AUTOMATED ENDPOINT SECURITY AND INCIDENT RESPONSE

Supercharging Security Operations & IR Teams

THE REALITY OF SECURITY OPERATIONS

Security teams are in a constant battle, overwhelmed by security alerts, restricted by staffing and burdened by tools that lack insight into either external or insider threats. These realities force teams to be reactive in nature, focusing only on a portion of priority alerts and then being reliant on time-consuming, manual investigative techniques for analysis. It is little wonder that the average discovery (MTTD) and recovery (MTTR) time of an actual breach are 99 and 66 days, respectively[1].

The best effort for resolving these realities by most security-system vendors is by maintaining a 30-day record of process activity coupled with limited remediation capabilities via an endpoint detection and response (EDR) solution. However, this is not a solution, rather an expensive and underpowered microscope that is usable only by experienced incident responders who can make sense of the recording—and only if the threat is discovered within 30 days and not 99.

SECDO GOES WAY BEYOND EDR

No other solution combines EDR with security automation and artificial intelligence (AI) to reduce the investigation and response time required at each stage of security operations, from alert triage to threat detection to incident resolution. Secdo makes this possible by integrating its leading endpoint data collection and patented Causality Analysis Engine™ with SIEM and other threat-detection technologies to automatically investigate each incoming security alert within seconds.

Only Secdo can multiply the current rate[2] of alert resolution by 10-100x, empower less-experienced security analysts to be as accurate as seasoned experts, and enable advanced threat hunting that learns from its results to prevent future threats, continuously reducing the risk of successful breaches.

[1] Mandiant - M-TRENDS® 2017: A View From the Front Lines

[2] Data from Secdo customer usage

Business Benefits

Improve Security Posture Quantifiably
Decrease the number of alerts immediately and prevent related attacks in the future

Stop Alert Fatigue and Attrition
Increase analyst capability and morale by noticeably reducing the alert backlog

Customize Detection and Prevention
Close the attack vectors that are unique to your network

Increase ROI from Current Resources
Improve the efficiency and effectiveness of current staff, processes and tools

Reduce Mean Time To Discovery (MTTD) by 98%
Validate security alerts in seconds allowing hundreds to be reviewed per day

Reduce Mean Time To Recovery (MTTR) by 97%
Respond to external and insider threats with actionable information provided in seconds

Reduce Business Risk
Build a proactive defense that stops incidents from becoming data breaches

Use Cases

- Automated alert investigation
- Root cause analysis
- Incident Response
- Incident containment and recovery
- Post-incident impact analysis
- Insider-threat detection
- External threat detection
- Threat hunting
- IOC and Threat Intelligence searches
- Policy assessment and hardening
- File-less attack protection
- Ransomware protection
- Custom prevention
- Application control

SECDO

E info@secdo.com T 917.338.2277 www.secdo.com

Key Capabilities

Thread-level host visibility

Storing all endpoint activity for 100+ days time

Secdo's lightweight agent continuously collects all endpoint activity at the thread-level, storing it in a secured server on-premise or in a private cloud. Secdo collects the widest breadth of data even beyond malware to discern insider threats, business risk, application risk, user activity, policy violations, system/file attribute violations, and more.

Automated alert investigation

Revealing root cause of every alert from any source in seconds

Secdo ingests alerts from any source (including any SIEM), and automatically correlates the alerts with the historical endpoint data. For each alert, the root cause is instantly revealed, malicious entities are reputation-checked and the scope is assessed, so even a junior analyst can easily validate any alert.

Scalable response and remediation

Providing the widest toolset of remote, precise response tools

Secdo provides the broadest range of remote response actions including containment (freeze applications and threads, etc.), remediation (quarantine, kill process, etc.), forensics (web-based remote terminal to run shell, etc.) and enforcement tools (blacklist processes and IPs, etc.). The Secdo Response Center enables IT and security teams to apply any action to individual endpoints or across all endpoints at once and add signatures for immediate protection.

Adaptive defense

Applying behavior-based IOCs to catch future attacks

With Secdo, security teams can apply the learnings from previous investigations to defend against future attacks, shifting from reactive to proactive defense. Analysts can create behavioral indicators of compromise (BIOCs) rules that look for the attack method/vector used, and detect it any time this event occurs, creating an alert and if required, automatically containing it.

Limitless threat hunting

Hunting for external and file-less attacks, insider threats and more

With Secdo's unmatched endpoint visibility, security teams can hunt for any type of attack: External threats and file-less attacks, insider threats or malicious insiders, policy audits and violations, and compliance audits.

Operational Benefits

Increase the Number of Alerts Handled by 10-100x
Deplete the backlog by analyzing every alert

Eradicate False-Positive Security Alerts
Directly apply learnings from automated investigations of alerts to refine policies, decreasing noise and risk

Slash Time from Triage to Response to Minutes
Build an efficient operations team that achieves alert triage to full recovery from a single console

Remediate Effectively without Business Interruption
Respond with surgical precision to remove threat actors and implement future preventions without disrupting user or system productivity

Detect and Respond to Any Threat
Protect the network against malicious insiders, policy violations, external threats, ransomware, file-less and memory-only attacks, and advanced, zero-day malware

Reduce Reliance on External Teams
Utilize in-house staff to defend the network from pro-actively hunting for threats to permanently closing vulnerabilities

Tech Specs

Delivery Model
On-Prem / Private Cloud / Hybrid

Scale
Over 300,000 endpoints

Retention
100 days minimum storage of endpoint data

Deployment
Silent

Communication
SSL encrypted

Agent & Network Resources
< 1% CPU, 50 MB RAM
< 7 MB of network traffic / day

Windows | Mac | Linux

E info@secdo.com T 917.338.2277 www.secdo.com