

PREEMPTIVE INCIDENT RESPONSE

SECDO's unique Preemptive IR solution empowers cyber security teams to slash incident response time from months to minutes, remediate attacks surgically without impacting business continuity and apply the lessons learned to augment cyber defenses.

REPLACING TRADITIONAL IR WITH PREEMPTIVE IR

SECDO replaces the traditional after-the-incident response process and its tedious forensic data acquisition with preemptive continuous collection and analysis of all endpoint and server, activity in anticipation of incidents. The SECDO solution comprises three components: Observer, Analyzer and Responder.

OBSERVER: ZERO-GAP VISIBILITY OF ALL HOST ACTIVITY

Observer continuously records all events and behaviors (including user, file, memory, process, thread, registry, network, USB, etc.) down to the thread level on every endpoint and server and stores them on a secure server where they are retained for years. Analysts can investigate any alert or hunt for threats effectively.



Visibility enables quick discovery of any relation between users, files, hosts, processes, etc.



Forensic Timeline visualizes the complete history of all events on all hosts



Host Insights provides pre-built queries to see information across the network



IOC Searches can be initiated based on IOC files

BENEFITS

Incident Response time slashed

From alert to cleanup in minutes, minimizing the damage and disruption of a breach

Zero-gap host visibility

Complete historical, thread-level visibility into every endpoint and server in the network

Number of alerts processed is multiplied

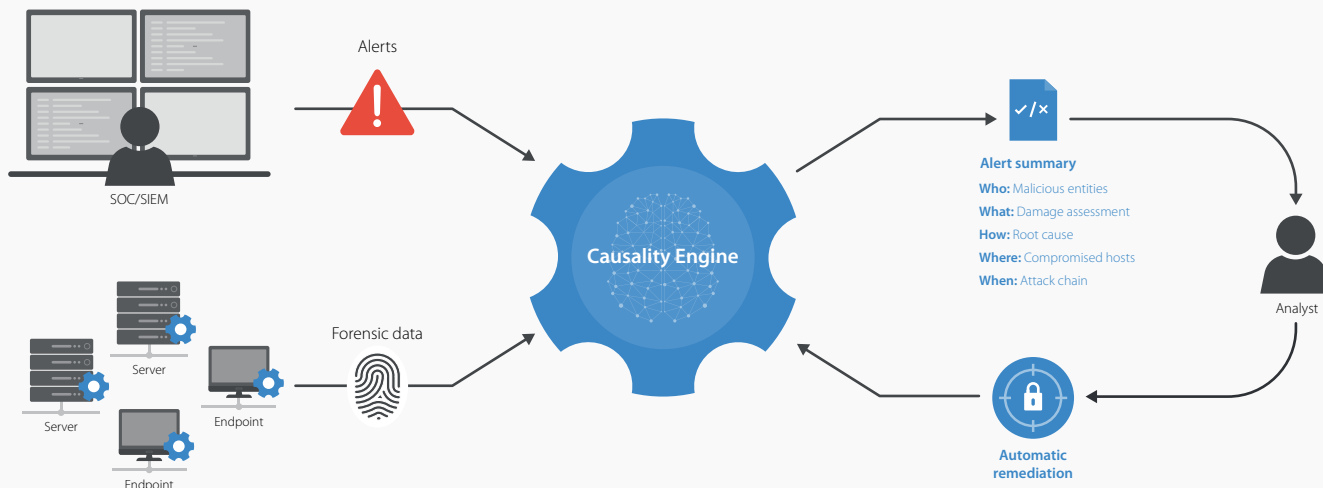
Automatic investigation allows SOC/IR teams to process many times more alerts with less expertise required

Rapid, remote remediation without impact on business continuity

Precise response and remediation are accomplished without disrupting users

Future attacks prevented

Root cause and the attack chain of every incident is revealed, so gaps in defenses can be closed



ANALYZER: AUTOMATIC ALERT INVESTIGATION

SECDO's Causality Analysis Engine™ continuously and automatically analyzes billions of historical host events to identify the causality chain behind every threat. As alerts from SIEM and detection systems are triggered, they are automatically correlated with the historical host forensic data, instantly revealing the full context of the alert. Analysts get conclusive answers and immediately understand the “who, what, where, when and how” behind each alert.



Visual analysis of any alert including a visual timeline of the attack chain back to the root cause, entities involved, affected hosts, behaviors and damage assessment



Automatic SIEM alert investigation through a bi-directional integration with leading SIEM systems, SECDO automatically and instantly investigates and validates every alert

RESPONDER: RAPID, SURGICAL RESPONSE & REMEDIATION

Responder includes a granular set of effective response tools, enabling rapid, remote and precise containment and remediation of actual threats. Security analysts and IT can remotely view, retrieve, assess, isolate, contain and delete individual processes/threads on any host from a single pane of glass. Users can continue to work while investigation and remediation take place.



IceBlock™ freezes execution chains in memory. Users can continue to work safely while the malicious process is frozen



Live Remote Terminal allows analysts and IT personnel to run commands and code interactively (Python, PowerShell, etc.) on any host



Complex response scripts and scenarios can be built without having to install Python on the endpoint



Isolation quarantines infected hosts from the network while allowing secure, remote access and prompt remediation



Live Forensics enables analysts to collect memory dumps and perform memory forensics remotely



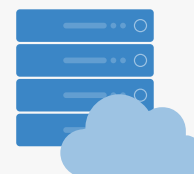
Automatable Response enables building of new rules and security policies for inclusion in Observer and Analyzer

SPECIFICATIONS



AGENT

- **Operating systems:** Windows, Linux
- **Resources:** Less than 0.1% CPU, 30MB RAM
- **Network:** <5MB of network traffic per day
- **Tamper-proof:** Kernel-level memory and file system self-protect
- **Operation:** Stealth-mode
- **Deployment:** Silent
- **Visibility:** Thread-level
- **Data collection:** All activity from user, file, memory, process, thread, registry, network, USB
- **Communications:** SSL encrypted



SERVER

- **Operating system:** Linux
- **Scalability:** Unlimited (cluster-based)
- **Deployment:** On-prem or cloud
- **Records:** All data from all hosts stored securely for years