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.

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.

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

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

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 57764
701-645-3443
questions@activecountermeasures.com

BE THE HUNTER
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.

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.

**Request a Personal Demo of AC-Hunter™**
https://acm.re/ac-hunter-demo/