Active Countermeasures / Corelight Joint Solution Brief

Corelight and Active Countermeasures have teamed up to reduce the time of network compromise detection

There is a hole in our security posture. Multiple studies have identified that the time between when an attacker compromises a system, to when that compromise is contained, is over six months. Recent data shows that this trend is getting worse, not better, and the longer an attacker remains in control the greater the business risk and the cost of recovery. In fact, when the numerous companies we've seen the news have experienced a compromise, they typically find out through an outside third party. Regardless of whether they were PCI, SOC or ISO 2700 compliant, their internal security controls failed to detect these compromises.

This problem is even more pronounced on large enterprise networks, who may have tens of thousands of desktops, servers, IoT and network hardware devices to protect. This is why Corelight and Active Countermeasures have teamed up to reduce the time of compromise detection from six months to less than 24 hours. By combining Active Countermeasures' network threat hunting solution AI-Hunter™ with Corelight's high speed sensors, Security Operation Centers can leverage junior staff members to threat hunt the network, regardless of the number of hosts being protected.

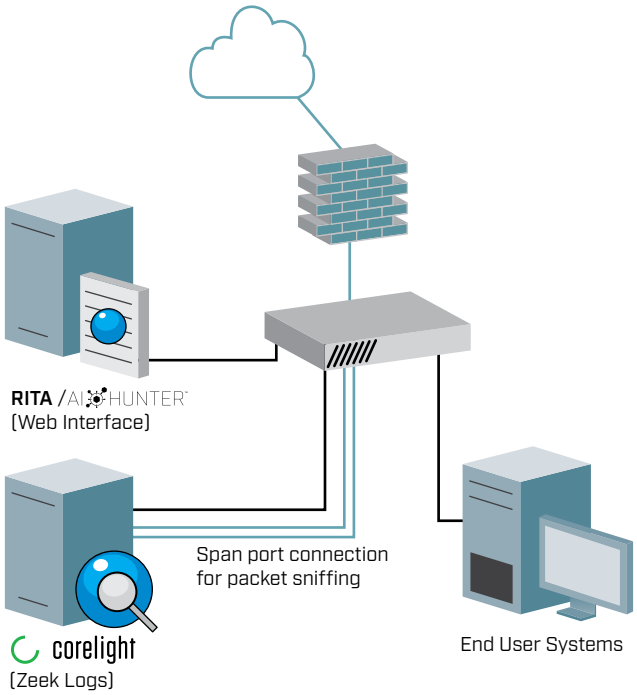
The joint solution provides:

- Quick and easy agentless install
- Actionable data within the first few hours
- Protection of all systems including clients, servers, network hardware, IoT, IIoT or BYOD
- Integration with common SOC logging solutions
- Simplified GUI focused on making junior analysts successful threat hunters

---

The Corelight probe is connected to the network so that all Internet based traffic can be monitored. This is done by connecting to the internal interface of the firewall, either via a span port or network tap. The Corelight logs are then fed to the AI-Hunter system, which analyzes the data looking for signs of command and control (C2) traffic. When an internal system becomes compromised, C2 communications is what permits a remote attacker to take control of that system. By identifying C2 communications, you can identify which internal systems are under the control of an outside party.

Unlike other threat hunting solutions, AI-Hunter does not try to pattern match on suspicious or unusual traffic patterns. Because of the efficiency of the Corelight logs, AI-Hunter can continually hunt through the previous 24 hours worth of network data. This permits AI-Hunter to be far more accurate in identifying C2 communications than competing solutions.



corelight / ACTIVE COUNTERMEASURES

When C2 communications are detected, the SOC is notified via Syslog compatible messaging or via Slack. An analyst can then login to the AI-Hunter interface to quantify the impact of the attack.

Corelight Sensors

Corelight Sensors transform network traffic into rich logs, extracted files, and custom insights via Zeek (formerly known as Bro), a powerful, open-source network security monitor used by thousands of organizations worldwide. Make quick sense of traffic so you can resolve incidents faster and threat hunt more effectively.

AI-HUNTER™

AI-Hunter detects malware by targeting its network communications. Rather than analyzing the host itself, where malware writers can leverage a wide range of evasion techniques. AI-Hunter scrutinizes network traffic for signs of a compromised system. It does not matter if the data is encrypted or using non-standard communication ports nor does it matter if the compromised system is running Windows, Mac OSX, Linux or running on an appliance. AI-Hunter can sort through millions of network connections and produce an action item list of the system most likely to be compromised.

AI-Hunter provides a wealth of information to support threat hunting activities. For example, one telltale sign of a compromise is a system that frequently communicates out to an attacker's command and control (C2) server. AI-Hunter produces easy to read graphs to make this activity stand out from normal network traffic.

AI-Hunter uses 24 patented processes to analyze timing and data size characteristics. AI-Hunter will quickly segregate normal communications from malicious communications and automatically show which systems are behaving badly. Data can also be reviewed manually for those who want to deep dive and achieve a better understanding of the suspicious traffic.

AI-Hunter is distinguished from other offerings in several ways:

- AI-Hunter detects compromises by analyzing traffic flow
- There are no agents to install which gives AI-Hunter the ability to protect all devices
- Desktops, servers, network hardware, IoT, SCADA, BYOD, and more
- AI-Hunter analyzes data in 24-hour periods delivering superior visibility of beacon activity
- Session size analysis enables AI-Hunter to detect covert communications over protocols that other vendors ignore. For example, email to public servers
- AI-Hunter can process raw pcaps. This is used when installing software/hardware onsite is not an option

Zeek Network Security Monitor

is an open source network monitoring tool that has been released under BSD licensing. It captures the network traffic passing by on your network and converts this information into logs that can be analyzed. It is considered to be one of the best network analysis tools available. More information can be found at:

https://www.zeek.org/

Zeek is sophisticated and flexible, but it's not easy to deploy or use in its open-source format.

The Corelight Sensor appliance simplifies Zeek deployment and management, making the installation and operation of AI-Hunter even more powerful.

Real Intelligence Threat Analytics (RITA)

is an open source framework for network traffic analysis. This open source project is developed, funded and supported by Active Countermeasures and can be found at:

https://acm.re/free-tools/rita/

The framework ingests Zeek Logs, and currently supports the following major features:

Beaconing Detection: Search for signs of beaconing behavior in and out of your network

DNS Tunneling Detection: Search for signs of DNS based covert channels

Blacklist Checking: Query blacklists to search for suspicious domains and hosts