Asimily for Incident Response

Quickly respond to cybersecurity incidents affecting medical and IoT devices

The average attacker stays on the target's environment for only **48 hours**. And with the average cost of a cyber incident in the millions of dollars, it's more important than ever for HDOs to create an incident response plan for their IoMT devices. Asimily Insight provides powerful capabilities for incident responders, network analysts, and SOC teams to detect and respond to incidents as they occur and prevent the next one from happening.

Detect

Asimily can detect suspicious or malicious network activity in two ways:

01 Anomaly Detection

Insight's built-in anomaly detection engine monitors all traffic to and from IoMT devices, to detect suspicious activity like:

- **Indicators of compromise**, such as callbacks to malicious command & control servers
- **Attempted compromises**, such as exploit code, whether or not it was successful
- **Risky activity** that could precipitate a breach, such as unencrypted or insecure protocols in use

02 Policy Management

Additionally, Insight offers powerful policy management functionality, enabling HDOs to create rules that correspond to their own corporate policies. Administrators can use more than 30 parameters to create these policies, enabling them to be customized on a per-network, per-facility, or per-device-type basis.

Investigate

Once an incident has been detected, Insight provides capabilities to empower further investigation through several ways:

01 **Topology report** shows which devices and other systems the device in question has been communicating with. These are often useful to perform follow-up investigations on, as they could be the target or source of lateral movement activity by attackers. By pivoting to the "neighbors" and then subsequently into those system's neighbors, an accurate map of device relationships can be created and leveraged for investigations.

02 **Flow analysis** shows which protocols a device is talking on, and to which systems. Looking at these data can provide additional evidence, for example if a device is sending large amounts of data to other systems, or using protocols that are unusual for its type or model.

03 Most medical devices do not keep detailed logs of network events, and the logs that do exist may not be easy to collect into a SIEM or workflow management solution. In an incident, often getting the right data collected constitutes **over 50%** of the total cost to respond. This is why Insight offers a **Distributed Sniffer**, which can capture any traffic to or from the devices in question in PCAP format. This can be initiated on demand, or automatically in response to an Anomaly event. This data can be leveraged for both incident response and forensic purposes, to reveal the tactics, techniques, and procedures that an attacker is using. In many HDO environments, there are no other ways to capture raw traffic without network changes and cross-team coordination, actions that take up valuable time while in the midst of an incident.

Respond

When an HDO wants to respond to an emergent incident, Insight integrates with common network access control (NAC) and firewall solutions such as Cisco ISE, Fortinet FortiGate, Extreme, Checkpoint, Aruba, and others. Directly from the Insight Console, administrators can quarantine devices, preventing them from communicating with other machines on the network, without interrupting their investigation. During an attack, time is of the essence and responding quickly can prevent an incursion from spreading laterally and causing serious damage.

Detect →

- Built-in policies detect new and emergent threats
- Custom rules enable targeting to HDO policies

Investigate →

- Topology and flow analysis provide targets for follow-up investigations
- Distributed Sniffer helps reconstitute an attacker's actions

Respond

- Quickly block or quarantine impacted devices
- via integrations with nforcement solutions