DATASHEET

SECDO

RANSOMWARE SOLUTION

SECDO DETECTS, BLOCKS AND REMEDIATES RANSOMWARE ATTACKS.

WITH CUTTING-EDGE DECEPTION TECHNOLOGY, SECDO TRICKS RANSOMWARE INTO REVEALING ITSELF, THEN FREEZES THE RANSOMWARE BEFORE FILES ARE ENCRYPTED. USING THE SECDO PLATFORM, YOU CAN THEN INVESTIGATE AND REMEDIATE THE THREAT BOTH ON THE AFFECTED ENDPOINT, AND ACROSS THE ENTIRE ORGANIZATION.

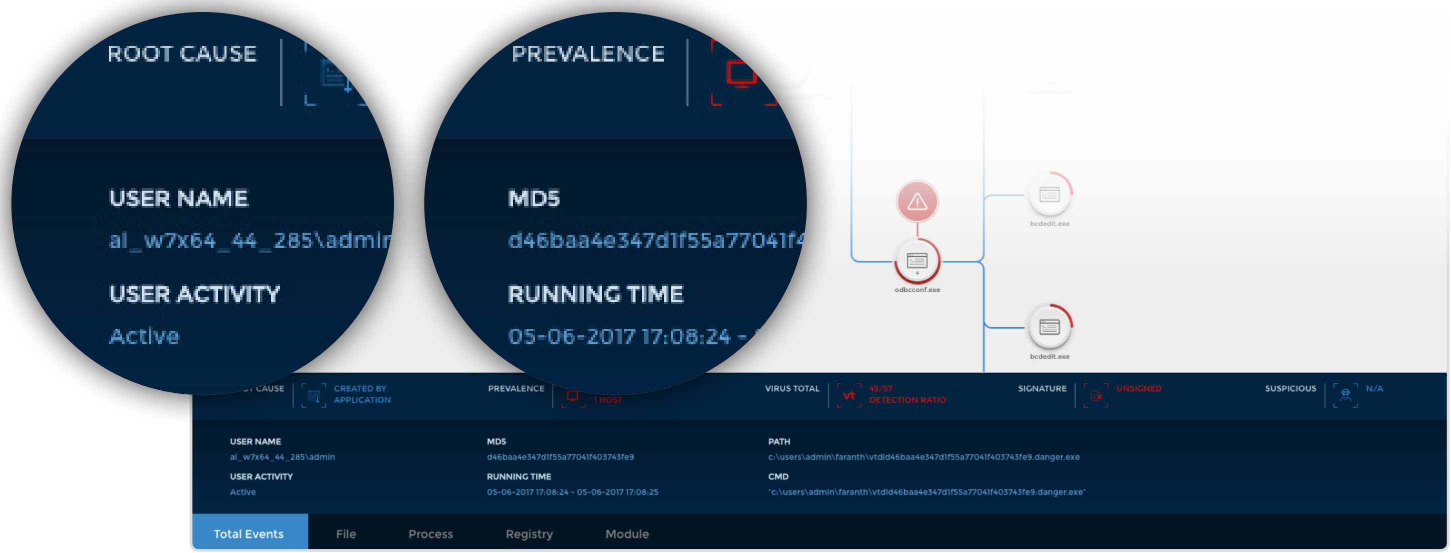
WHY WORRY ABOUT RANSOMWARE?

The frequency and sophistication of ransomware attacks are growing rapidly. Like other types of advanced malware, ransomware avoids conventional endpoint protection, and has already caused hundreds of millions of dollars in damage. To increase the stakes, hackers are now targeting hospitals, schools, banks and other organizations that cannot afford to shut down operations.

Since ransomware is so destructive, it is essential to detect and stop it quickly, before files are encrypted. That is easier said than done, since ransomware uses evasion, reconnaissance and stealth tactics to detect and avoid or disable security solutions.

KEY FEATURES

- **Block ransomware before files are encrypted**
- **Surgically contain the attack with minimum disruption**
- **Investigate and remediate across the enterprise**
- **Future-proof – not dependent on the attack vector**
- **No false positives**



USER NAME
al_w7x64_44_285\admin

USER ACTIVITY
Active

MD5
d46baa4e347d1f55a77041f403743fe9

RUNNING TIME
05-06-2017 17:08:24 - 05-06-2017 17:08:25

PATH
c:\users\admin\faranth\vtdld46baa4e347d1f55a77041f403743fe9.danger.exe

CMD
"c:\users\admin\faranth\vtdld46baa4e347d1f55a77041f403743fe9.danger.exe"

A COMPLETE SOLUTION FOR RANSOMWARE

Detecting ransomware is important, but it is not enough. While ransomware is dormant, it often spreads to other endpoints, shared folders, or backups. It can wait in silence as it spreads throughout the network and prepares to attack. To root out the infection and ensure that it doesn't reappear after files are restored, you need a solution that not only detects and contains ransomware, but tracks it down and removes it from the entire network.

The SECDO platform includes detection and prevention of ransomware, remediation of affected endpoints, and a complete forensic investigation of the incident.

HOW IT WORKS

1

SECDO uses proprietary deception technology to force ransomware to reveal itself before files can be encrypted.

The deception is effective regardless of the method the ransomware used to penetrate the organization.

2

Once the ransomware is revealed, ***IceBlock™ freezes the malicious processes and threads and prevents any further damage.*** This surgical approach enables users to work, leaving the rest of the endpoint functional until IT has an opportunity to handle the incident.

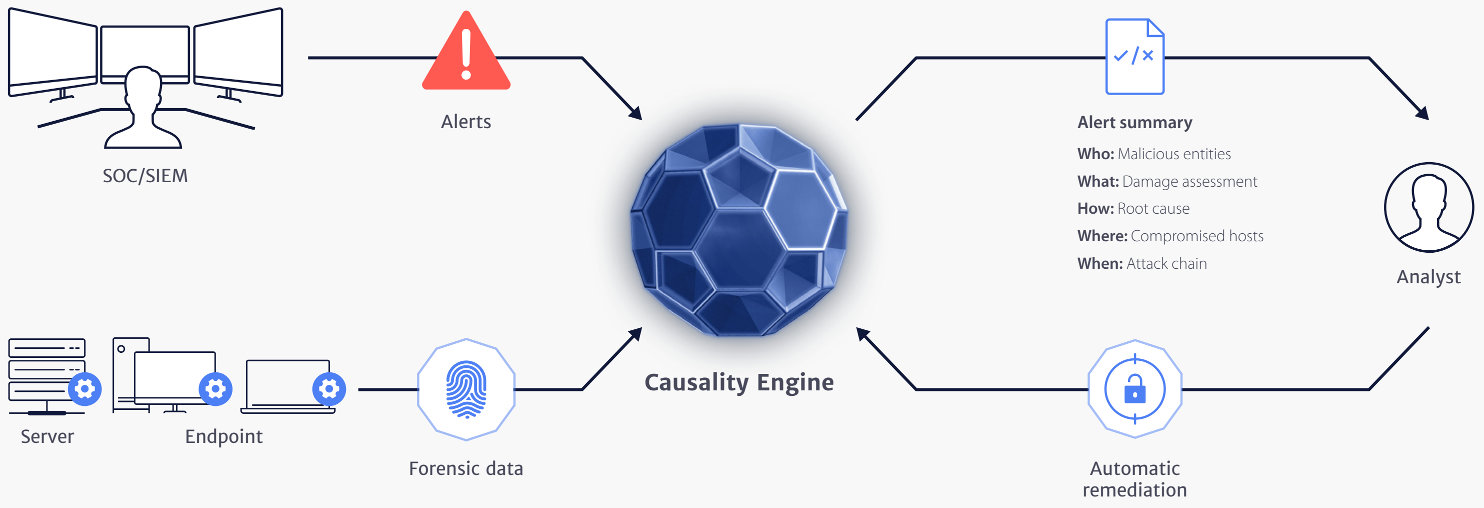
3

SECDO reveals the root cause as well as the entire attack chain and all behaviors of the ransomware on the endpoint and immediately alerts the security team.

4

Analysts can also perform forensic analysis on any of the endpoints and servers in the organization using SECDO's visual investigation platform.

Since the SECDO agent continually records endpoint activity and stores it for 100 days, analysts have direct access to historical endpoint data and can perform further investigations.


SOC/SIEM
Alerts
Causality Engine
Alert summary
Who: Malicious entities
What: Damage assessment
How: Root cause
Where: Compromised hosts
When: Attack chain
Analyst
Server
Endpoint
Forensic data
Automatic remediation