB0LUxhbmd1YWdlOiBlbi1VUw0KVXNlci1BZ2VudDogTW96aWxsYS81LjAgKExpbnV4OyBBbmRyb2lkIDk7IFNNLUc5NjVVKSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvK
SBDaHJvbWUvNzguMC4zOTA0LjYyIE1vYmlsZSBTYWZhcmkvNTM3LjM2DQpDb250ZW50LVR5cGU6IHRleHQveG1sOyBjaGFyc2V0PXV0Zi04DQpTT0FQQWN0aW9uOiAiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS9zcWxzZXJ2ZXIvMjAwNS8wNi8zMC9yZXBvcnRpbmcvcmV
wb3J0aW5nc2VydmljZXMvR2V0RXhlY3V0aW9uSW5mbzIiDQpBdXRob3JpemF0aW9uOiBOVExNIFRsUk1UVk5UVUFBQkFBQUFCNElJb2dBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFHQTRBbEFBQUFEdz09DQpIb3N0OiBlcXVpdHJ1c3RyZXBvcnRzZXJ2ZXINCkNvbnRlbnQtTGVuZ3RoO
iAwDQoNCg==\"}, \"http\": {\"http_user_agent\":\"Mozilla\\/5.0 (Linux; Android 9; SM-G965U) AppleWebKit\\/537.36 (KHTML, like Gecko) Chrome\\/78.0.3904.62 Mobile Safari\\/537.36\"}}"
```

PROCESS FLOW CONT.

- Actual alert from generated from Suricata
- Meer checks Redis for relevant data
- Meer submits alert and fingerprint results to SQL
- SOC Console displays both alert and fingerprints for the analyst
- SOC intelligence increased and research time decreased
- YAY!!

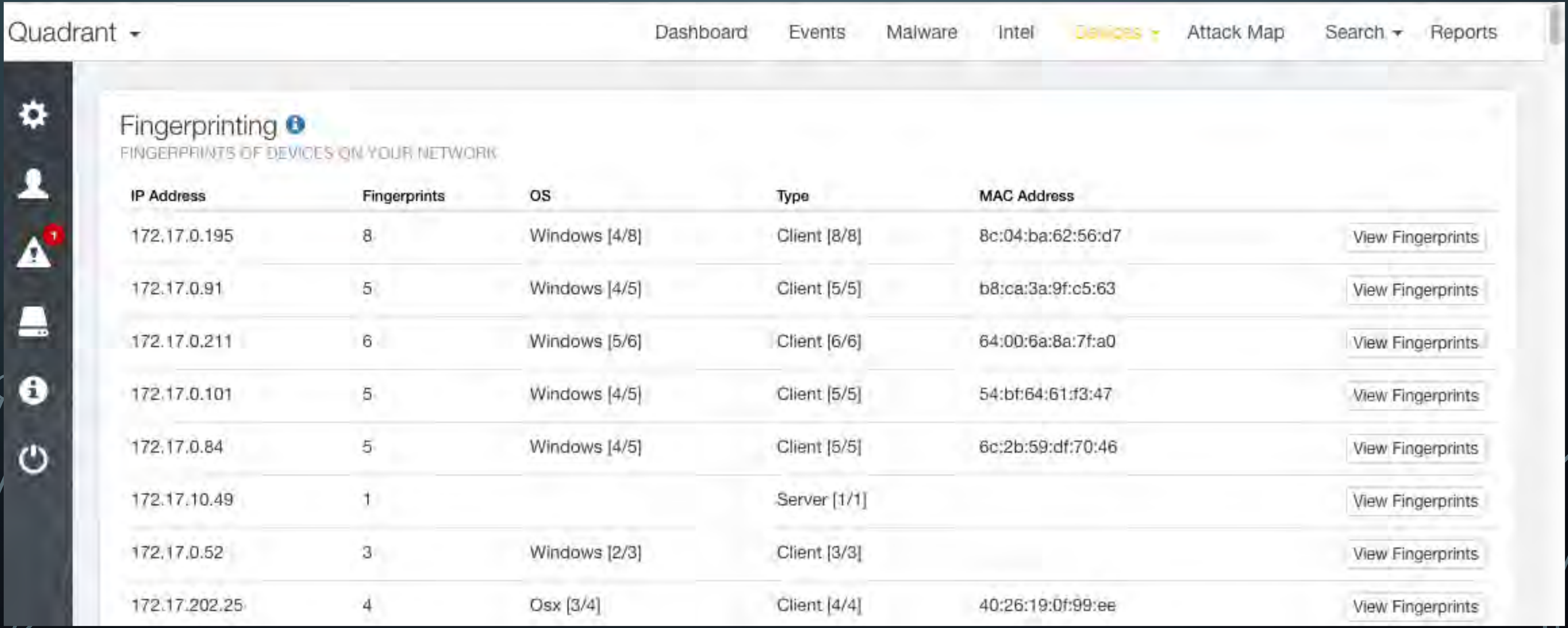
REDIS

- Why Redis?
  - Data handling is more dynamic
  - Originally put everything in MySQL
- Rule Keywords
  - metadata: fingerprint_os android, fingerprint_type client, fingerprint_expire 86400;
  - classtype:fingerprint;

ELASTICSEARCH

- Meer outputs to eve json file
- Includes fingerprint alert and DHCP
- Used for long term storage
  - Important when DHCP is considered
  - Allows for historical lookups

CONSOLE OUTPUT

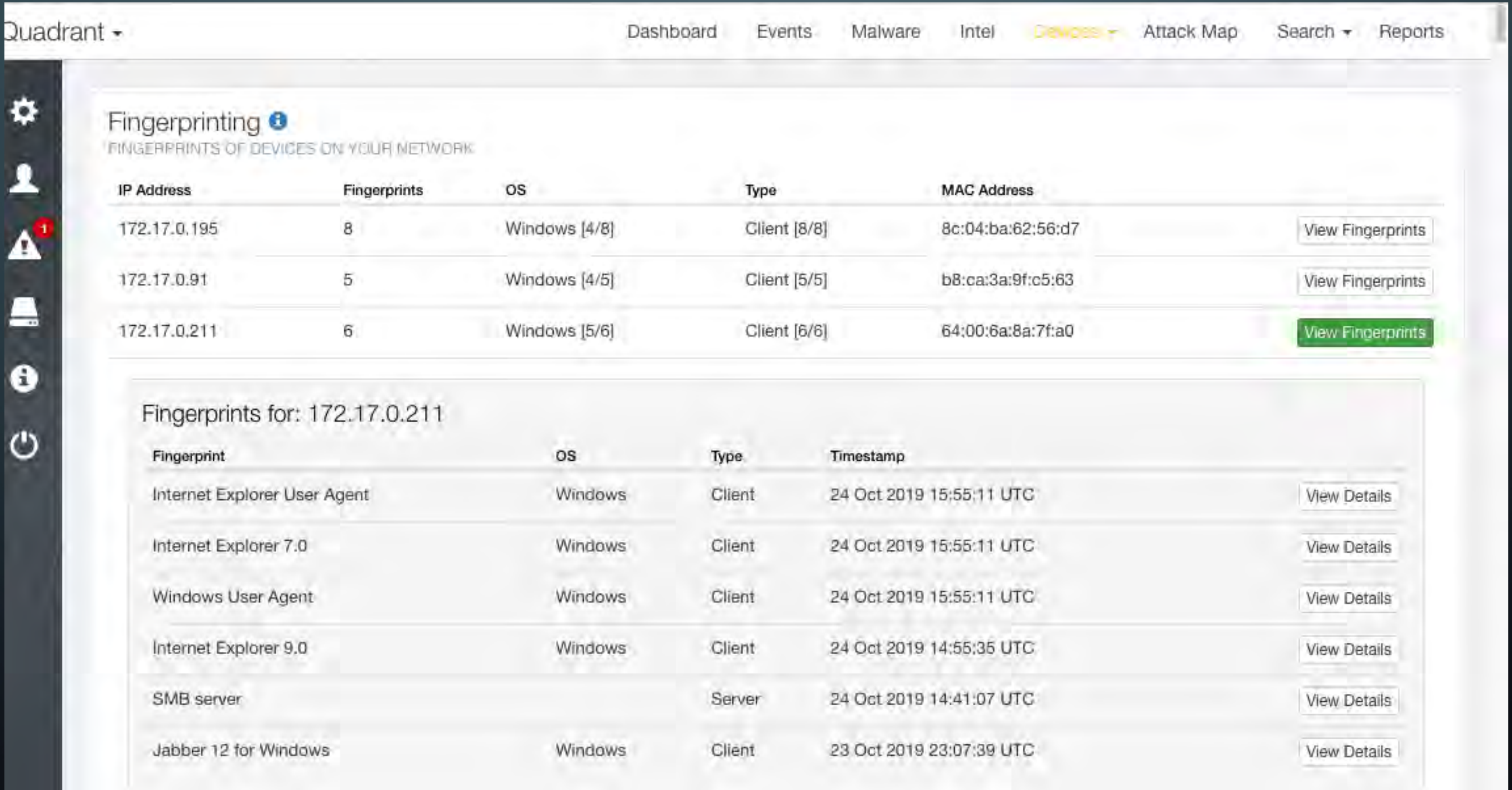


Fingerprinting

FINGERPRINTS OF DEVICES ON YOUR NETWORK

IP Address	Fingerprints	OS	Type	MAC Address	
172.17.0.195	8	Windows [4/8]	Client [8/8]	8c:04:ba:62:56:d7	View Fingerprints
172.17.0.91	5	Windows [4/5]	Client [5/5]	b8:ca:3a:9f:c5:63	View Fingerprints
172.17.0.211	6	Windows [5/6]	Client [6/6]	64:00:6a:8a:7f:a0	View Fingerprints
172.17.0.101	5	Windows [4/5]	Client [5/5]	54:bf:64:61:f3:47	View Fingerprints
172.17.0.84	5	Windows [4/5]	Client [5/5]	6c:2b:59:df:70:46	View Fingerprints
172.17.10.49	1		Server [1/1]		View Fingerprints
172.17.0.52	3	Windows [2/3]	Client [3/3]		View Fingerprints
172.17.202.25	4	Osx [3/4]	Client [4/4]	40:26:19:0f:99:ee	View Fingerprints

CONSOLE OUTPUT EXPANDED



Fingerprinting

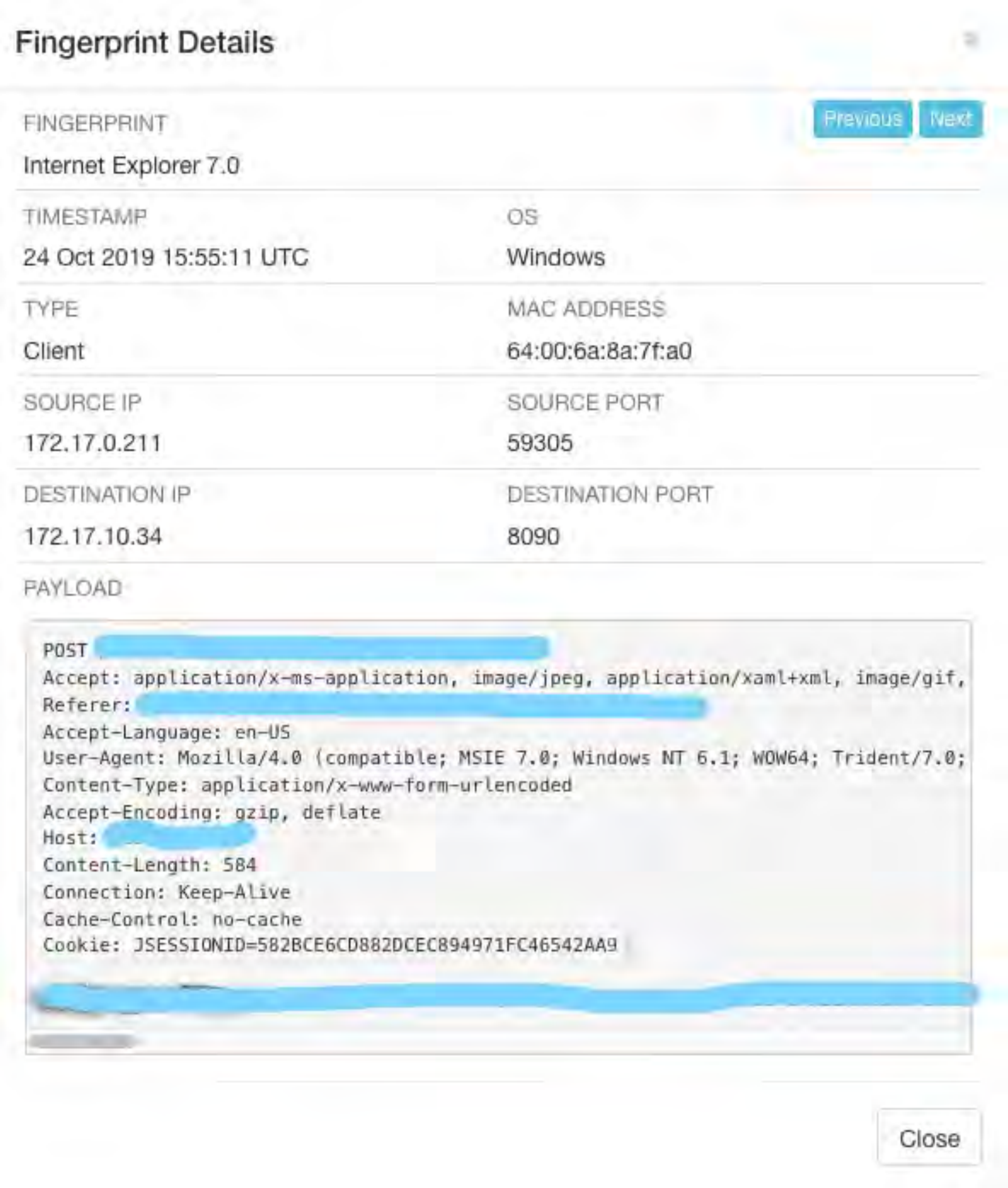
FINGERPRINTS OF DEVICES ON YOUR NETWORK

IP Address	Fingerprints	OS	Type	MAC Address	
172.17.0.195	8	Windows [4/8]	Client [8/8]	8c:04:ba:62:56:d7	View Fingerprints
172.17.0.91	5	Windows [4/5]	Client [5/5]	b8:ca:3a:9f:c5:63	View Fingerprints
172.17.0.211	6	Windows [5/6]	Client [6/6]	64:00:6a:8a:7f:a0	View Fingerprints

Fingerprints for: 172.17.0.211

Fingerprint	OS	Type	Timestamp	
Internet Explorer User Agent	Windows	Client	24 Oct 2019 15:55:11 UTC	View Details
Internet Explorer 7.0	Windows	Client	24 Oct 2019 15:55:11 UTC	View Details
Windows User Agent	Windows	Client	24 Oct 2019 15:55:11 UTC	View Details
Internet Explorer 9.0	Windows	Client	24 Oct 2019 14:55:35 UTC	View Details
SMB server		Server	24 Oct 2019 14:41:07 UTC	View Details
Jabber 12 for Windows	Windows	Client	23 Oct 2019 23:07:39 UTC	View Details

CONSOLE OUTPUT DETAILED



Fingerprint Details

FINGERPRINT
Internet Explorer 7.0

TIMESTAMP
24 Oct 2019 15:55:11 UTC

OS
Windows

TYPE
Client

MAC ADDRESS
64:00:6a:8a:7f:a0

SOURCE IP
172.17.0.211

SOURCE PORT
59305

DESTINATION IP
172.17.10.34

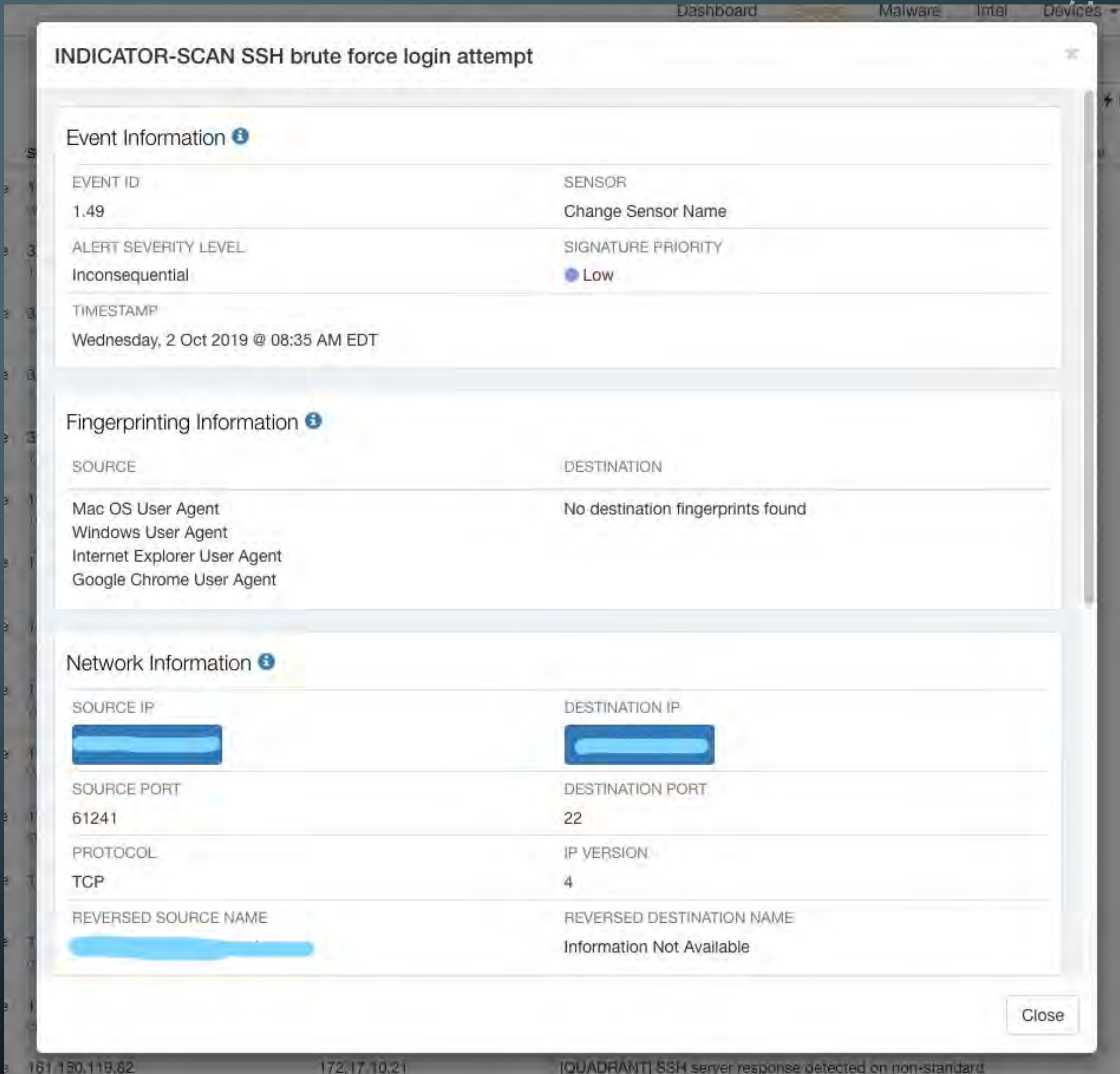
DESTINATION PORT
8090

PAYLOAD

```
POST [redacted]
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif,
Referer: [redacted]
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0;
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: [redacted]
Content-Length: 584
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: JSESSIONID=582BCE6CD882DCEC894971FC46542AA9

[redacted]
```

SOC ANALYST VIEW



INDICATOR-SCAN SSH brute force login attempt

Event Information

EVENT ID 1.49	SENSOR Change Sensor Name
ALERT SEVERITY LEVEL Inconsequential	SIGNATURE PRIORITY ● Low
TIMESTAMP Wednesday, 2 Oct 2019 @ 08:35 AM EDT	

Fingerprinting Information

SOURCE	DESTINATION
Mac OS User Agent Windows User Agent Internet Explorer User Agent Google Chrome User Agent	No destination fingerprints found

Network Information

SOURCE IP [redacted]	DESTINATION IP [redacted]
SOURCE PORT 61241	DESTINATION PORT 22
PROTOCOL TCP	IP VERSION 4
REVERSED SOURCE NAME [redacted]	REVERSED DESTINATION NAME Information Not Available

161.150.119.82 172.17.10.21 [QUADRANT] SSH server response detected on non-standard

THANK YOU!!

- Meer
  - https://github.com/beave/meer
- Fingerprint Rules
  - NEED MORE!!! Feel free to help!
  - https://github.com/quadrantsec/fingerprint-rules