stealthDEFEND

STEALTHDEFEND® FOR ACTIVE DIRECTORY

Real-time detection and response for threats against Active Directory

stealthbits
NOW PART OF netwrix

Active Directory (AD) provides a wealth of information about the users within an organization, groups used to secure access, network topology, applications hosted, and overall security policies. The same information used to benefit trusted users and systems within the network can also provide attackers with detailed schematics of an organization, retrievable from any compromised system.

Today's cybersecurity attacks are substantially more sophisticated than in years past, requiring a different approach as we now operate under the assumption of a breach. Our new job is to identify an attacker who is hiding all of their activity as a valid user, hidden among all other activity coming from systems managed by IT operations.

What is StealthDEFEND for Active Directory?

StealthDEFEND is a real-time threat detection and response solution for attacks against an organization's credentials and data. StealthDEFEND consumes an enriched, optimized audit stream of data including all authentications, changes, and requests occurring within Active Directory. StealthDEFEND effectively builds organizational behavioral profiles using unsupervised machine learning algorithms. The result is the ability to detect abnormal and advanced attack behaviors with unprecedented accuracy.

"Companies that identified a breach in **less than 100 days saved more than $1M** compared to those that took more"

(Source: 2018 VDBIR)

"68% of breaches **took months or longer to discover**"

(Source: 2018 VDBIR)

"The insider threat is difficult to guard against - **it's hard to spot the signs if someone is using their legitimate access** to your data"

(Source: 2018 VDBIR)

KEY BENEFITS

Simplified Advanced Threat Detection

Advanced attacks against AD are highly complicated, which is why StealthDEFEND is designed to take the guesswork out of the equation.

Reduced Time to Detection

StealthDEFEND focuses on helping organizations reduce time to detect and contain breaches.

Best Practice Alignment

25% of breaches are a result of user error that goes undetected according to the 2018 VDBIR. StealthDEFEND identifies activities that don't follow best practices for security teams to evaluate and respond to.

Increased Efficiency

Built-in integration with the market's leading SIEM solutions and other popular technologies such as ServiceNow, Slack, and Microsoft Teams ensures threat data resides in the places you need and want it most

Instant Awareness

Truly real-time alerts are triggered instantly and can be delivered in a variety of ways, including email, integration with SIEM via syslog, or other relevant technologies.

KEY FEATURES OF StealthDEFEND FOR ACTIVE DIRECTORY

Response Playbooks

StealthDEFEND provides automated response options when threats are identified and can trigger follow-up responses based on initial playbook success or failure. In addition to an extensive catalog of preconfigured response actions, StealthDEFEND can be configured to integrate with your own business processes using PowerShell or webhook facilities.

StealthDEFEND can also deliver threat data to administrators in their preferred applications, including ServiceNow, Slack, Microsoft Teams and a wide variety of SIEM platforms.

Machine Learning & User Behavior Analytics (UBA)

Identifies outlier activity as compared to the behavior profile created by the unsupervised learning engine. This allows a large amount of events to be analyzed and suspicious behaviors to be elevated for review automatically

Deception Tools

Proactively lure attackers into making the wrong move with built-in honeypot deployment, management, and detection

Automated Context Injection

By default, StealthDEFEND automatically monitors privileged built-in users, groups, and members of those groups as sensitive, adding valuable context to the analysis and alerting it performs

Comprehensive Investigations

An attack is frequently a collection of related activities that tell a larger story. StealthDEFEND pulls together all related events to allow administrators to perform comprehensive investigations for forensic compilation of digital case files

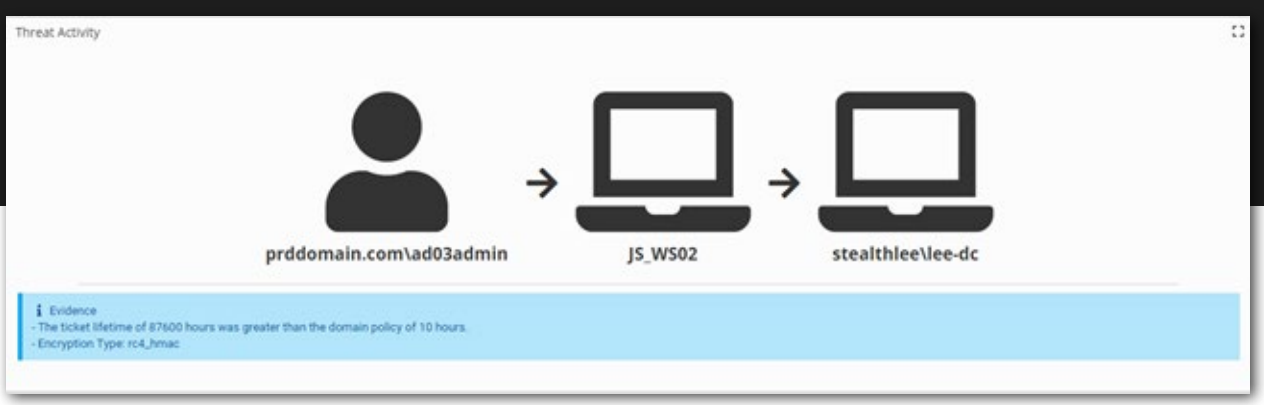
User-Defined Threats

A threat solutions needs to be flexible in order to provide the most value. StealthDEFEND allows administrators to easily add new threats that align to their organization's specific requirements

ADVANCED ATTACKS

StealthDEFEND detects and responds to specific tactics, techniques, and procedures that attackers leverage to compromise AD:

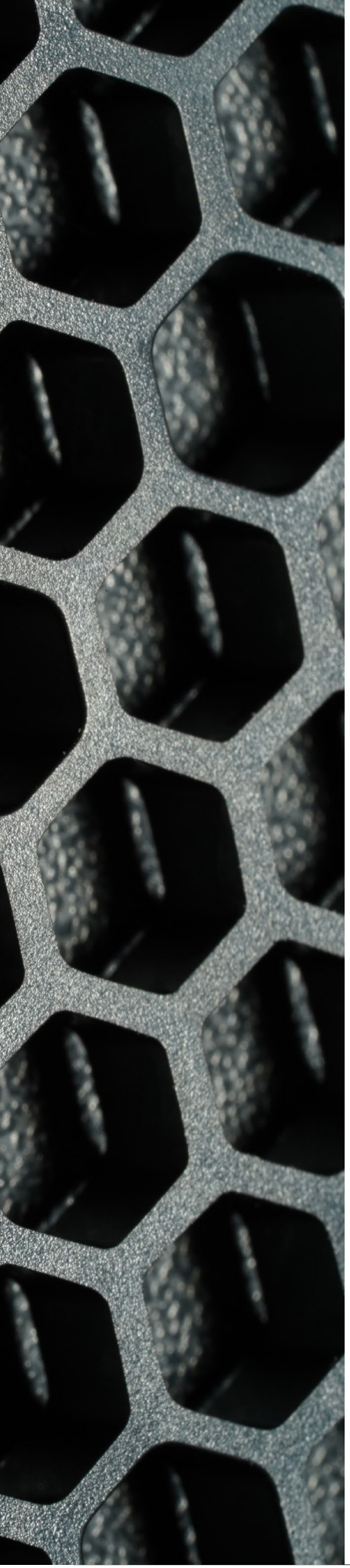
- DCShadow
- DCSync
- Golden Ticket
- Kerberoasting
- LSASS Process Injection
- Password Spraying
- Replication Permissions Tampering
- AdminSDHolder ACL Tampering
- Pass-the-Ticket
- Group Managed Service Account (GMSA) Exploitation
- Forged PAC
- LDAP Reconnaissance
- NTDS.dit Password Extraction
- Plaintext Password Extraction – Group Policy Preferences
- Silver Ticket
- SID History Tampering



ABNORMAL BEHAVIOR AND SECURITY EVENTS

StealthDEFEND has been designed to detect suspicious and outlier activities, as well as actions that violate AD Security Best Practices, including:

- Abnormal Behavior (e.g. Anomalous authentications, including indicators of pass-the-hash activity)
- Hidden Object
- Insecure UAC Change
- Exposed Admin Credentials
- Sensitive Group Changes
- Service Account Misuse
- SID History Tampering



NEXT STEPS

Schedule a demo
stealthbits.com/demo

Download a free trial
stealthbits.com/free-trial

Contact us
info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix