Introducing ActiveSOC™

Incident response decision-making by
validating below-the-threshold intelligence

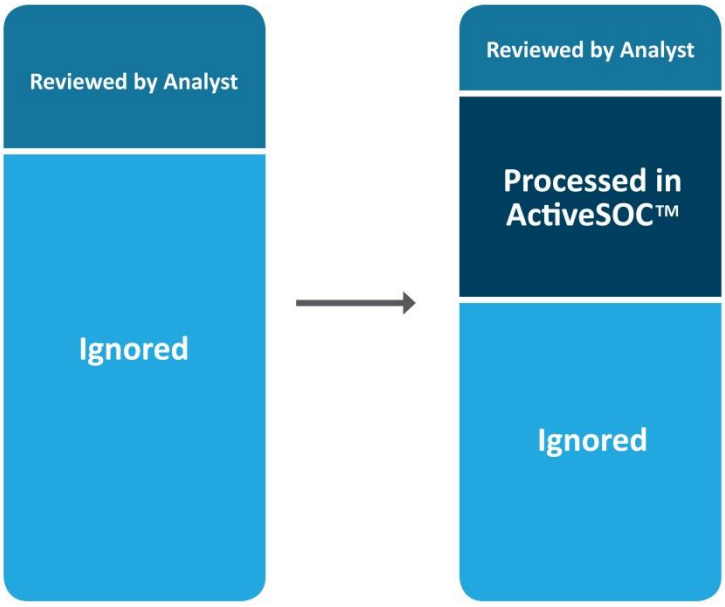
INTRODUCING ACTIVESOC™

When ActiveSOC processes an alert/event, it deploys deception elements to the alert's origin. This validates, without interfering with IT systems or the user, that there is an actual attack taking place (this alert/event would otherwise probably have been discarded). Afterwards, the deception elements that were deployed are automatically removed.

In essence, ActiveSOC automatically validates that low-scoring events (e.g., "User logged in from an unusual location") are attacks.

Benefits of using ActiveSOC:

- Reduce SOC costs and the number of alerts an analyst sees by validating alerts before they reach the analyst.
- Create new intelligence out of discarded "below-the-threshold" events.
- Give the analyst another response option (i.e., *validate* this alert), allowing the analyst to activate an automated validation process.
- Reduce friction for the end user by *reducing* disruptions such as reimaging the user's system.



INTRODUCTION TO DECEPTION

Deception catches threat actors as they make their first movements inside a network, by leveraging the fact that after gaining access to a network, attackers follow a predictable attack pattern: reconnaissance, lateral movement, and exploitation. Starting from the initial reconnaissance phase, deception technology takes advantage of this and creates a controlled path for attackers to follow. Deception focuses on critical stages through which all attackers must pass: infiltration and lateral movement. This allows for the hunting and catching of APTs, as well as less sophisticated threat actors.

DECEPTION ORCHESTRATION™: A NEW APPROACH TO IR

Based on an event *trigger*, your alerting system activates our deception platform's API, which in turn intervenes with a deception option. This option will validate that there is an actual attack taking place, without interfering with IT systems or the user. Afterwards, the intervention is removed.

With Deception Orchestration™, you deploy to ***where*** you need to deploy, ***when*** you need to deploy, based on intelligence you already own.

When a *trigger* is identified, the ActiveSOC is activated via either the API or a direct integration (or a plugin) for your specific system (e.g., ArcSight, Splunk, ThreatConnect).

EXAMPLE

Trigger: **A user logged in from an unusual location.**

This could mean any number of things: the user might be traveling or connecting from a different network. It could also mean the user's credentials have been compromised and an attacker is now using them to gain access to your systems.

By itself and under most correlations, this event would not score high enough for analyst attention and it would be discarded – if it is even collected to begin with. With ActiveSOC, it is validated.

Attacker path analysis

If this is indeed an attack, an Attacker Path Tree™ unfolds.

First the attacker will try to ascertain whether the system is valuable. If they deem it to be valuable, they are likely to check for administrative access. If they are unable to obtain administrative access, they will either proceed to steal all relevant data and then pull out of the system, or attempt to gain higher privileges by use of an exploit, based on the previously determined value of the system. Once the attacker gains administrative access, they may attempt to carry out any number of activities, such as sniffing the network or dumping credentials from memory using mimikatz.

Intervention:

Knowing how the Attacker Path Tree unfolds, we could quickly proceed and leave a credential – a "breadcrumb" – in memory for the attacker to find.

If there is a real attacker, when the breadcrumb is found, it is used to access a decoy machine we created in advance. A high-fidelity alert will be generated.

Thus:

- ActiveSOC verifies that this event is a real incident carried out by a real attacker.
- ActiveSOC provides the analyst with the relevant IoCs (such as a sample of what the attacker used) as well as the endpoints that were compromised (such as the one from where the breadcrumb was stolen, and the one used to connect to the decoy).

OTHER TYPES OF *TRIGGERS*

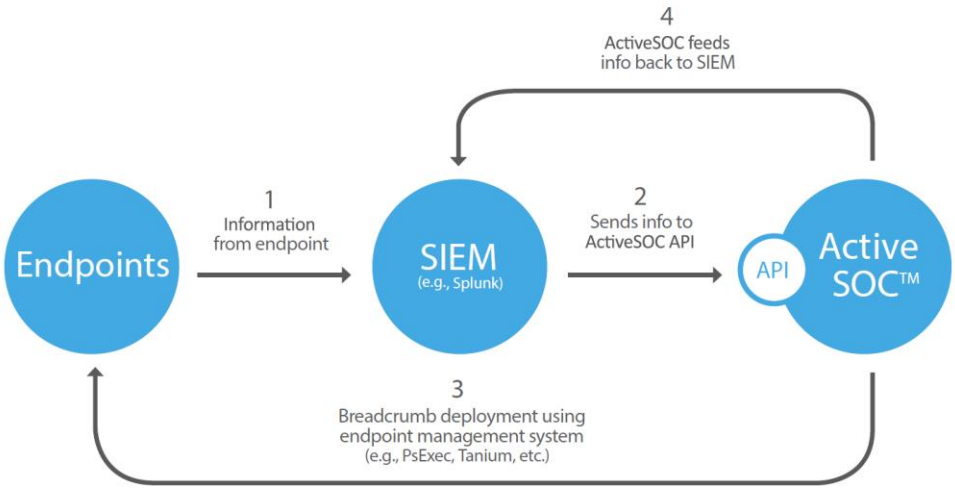
Triggers could be any type of event, from a user logging in from an unusual location, to a privilege escalation alert (someone logged in as admin), all the way to a computer connecting to an IP that doesn't exist and now reaching a decoy, or someone attempting to access a web page/app that doesn't exist.

The intervention for each such *trigger* is based on the Attacker Path Tree; it could be creating a decoy on the network to answer the computer attempting to access the non-existent IP address or web page, or as basic as a *credential hash* in memory.

HOW IT WORKS – INTEGRATION WITH EXISTING SYSTEMS

ActiveSOC works by integrating with existing systems to receive *triggers*, deploy deception elements, report back, and clean up after itself.

1. SIEM (or similar) receives *information* from endpoint solutions, or from other sources.
2. Based on the *events received by the SIEM,* actions are triggered in the ActiveSOC via the ActiveSOC API or system-specific plugins. Actions could also be triggered in the ActiveSOC by an IR system.
3. ActiveSOC deploys (and later will remove) deception elements using your endpoint management and provisioning systems (e.g., Tanium, McAfee, Phantom, Chef/Puppet, etc.).
4. ActiveSOC feeds information back to your event management system or IR orchestration, then cleans up after itself (using your endpoint management system, as mentioned above).



INTELLIGENCE PRODUCER VS. INTELLIGENCE PROVIDER

A SIEM-like system works by correlating events to a score. If the score is above a certain threshold, an analyst will be alerted. Otherwise, the event will be discarded (potentially used for big data analysis later on).

ActiveSOC is an intelligence producer. Verified *events/alerts* are created out of the otherwise discarded "under-the-threshold" events in your log handling and analysis system, such as your SIEM or threat intelligence platform.

With ActiveSOC, such events can be treated as *triggers*, activating a deception intervention that validates that there is an actual incident happening, and then proceeds to alert the analyst with the relevant intelligence.

Discarded events are now validated as real incidents, without disturbing the IT environment or the user.

REDUCE IT COSTS OF INTEGRATING DECEPTION

ActiveSOC provides significant security and workflow value to the customer in intelligence generation and decision making, while solving some of the biggest challenges faced when deploying deception solutions.

The two biggest challenges faced when deploying deception solutions are:

- Deployment scalability – Before ActiveSOC, deploying deception solutions often required a wide deployment, which is difficult in some IT environments. With ActiveSOC, deception is only deployed **when** and to **where** it is needed.
- IT integration – As a result of the above, IT integration is much smoother.

IS THERE SECURITY VALUE IN ACTIVESOC™ WHEN COMPARED WITH MAZERUNNER?

Wouldn't it be better to simply deploy deception across our organization?

If you can do that, it may be the best solution for you and you may want to check out our cyber deception platform, MazeRunner. However, ActiveSOC is not just about deployment and IT integration: there is much to be said for tailoring deception to specific intelligence requirements, and orchestrating your automated response accordingly.

FOR MORE INFORMATION OR FOR A PRODUCT DEMONSTRATION, PLEASE CONTACT IRENE AT IRENE@CYMMETRIA.COM