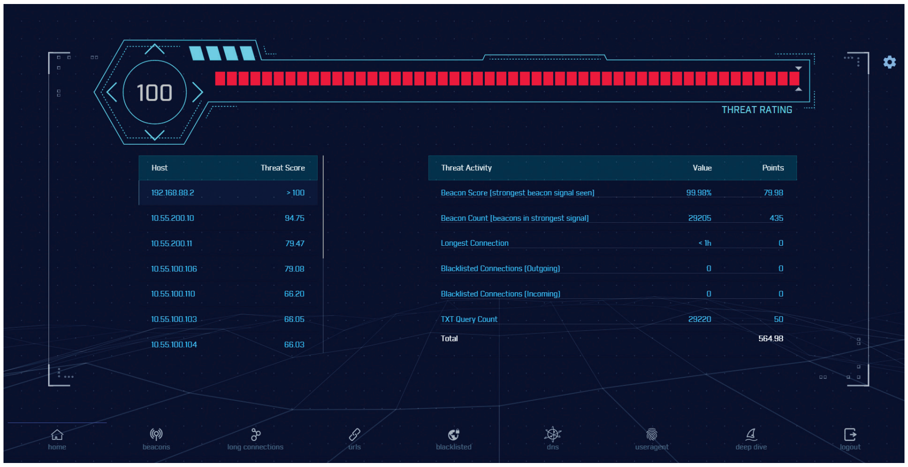
AC-HUNTER™

ANALYZE. IDENTIFY. HUNT.

NETWORK THREAT HUNTING SOLUTION

CIOs and CSOs need to be able to answer one simple question, have any of the systems on their network been compromised? This question is much harder to answer than it should be.

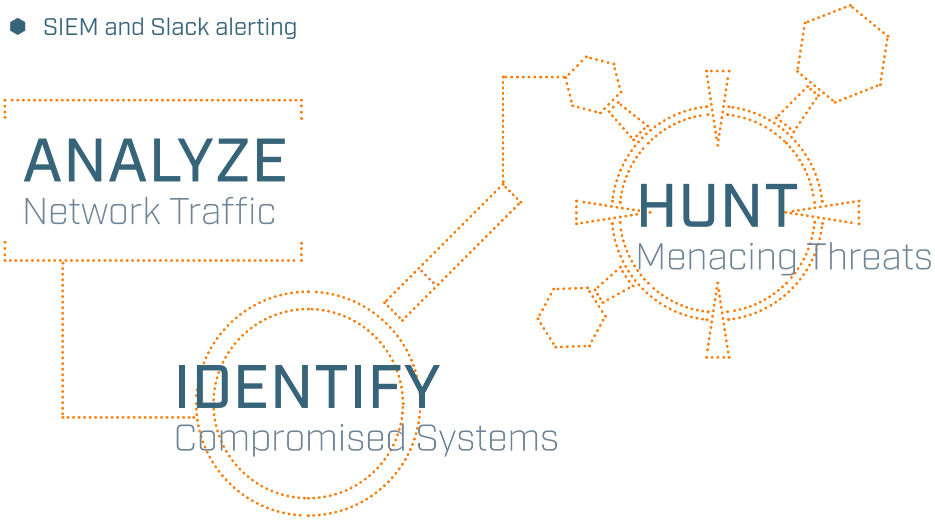


Host	Threat Score
192.168.88.2	> 100
10.55.200.10	94.75
10.55.200.11	79.47
10.55.100.106	79.08
10.55.100.110	66.20
10.55.100.103	66.05
10.55.100.104	66.03

Threat Activity	Value	Points
Beacon Score [strongest beacon signal seen]	99.98%	79.98
Beacon Count [beacons in strongest signal]	29205	435
Longest Connection	< 1h	0
Blacklisted Connections (Outgoing)	0	0
Blacklisted Connections (Incoming)	0	0
TXT Query Count	29220	50
Total		564.98

AC-HUNTER™ FEATURES INCLUDE

- Threat rating for all internal systems
- Patented beacon detection
- Simple interface focused on junior analysts
- SIEM and Slack alerting



ANALYZE
Network Traffic

HUNT
Menacing Threats

IDENTIFY
Compromised Systems

BEACONS MODULE

Rather than focus on signatures for known bad actors, AC-Hunter detects consistencies and patterns in the behavior of backdoors. How? It utilizes a mixture of detection techniques that rely on attributes like an interval of connections, data size, dispersion, and advanced algorithms.

LONG CONNECTIONS MODULE

Rather than calling home on a regular basis, attackers may try to simply call home and leave the connection open indefinitely. To spot this traffic, you can use our long connections module.

DEEP DIVE MODULE

Ever have the need to look deeper at a system? Sure, there may be something interesting, but what about the whole picture? AC-Hunter has the ability to show a total snapshot of a host in one view, and allows you to dive deeper into the different endpoints and protocols used by that host.

ALERTING

AC-Hunter continuously hunts your network looking for signs of command and control activity. When a backdoor is identified, you'll be notified via Slack, the SIEM of your choice, or a centralized logging server. This way security personnel only need to jump in when an actual threat is detected.

WHITELISTING

AC-Hunter gives you the ability to whitelist IP addresses that you wish to exclude from your threat hunting analysis. It's a popular feature, as you can whitelist based on individual IP addresses, subnets, or even full autonomous system numbers (ASNs).

www.activecountermeasures.com

115 W Hudson Street
Spearfish SD 57754
701-645-3443
questions@activecountermeasures.com

BE THE HUNTER

EFFECTIVE SIMPLE ECONOMICAL

Start focusing your valuable time on the systems that need your expertise with AC-Hunter™

"We have been working with top right Gartner quadrant tools for years, yet AC-Hunter delivered more critical actionable intelligence in 24 hours than the other tools did combined in 2 years. At last, let the hunt begin!"

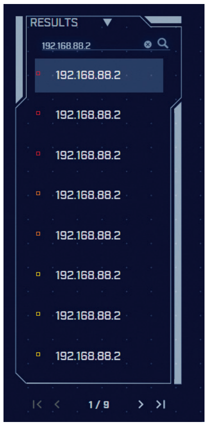
- Sam Ainscow, Barrett Steel Limited

"What kind of black magic is this?"

- CERT Team, Europe

"If you are happy not knowing if you are breached or not, do not use this product."

- Cliff Janzen, OSCP, rSolutions



RESULTS

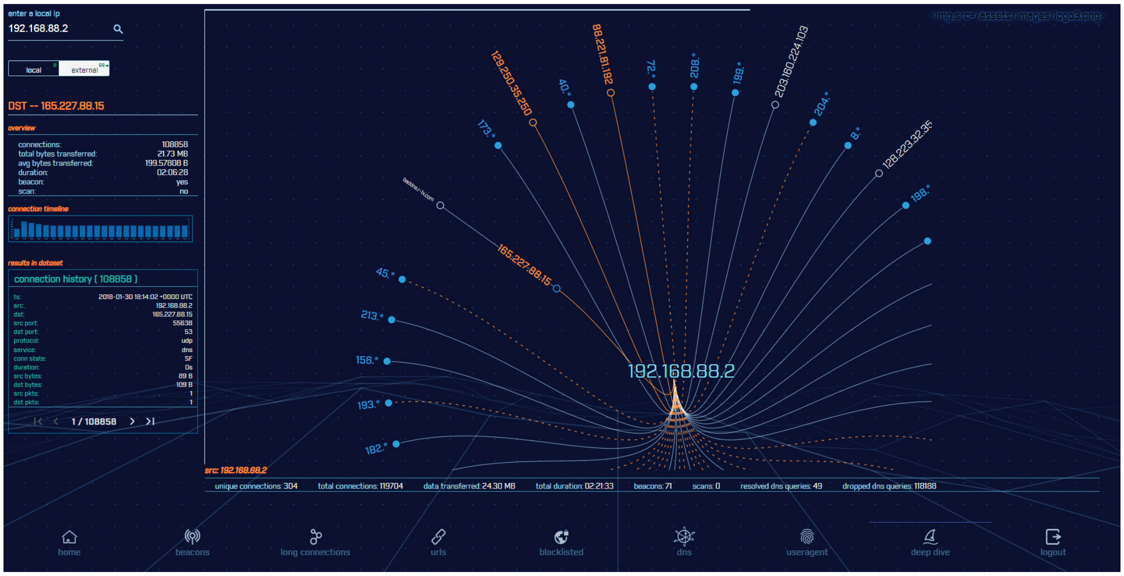
192.168.88.2

192.168.88.2
192.168.88.2
192.168.88.2
192.168.88.2
192.168.88.2
192.168.88.2
192.168.88.2
192.168.88.2

1 / 9

Active Countermeasures offers AC-Hunter a network threat hunting solution that analyzes network traffic to detect which internal systems have been compromised. There are no agents to install — AC-Hunter verifies all devices regardless of operating system or hardware. AC-Hunter also inspects encrypted sessions while maintaining data privacy and integrity.

- AC-Hunter has the ability to protect all devices; desktops, servers, network hardware, IoT, SCADA, BYOD, and more.
- The simple-to-use interface is focused on enabling threat hunting success for everyone from junior analysts to seasoned pros.



enter a local ip
192.168.88.2

local 0 | external 88

DST -- 165.227.88.15

overview

```
connections:                      108858
total bytes transferred:        21.73 MB
avg bytes transferred:      199.57808 B
duration:                       02:06:28
beacon:                              yes
scan:                                 no
```

connection timeline

results in dataset

connection history (108858)

```
ts:          2018-01-30 18:14:02 +0000 UTC
src:                       192.168.88.2
dst:                      165.227.88.15
src port:                         55638
dst port:                            53
protocol:                           udp
service:                            dns
conn state:                          SF
duration:                            0s
src bytes:                         89 B
dst bytes:                        109 B
src pkts:                             1
dst pkts:                             1
```

1 / 108858

src: 192.168.88.2

```
unique connections: 304   total connections: 119704   data transferred: 24.30 MB   total duration: 02:21:33   beacons: 71   scans: 0   resolved dns queries: 49   dropped dns queries: 118188
```

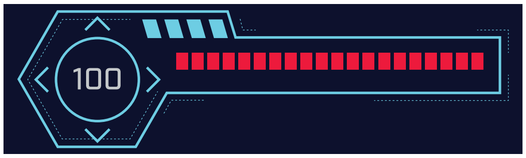
Today's adversaries are getting better and better at hiding their backdoor command and control traffic, and the data they're sneaking out of your network. The skills gap to ramp up new SOC personnel is getting more and more difficult to bridge.

VISUALIZATION DASHBOARD

You no longer need to dig through millions of log entries to identify suspect systems. AC-Hunter does the first pass of the threat hunt for you and provides a threat score for each of your internal systems. The higher the score, the more likely the system has been comprised. All in a single easy-to-read dashboard.

PRIORITIZE YOUR TIME

AC-Hunter prioritizes and color codes your systems to identify which ones are most likely compromised. Simply start at the top of the list.



Request a Personal Demo of AC-Hunter™

https://acm.re/ac-hunter-demo/