A Look at Espy

Common Problem

- Remote workforces are hard to threat hunt
- There is no single point where a network sensor can be placed
- Placing a sensor in every employee's home network can be expensive
- ...not to mention a major privacy issue

espy

- Collects network traffic on Windows hosts regardless of whether or not the host is on-prem or remote by running a small agent in the background, one time setup
- Network traffic from all hosts is collected onto a centralized server
- Traffic is turned into Zeek logs
- Traffic can also be sent to Elasticsearch/BeaKer

What is espy?

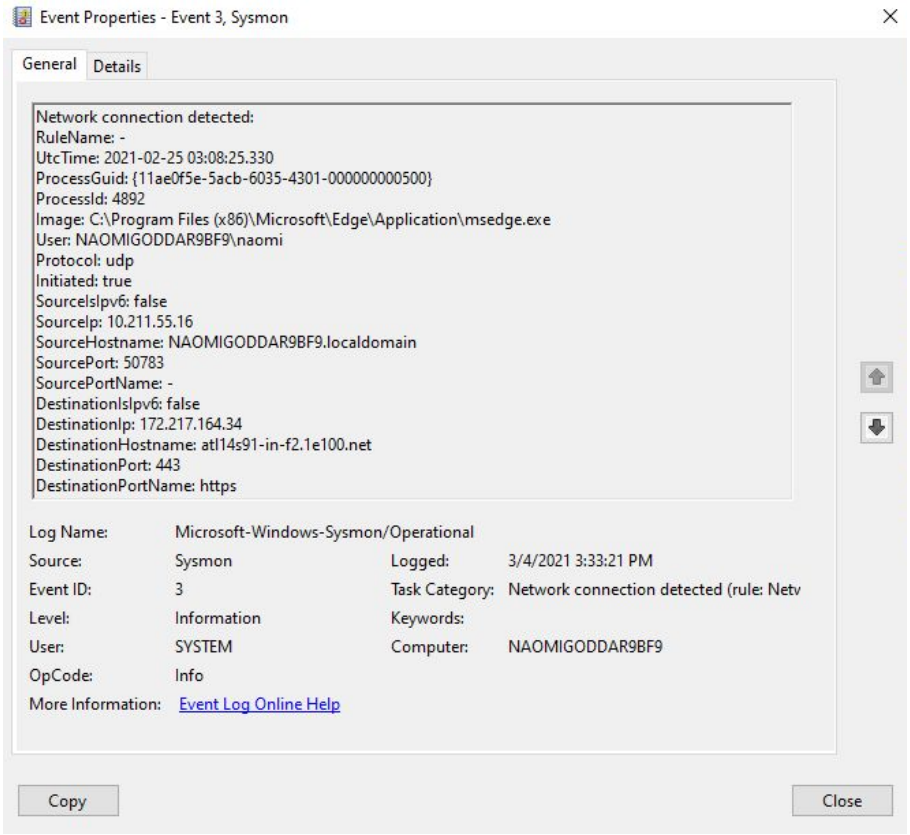
- A reference to the word espy, (ee-spy), which means to “catch sight of”
  - Espy captures traffic on remote hosts, giving you the chance to catch sight of threats you might not have otherwise been able to
- Open source project
- Combines:
  - Sysmon
  - Winlogbeat
  - Zeek log/ECS (elastic common schema) output

Sysmon

- Developed by Microsoft Sysinternals group
- Free, but doesn't ship with Windows
- Runs as a background process
- Permits you to collect event activity from the local system
- Espy focuses on Event ID 3's

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

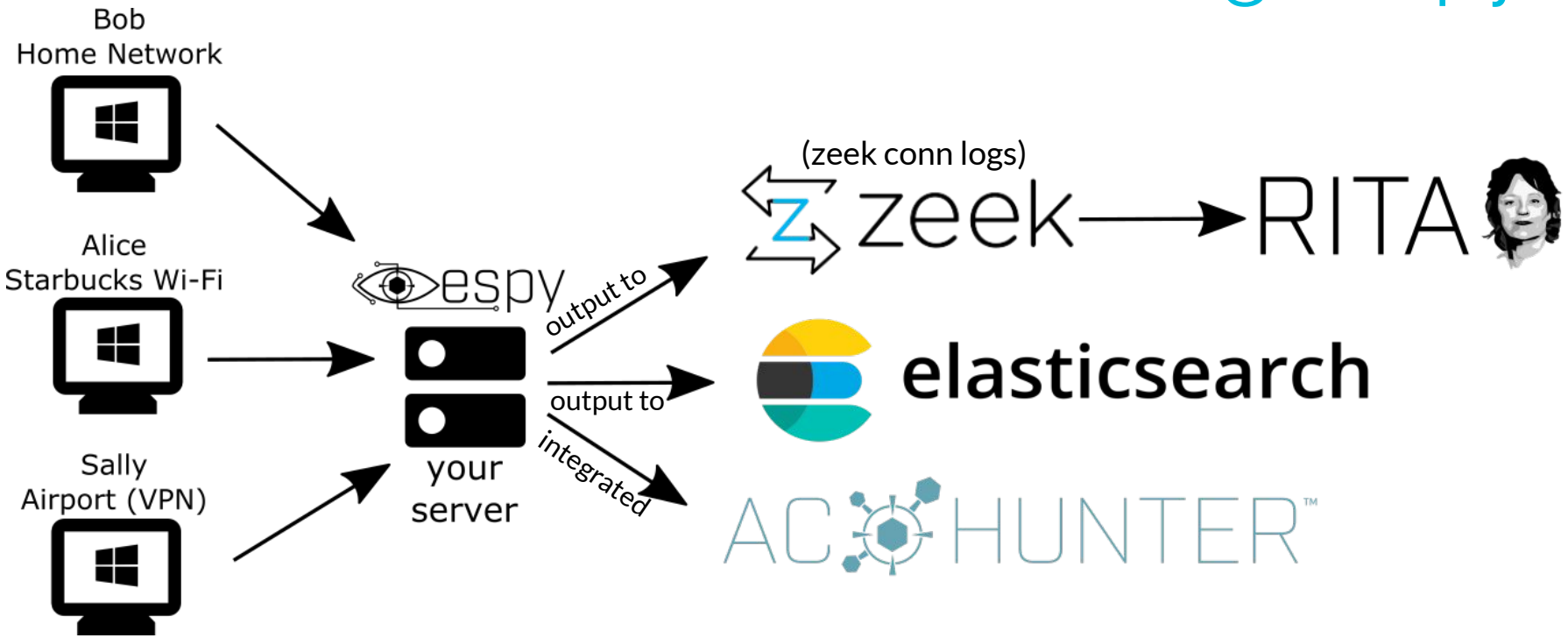
Event ID 3 Example



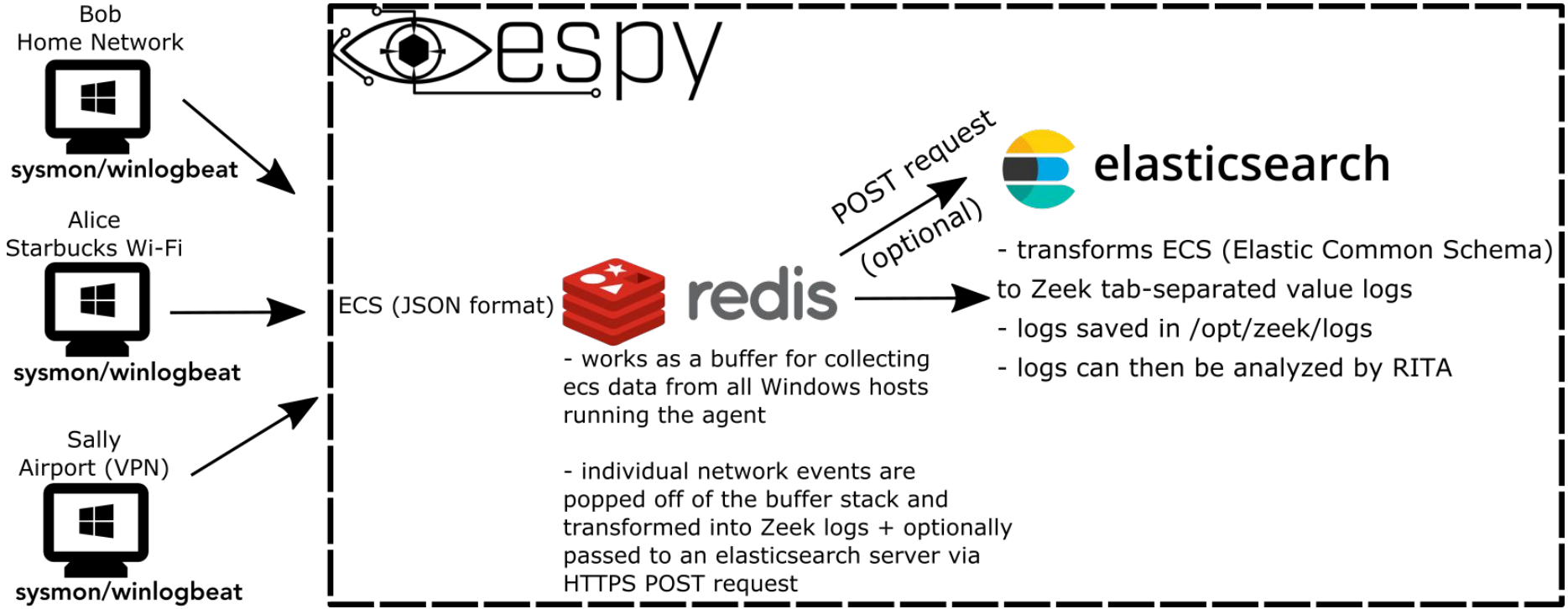
The network connection event logs TCP/UDP connections on the machine. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.

These logs can be viewed in Event Viewer under Applications & Services Logs > Microsoft > Windows > Sysmon

Visualization of data flow through espy



Data flow from a dev perspective



Espy's Zeek Logs

- Logs are rotated every hour
  - Logs can be found in /opt/zeek/logs/, grouped in folders by day, with a conn log each hour
- Conn logs contain traffic from all hosts running the Windows agent
- Logs contain a unique identifier for each host, as well as the host's NetBIOS computer name

Espy Zeek log example

1614125128.365000	-	10.211.55.16	59589	239.255.255.250	1900	udp	-	-	-	-	-	F	F	-	-	-	-	-
1614125178.561000	-	224.0.0.251	5353	10.211.55.2	5353	udp	-	-	-	-	-	F	F	-	-	-	-	-
1614125178.561000	-	224.0.0.251	5353	10.211.55.2	5353	udp	-	-	-	-	-	F	F	-	-	-	-	-
1614125357.684000	-	10.211.55.17	50979	52.137.103.96	443	tcp	-	-	-	-	-	F	F	-	-	-	-	-
1614125357.695000	-	10.211.55.16	50980	52.137.103.130	443	tcp	-	-	-	-	-	F	F	-	-	-	-	-
1614125423.487000	-	10.211.55.16	68	10.211.55.1	67	udp	-	-	-	-	-	F	F	-	-	-	-	-
1614125423.505000	-	10.211.55.18	5353	224.0.0.251	5353	udp	-	-	-	-	-	F	F	-	-	-	-	-
1614125423.505000	-	224.0.0.251	5353	10.211.55.16	5353	udp	-	-	-	-	-	F	F	-	-	-	-	-

-	-	(empty)	0ad0e0a9-6dd0-4b0d-a300-3746b13eab84
-	-	(empty)	0ad0e0a9-6dd0-4b0d-a300-3746b13eab84
-	-	(empty)	0ad0e0a9-6dd0-4b0d-a300-3746b13eab84
-	-	(empty)	1ad1e1a9-6xx0-4g1f-b568-3584b13fgts84
-	-	(empty)	0ad0e0a9-6dd0-4b0d-a300-3746b13eab84
-	-	(empty)	2ad2e2a9-9fs6-9r2b-s415-6713n269ask68
-	-	(empty)	0ad0e0a9-6dd0-4b0d-a300-3746b13eab84

NAOMIGODDAR9BF9
NAOMIGODDAR9BF9
NAOMIGODDAR9BF9
NAOMIGODDAR9BF9
BOBSMITH6CH6
NAOMIGODDAR9BF9
ALICEJERRY2AN2
NAOMIGODDAR9BF9

Espy Installation

- Setup espy server first before installing agent on any host (install script in root of GitHub repo)
  - To view the logs for espy: `./espy.sh logs -f espy`
  - To view the logs for redis: `./espy.sh logs -f redis-server`
- Each remote host needs the espy agent installed (Windows only)
  - Agent install script in `/agent/install-sysmon-beats.ps1` in espy GitHub repo
  - May have to modify execution policy first to allow script to run: `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine`

Leveraging espy with RITA

- Imported datasets will now have the network name of the source and destination of the connection, so that each host is distinguishable across different networks
  - For hosts that are not running the espy Windows Agent, Source will be labeled as “Unknown Private”, Destination will be labeled as “Public
- Analysis will only produce results for beacons, strobes, and long connections

Leveraging espy with RITA

- Analysis of hosts does keep each host unique, so if there are two hosts with the same ip address, they will be treated as separate hosts
  - If the connection between 10.55.200.10 (Alice at Starbucks) and 205.251.197.77 displays beaconing behavior, but Carol at home also has an ip of 10.55.200.10, Carol's network traffic will not contribute to Alice's beaconing analysis
- This also means that analysis is separate for each host's ip address
  - If Alice has an ip of 10.55.200.10 at Starbucks and later goes home with an ip of 192.168.1.15, analysis will be done separately for each ip
    - A beacon connection with a 10.55.200.10 as the source will not contribute to analysis done for 192.168.1.15, even though it is the same physical host

RITA Output w/ Espy-Generated Logs

*Using the -nn flag on RITA show commands will display the network names of the hosts listed in the output

```
./rita show-beacons espy-example --human-readable -nn
```

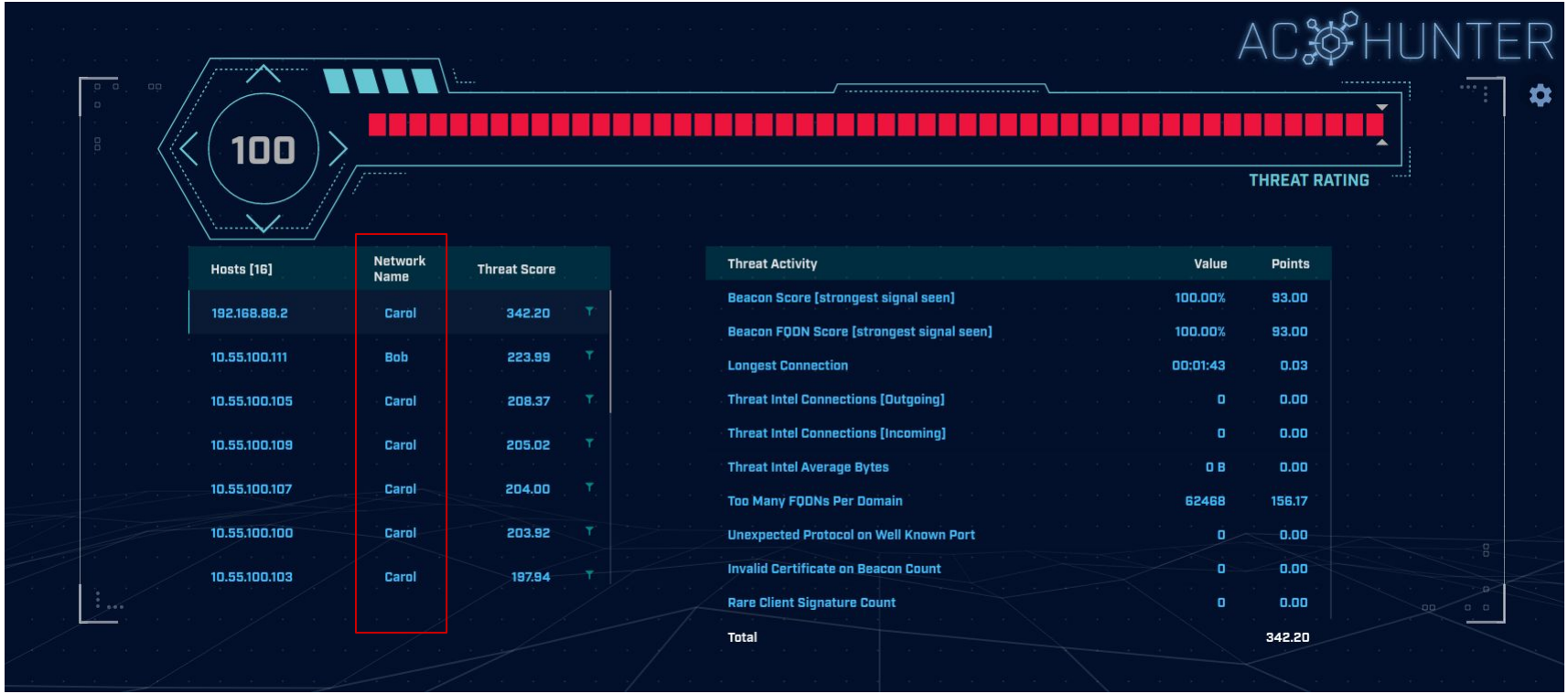
SCORE	SOURCE NETWORK	DESTINATION NETWORK	SOURCE IP	DESTINATION IP	CONNECTIONS	AVG BYTES	INTVL RANGE	SIZE RANGE	TOP INTVL	TOP SIZE	TOP INTVL COUNT	TOP SIZE COUNT
1	Carol	Public	192.168.88.2	165.227.88.15	108858	199	860	230	1	89	53341	108319
1	Bob	Public	10.55.100.111	165.227.216.194	20054	92	29	52	1	52	7774	20053
0.836	Alice Late	Public	10.55.200.10	205.251.194.64	146	308	353	4	300	70	84	142
0.835	Carol	Public	10.55.200.11	205.251.197.77	69	308	1197	4	300	70	38	68
0.834	Carol	Public	192.168.88.2	13.107.5.2	27	198	2	33	12601	73	4	15
0.834	Bob	Public	10.55.100.111	34.239.169.214	34	1259	5	14388	1	156	15	30
0.833	Carol	Public	10.55.100.103	23.52.161.212	26	5401	39563	52	1800	505	22	23
0.833	Carol	Public	10.55.200.11	205.251.194.64	231	308	354	4	300	70	101	222
0.833	Bob	Public	10.55.100.111	23.52.162.184	27	2370	37828	52	1800	467	23	25
0.833	Carol	Public	10.55.100.106	23.52.161.212	27	5425	38031	52	1800	505	19	19
0.833	Carol	Public	10.55.182.100	23.52.161.212	25	5362	41422	40	1800	465	19	13
0.833	Carol	Public	10.55.182.100	23.52.162.184	25	2376	41611	52	1800	467	20	23
0.833	Carol	Public	10.55.100.109	23.52.161.212	26	5417	39646	52	1800	505	21	20
0.833	Carol	Public	10.55.100.107	23.52.161.212	24	5404	43235	52	1800	505	19	21
0.833	Carol	Public	10.55.100.108	23.52.161.212	24	5393	43303	0	1800	505	15	24
0.833	Carol	Public	10.55.100.100	23.52.161.212	26	5388	36042	52	1800	505	16	25
0.833	Carol	Public	10.55.100.107	23.52.162.184	24	2397	43356	52	1800	467	18	18
0.833	Carol	Public	10.55.100.108	23.52.162.184	24	2370	43303	0	1800	467	18	24
0.833	Bob	Public	10.55.100.111	23.52.161.212	27	5379	37752	92	1800	505	17	20
0.832	Bob	Public	10.55.100.111	23.38.128.68	23	8177	1888	0	1800	868	16	23
0.832	Carol	Public	10.55.100.105	23.38.128.68	26	8168	14421	0	1800	868	18	26
0.832	Carol	Public	10.55.100.103	23.38.128.68	25	8156	19	206	1800	868	19	15
0.832	Carol	Public	10.55.100.109	23.38.128.68	26	8120	14527	80	1800	868	22	19
0.832	Carol	Public	10.55.100.106	23.38.128.68	27	8170	15341	40	1800	868	19	24
0.832	Carol	Public	10.55.100.104	23.38.128.68	28	8184	14458	166	1800	868	22	27
0.832	Carol	Public	10.55.100.107	23.38.128.68	26	8161	14402	0	1800	868	21	26
0.832	Carol	Public	10.55.100.108	23.38.128.68	30	8155	10929	40	1800	868	23	26
0.832	Carol	Public	10.55.100.100	23.38.128.68	31	8175	10901	0	1800	868	22	31
0.83	Carol	Public	10.55.200.11	205.251.192.89	96	324	1210	0	300	86	31	96
0.83	Carol	Public	10.55.200.11	205.251.197.245	120	322	1138	0	300	86	50	120
0.83	Alice Late	Public	10.55.200.10	205.251.197.77	98	306	354	4	300	70	38	93
0.829	Carol	Public	192.168.88.2	13.107.3.1	57	190	5902	3	3154	73	9	35
0.829	Alice Early	Public	10.55.200.10	205.251.194.64	64	308	354	4	300	70	25	63
0.829	Carol	Public	192.168.88.2	64.4.48.4	25	201	11133	0	3154	76	6	25
0.829	Carol	Public	192.168.88.2	13.107.3.2	60	193	7576	3	3154	73	10	43

Leveraging espy with AC-Hunter

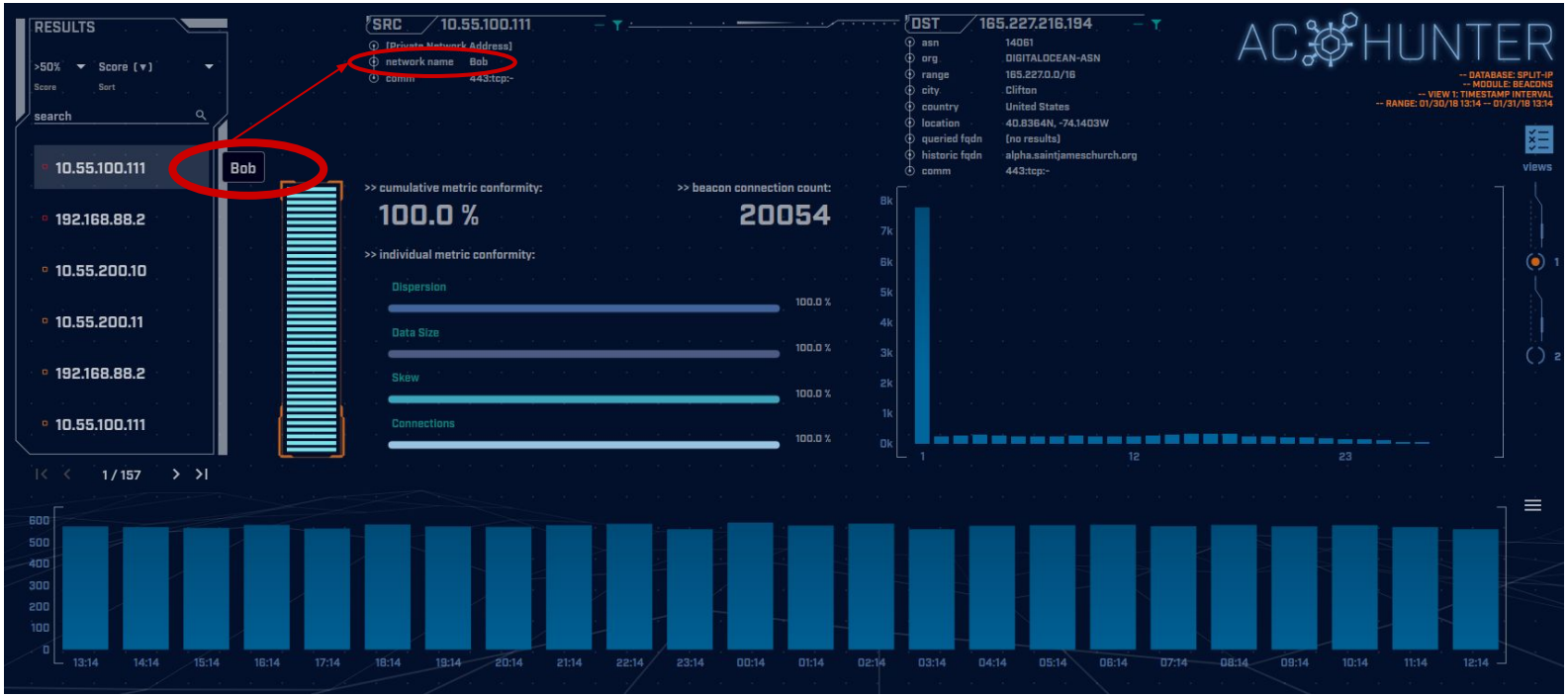
When espy is installed alongside AC-Hunter, logs created by espy are ingested along with the standard Zeek logs

The NetBIOS names for hosts running the espy agent will appear in the hostname fields introduced in version 5.0

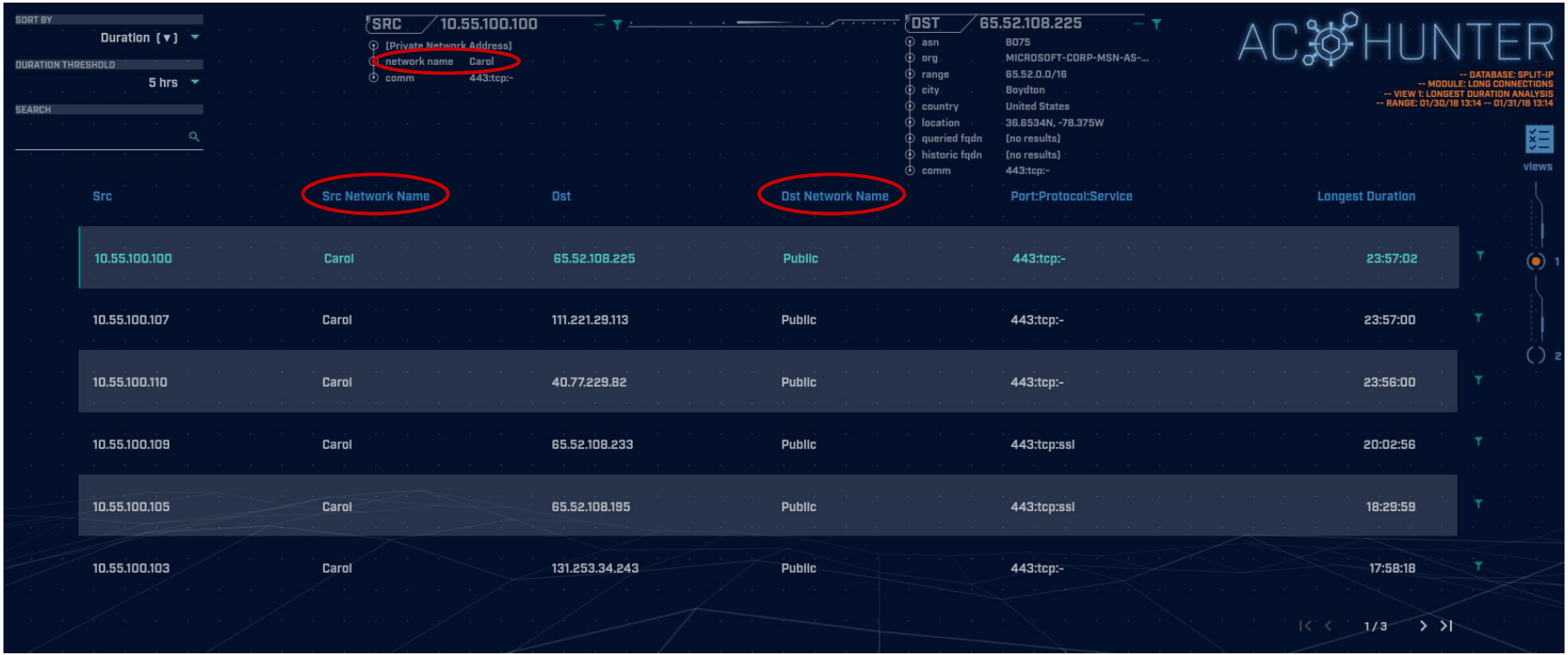
Home screen shows top scoring hosts with their NetBIOS names



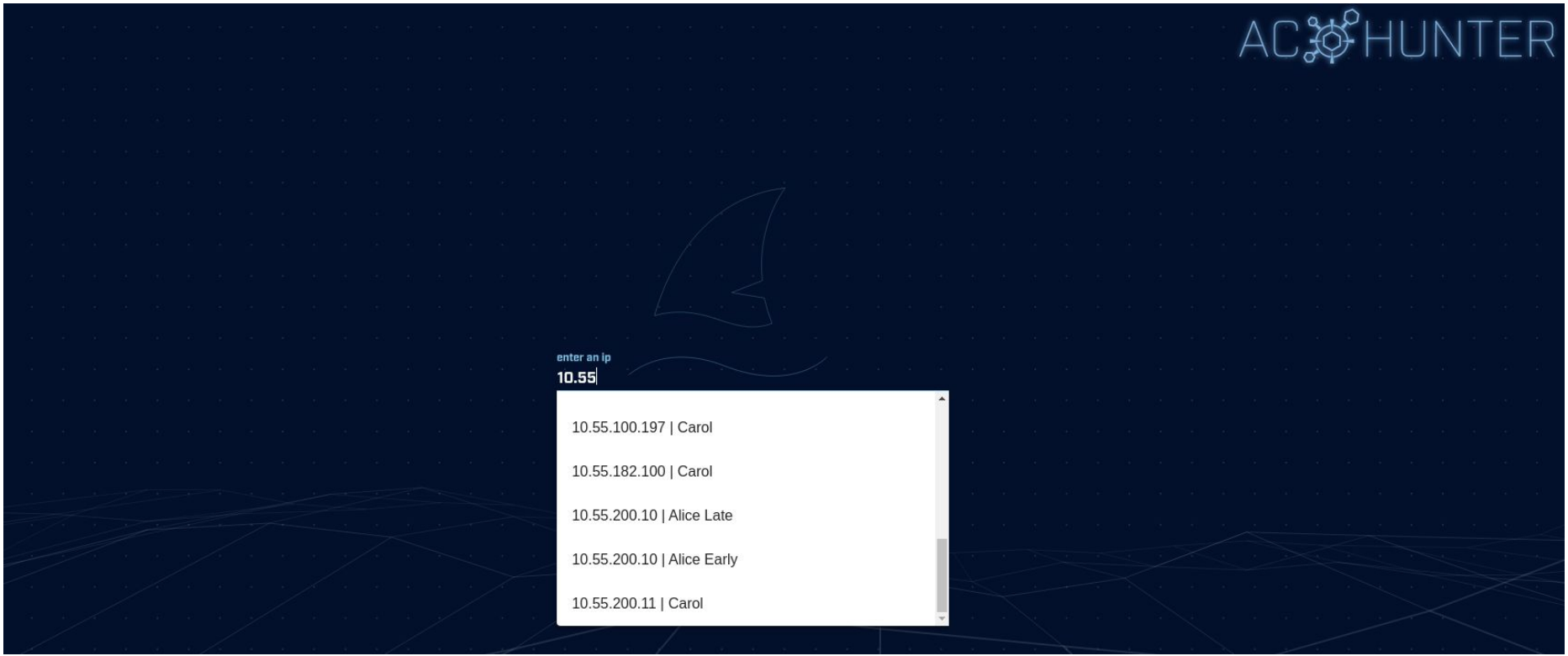
Can see NetBIOS name of source host in a connection w/ beaconing behavior



Can see the source and destination NetBIOS names for long connections



Can see the NetBIOS name when searching for an ip in deep dive



Can see the NetBIOS name when searching for an ip in deep dive