

SOURCETEKIT VS CROWDSTRIKE

COMPETITIVE ANALYSIS



**FOR MORE INFORMATION
CONTACT US**



THE SOURCETEKIT DIFFERENCE

Detailed Explanation



ATTACK PREVENTION & DETECTION

Malicious activity manifests itself in one of three ways: file/process execution, network traffic and user behavior. CROWDSTRIKE is oriented on file/process-based threats: malware, exploits, file less, Macros etc., and typically gain good results on that field. However, CROWDSTRIKE lacks the ability to identify and block attacks that manifests only in anomalous network traffic (lateral movement, data exfiltration and network-based credential theft) or user behavior (anomalous login of compromised user account).

SourcetekIT uses Proprietary technology to continuously collect and analyze endpoint, user and network activities within the protected environment, powering the ability to identify and block both file / process-based attacks, as well network and user-based ones, rendering complete coverage beyond the capabilities of CROWDSTRIKE.

Moreover, by fusing together all the environment activity signals, SourcetekIT is able to form the true context of each process execution network traffic and user behavior to unveil and block threats that are undetectable by monitoring just file/processes as CROWDSTRIKE does. In that way, SourcetekIT would successfully block the execution of processes that CROWDSTRIKE allows to run.



THE SOURCETEKIT DIFFERENCE

Detailed Explanation

RESPONSE

Coverage

Advanced cyberattacks leave their mark across all parts of the targeted environment: endpoints, files, process, user accounts and network traffic.

Unlike CROWDSTRIKE that has a limited number of endpoints/file remediations (isolate, kill process and delete/quarantine file), SourcetekIT uses Proprietary technology to provide a complete set of remediation tools for infected endpoints, malicious files/ processes, compromised user accounts and attacker-controlled traffic. Moreover, SourcetekIT can act as a response orchestration interface that communicates with core components such as Firewalls and Active Directory to expand the response process across the entire environment.

Automation

SourcetekIT supports the use of pre-set and user-created remediation playbooks that automate response for detected threats by chaining together several discreet remediation actions (for example, isolate the endpoint + disable user account in Active Directory as an automated response user account compromise detection). These playbooks both scale the security team alert-handling capacity by automating repetitive tasks and radically increase the share of attacks that are autonomously addressed and resolved by SourcetekIT without need of human intervention.

MONITORING & CONTROL

Continuous monitoring of all entities and activities in the environment enables users to discover exposed attack surfaces and address them (vulnerable systems and apps, unchanged user passwords, etc.), and by that eliminate the risk of up to 60% of common attack vectors.

SourcetekIT uses Proprietary technology to automate the collection and correlation of executed file/processes, user account activities, file access and network traffic, introducing unmatched speed and ease to all monitoring and control workflows.



SOURCEKIT VS CROWDSTRIKE COMPARISON TABLE



PREVENTION & DETECTION



Multi Layered Malware Protection

ML Based Static Analysis



Compromised User Account Detection

Anomalous User Logins



Pre-set User Activity Rules



Malicious Insider

Credential Theft (LLNMR\NBT-NS Attacks)



Lateral Movement (Pass The Hash etc.)



Reconnaissance (Scanning Attacks)





SOURCEKIT VS CROWDSTRIKE COMPARISON TABLE



Deception

Decoys: Data Files, Credentials, Network Shares, URL, RDP



RESPONSE

Host Remediation

Isolate, Restart, Change IP, Delete/Disable Service, Delete/Disable Scheduled Task, Run Command, Run Script

Isolate, Run Command, Run Script.

User Remediation

Disable/Enable, Reset Password



Network Remediation

Block Traffic, Clear DNS Cache



Orchestration

Expand remediation across the environment infrastructure: firewall, proxy, AD, etc.



Automation

Chain discreet remediation actions to a single flow that runs automatically when a predefined alert is triggered





SOURCEKIT VS CROWDSTRIKE COMPARISON TABLE



INFRASTRUCTURE

OS Support

Windows XP P2 and above, Server 2003 and above Linux, Mac

Windows 7 and above, Server 2008 and above, Mac OS El Capitan and above, Linux

Deployment Model

Flexible: on-prem, SaaS or Hybrid

SaaS only

Self-Distributing Agent

Auto-deployment on newly joined endpoints without need of manual configuration



Clashes with Existing Software, Manual Exclusions, Blue Screens



Monitoring & Control

Full MDR Integrated in the Product Offering



Full MDR Integrated in the Product Offering

