Nominee: Secdo

Nomination title: Automated Endpoint Security and Incident Response

Secdo Automated Endpoint Security and Incident Response software modernizes the defense of endpoints with the steady collection of all activities and actions at the endpoint and server level. The product's Causality Analysis Engine(TM) continuously and automatically analyzes billions of historical endpoint transactions to identify the chain of events associated with any sub-process, host, user, connection or file, and the causality chain behind every threat. The solution then provides remedies and can be taught to catch similar threats in the future.

Secdo takes automated incident response to the next level for the enterprise by offering the following advantages:

1) Powerful protection of network endpoints: Thread level visibility across all endpoints, threat hunting, insider threat auditing, alert integration, automated investigation, risk assessment, pre-emptive defense, containment, forensics, enforcement, and surgical remediation.

2) Behavioral Based Indicators of Compromise (BIOC) technology: This allows analysts at any expertise level to configure and tune BIOC rules and optimize the ongoing detection of recurring attacks in the enterprise. The feature blocks malicious activities and behavioral patterns as well as other harmful processes before they can do damage to the organization.

3) Fast and accurate incident response: The Secdo Response Center includes a comprehensive response portfolio that supports security administrators responsible for responding to an endpoint attack with many more options to choose from so a response that is most appropriate for the incident can be deployed.

The features in Secdo Automated Endpoint Security and Incident Response software provide a first-time solution for security teams to customize BIOCs to catch threats based on their specific environment in order to trigger an automated response any time these behaviors are spotted. This capability is especially important when new vulnerabilities are found – as analysts can immediately create a BIOC to automatically catch and remediate the new threat even before a patch is deployed. This drastically reduces the 'cat and mouse' game that IT and cyber security teams are engaged when it comes to the deployments of patches.

Why nominee should win

- Scalable & Surgical Remediation - Quarantining, terminating a process, deleting a file, deleting and modifying registry keys, stopping a service/driver, removing user accounts, etc.

- Containment – Endpoint and process freezing/unfreezing (IceBlockTM), endpoint isolation, disable user accounts, etc.

- Forensics - Live terminal, live PowerShell, live Python, dump process memory, dump process strings, grab screenshot, upload tools, download files, etc.

- Enforcement - Blacklist processes, whitelist processes, blacklist IP/host, custom playbook actions on IOCs and Behavioral IOCs, etc.

- Notification - Create alerts, send alerts to the SIEM, send email, etc.