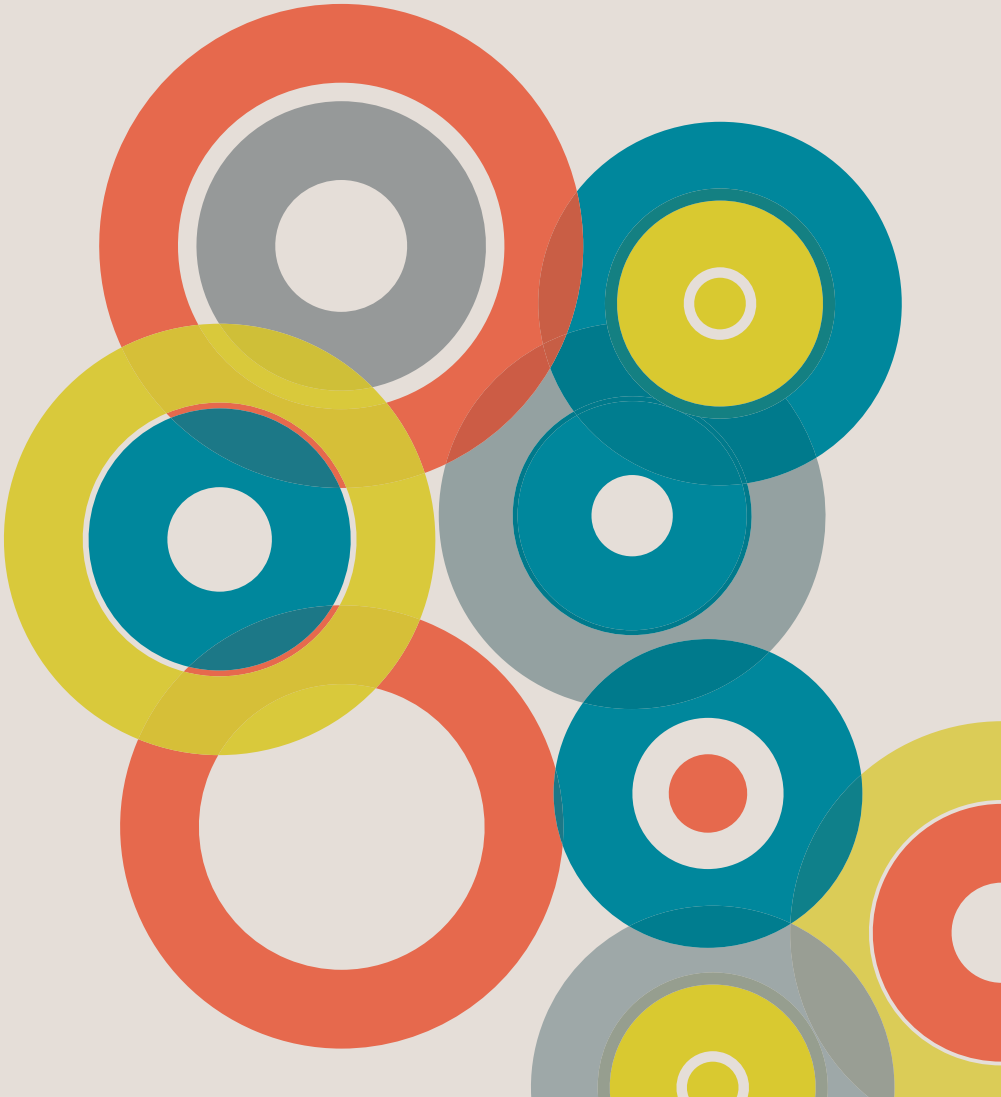
CAPSULE8

Overview: Capsule8's Attack Detection Methods

A Capsule8 Quick Read



The Capsule8 Design Philosophy

The detection methods on Capsule8 Protect were built on the following principles:

1. **Quality Telemetry:** minimizes false positive alerts generated in runtime environments
2. **Full Stack Support:** integrates with your existing IT and cloud infrastructure and security technologies
3. **Flexibility:** ensures that each detection method has flexible policies around it so that you can tailor according to your requirements
4. **Continuous Innovation:** Capsule8 works closely with customers to prioritize, design, and build new detection methods in response to the latest exploits

Capsule8's real-time detection methods range from those implemented at the kernel level all the way up to network level. Let's look at each category.

A. KERNEL-LEVEL DETECTION

Capsule8 kernel-level detection methods are designed to detect when kernel functions known to be useful for exploitation are returning directly to userland. In addition, probing code (or "kernel landmines") are embedded at both the local and host level, and are triggered when access restrictions within the kernel are either bypassed or disabled by malicious actors. An example of this is the detection of SMEP/SMAP privileges being disabled by an attacker.

Capsule8 kernel-level detection methods are characterized by low overhead and minimal performance impact to production. Since Capsule8 sensors run outside the Linux kernel and collects kernel-level data without the need for a kernel module.

For a closer look at how Capsule8 kernel-level detection works under a simulated attack, download our technical whitepaper.

B. USERLAND DETECTION

Capsule8 userland detection methods consist of policies setting user privileges as well as the bounds of a process stack (e.g. detecting inappropriately large stack sizes).

The Capsule8 solution focuses on creating userland detection policies that are meaningful without the environment becoming too restrictive for practical use, or, in most cases, overwhelming security teams with too many alerts (that get ignored).

C. FILE SYSTEM DETECTION

Capsule8 file system detection methods regulates the creation of new files, sets file permissions, and enforces file integrity in real-time. This includes detecting unexpected changes to monitored files / directories, or changes made by unexpected programs or users.

Typically, file system detection policies have the potential to flood security teams with false positives. To combat this risk, Capsule8 has built in a Detection Force Multiplier, a proprietary method for detecting indicators of common exploitation techniques, one that can prioritize high-fidelity data, reducing a customer's flood of alerts to a trickle.

D. NETWORK DETECTION

Capsule8 offers a comprehensive suite of network detection methods, ranging from policy-based detection for network traffic to more workload-specific monitoring for outbound TCP connections.

Some of Capsule8's network detection methods are vendor specific. For example, a strategy that detects communication with AWS metadata IP.

The Capsule8 Vision

This overview covers only a fraction of the detection methods currently available on Capsule8 Protect. It does not included Capsule8's investigations and automated response capabilities as well as behavioral-based methods currently being developed for 2019 and beyond.

At Capsule8, we are continuously working with customers to prioritize, design and build new detection methods that work for their unique operating environments. For a closer look at Capsule8 Protect in action, sign up for a demo today.

CAPSULE8

About Capsule8

Capsule8 is the industry's only real-time, zero-day attack detection platform capable of scaling to massive production deployments. Capsule8 delivers continuous security across your entire production environment — containerized, virtualized and bare metal — to detect and disrupt attacks as they happen.

Learn more at www.Capsule8.com.