KuppingerCole Report

EXECUTIVE VIEW

by Mike Small | May 2018

StealthDEFEND®

Cyber-attacks often involve a complex process, including an insider threat element, which exploits compromised or illicit user credentials to gain access to data. StealthDEFEND is the real time file and data threat analytics component of the STEALTHbits' Data Access Governance Suite.

by **Mike Small**
mike.small@kuppingercole.com
Mai 2018

Content

Related Research Documents

Advisory Note: Real Time Security Intelligence - 71033

Blog: Real-time Security Intelligence – more than just "next generation SIEM"

Leadership Compass: Privilege Management - 72330

Executive View: STEALTHbits® Products Overview - 70270

Advisory Note: Redefining Access Governance - Beyond annual recertification - 72529

Advisory Note: Understanding and Countering Ransomware - 70282

Survey: State of Organizations: Does Their IAM Meet Their Needs in the Age of Digital Transformation? - 74003

Leadership Brief: How to close the skill gap in your Cyber Defense Center - 72800

1 Introduction

Detecting and managing attacks on IT systems is a serious problem. Cyber criminals are using increasingly sophisticated techniques to infiltrate organizational IT systems to commit crimes including data theft, denial of service and blackmail. However, statistics show most data breaches are detected by agents outside of the organization rather than internal security tools.

Traditional perimeter security devices like firewalls, IDS (Intrusion Detections Systems) and IPS (Intrusion Prevention Systems) are widely deployed. These tools are effective at controlling certain kinds of weaknesses for known threats, patterns and signatures. They also generate alerts when suspicious events occur; however, the volume of these events is such that it is almost impossible to investigate each as they occur. While these devices remain an essential part of the defence for the agile connected business, they are not able to detect a range of threats including the use of compromised credentials, insider threats, data exfiltration, access misuse and zero-day attacks.

SIEM (Security Information and Event Management) is often promoted as a solution to these problems. However, SIEM is just a set of tools that can be configured and used to analyse event data after the fact and to produce reports for auditing and compliance purposes. While SIEM is a core security technology it has not been successful at providing actionable security intelligence in time to avert loss or damage.

External attacks now involve a complex process, often including an element of social engineering, which exploits compromised or illicit user credentials to gain access to data. This is partly because of the strength of conventional network defences against direct frontal attack, and also because the use of apparently legitimate credentials bypasses other security controls like encryption. Furthermore, insider threats continue to be a real problem and these invariably involve the misuse of access rights. For these reasons identity and access controls have become the new perimeter.

The most effective way of detecting illegitimate access to data is through the monitoring of user identity, access and activity. Even more importantly, better access governance is essential to reduce the risks of data theft. Some traditional SIEM vendors are starting to include analysis of user activity logs in their products. However, recognizing what is abnormal versus normal remains a problem. Big Data machine learning technology provides a potential solution to this by identifying identity, access and activity patterns that are common among peer groups of users.

What is needed is the integration of user identity, access and activity analysis into cyber-defence to enhance threat prediction and detection as well as to enable remedial action to be taken before damage is done. This requires techniques taken from big data infrastructure and business intelligence machine learning to analyse the massive amount and variety of data from the many sources to raise alarms only where there is a high confidence that the threat from the anomalies detected is real.

The volume of threats to IT systems, their potential impact and the challenges in discriminating between real threats and false alarms are the reasons why a new approach is needed. The need to calibrate what is normal to reduce the signal-to-noise ratio in order to detect anomalies remains a challenge and accomplishing this using bespoke rules within some tools requires considerable skill. It is important to look for a solution that can easily build on the knowledge and experience of the IT security community, vendors, and service providers. End user organizations should always opt for solutions that include managed services and pre-configured analytics, not just bare tools.

2 Product Description

STEALTHbits Technologies is a privately held software company with its head office in Hawthorne NJ in the USA. The company is focused on protecting organizational credentials and data. Its products focus on removing inappropriate data access, enforcing security policy, and detecting cyber threats to reduce security risk, to fulfil compliance requirements and to decrease operational costs.

This report covers StealthDEFEND®. This is one of a suite of products designed to address IT security risks, compliance requirements, and day-to-day management functions spanning Data Access Governance, Active Directory Management & Security, and Threat Detection.

2.1 STEALTHbits Products Overview

STEALTHbits provides several products to support credential and data security processes for a range of environments. The products include:

- StealthAUDIT®: Automated data collection, analysis, and governance;
- STEALTHbits Activity Monitor: monitors and stores machine and user activity;
- StealthDEFEND®: Real-time threat analytics and alerting;
- StealthINTERCEPT®: Real-time policy enforcement, change & access monitoring and Active Directory Security;
- StealthRECOVER®: Rollback and recovery of unwanted Active Directory changes.

2.2 StealthDEFEND®

StealthDEFEND is the real-time threat analytics component of STEALTHbits' Data Access Governance Suite. It uses data from STEALTHbits Activity Monitor and unsupervised Machine Learning to detect threats to files and data as they occur.

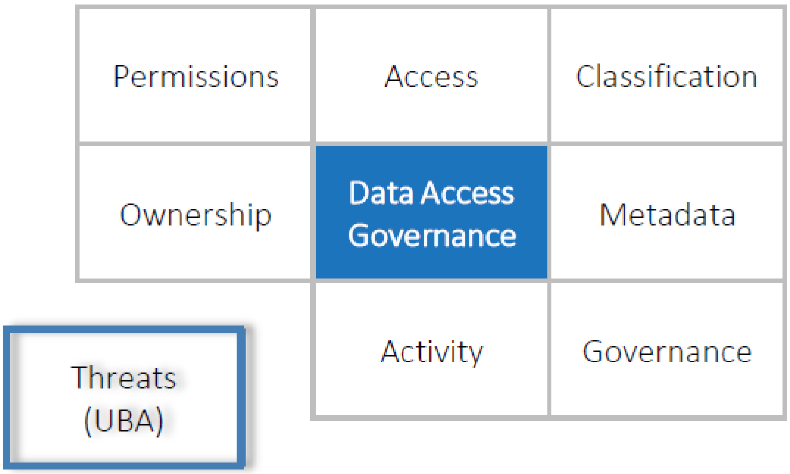

Figure 1: StealthDEFEND as part of STEALTHbits' Data Access Governance

StealthDEFEND employs unsupervised Machine Learning technology that can detect patterns not discernible through summary statistical analysis. It is based on a scalable architecture that enables real-time detection of abnormal and nefarious activities – regardless of where they originate from - inside or outside the organizational network.

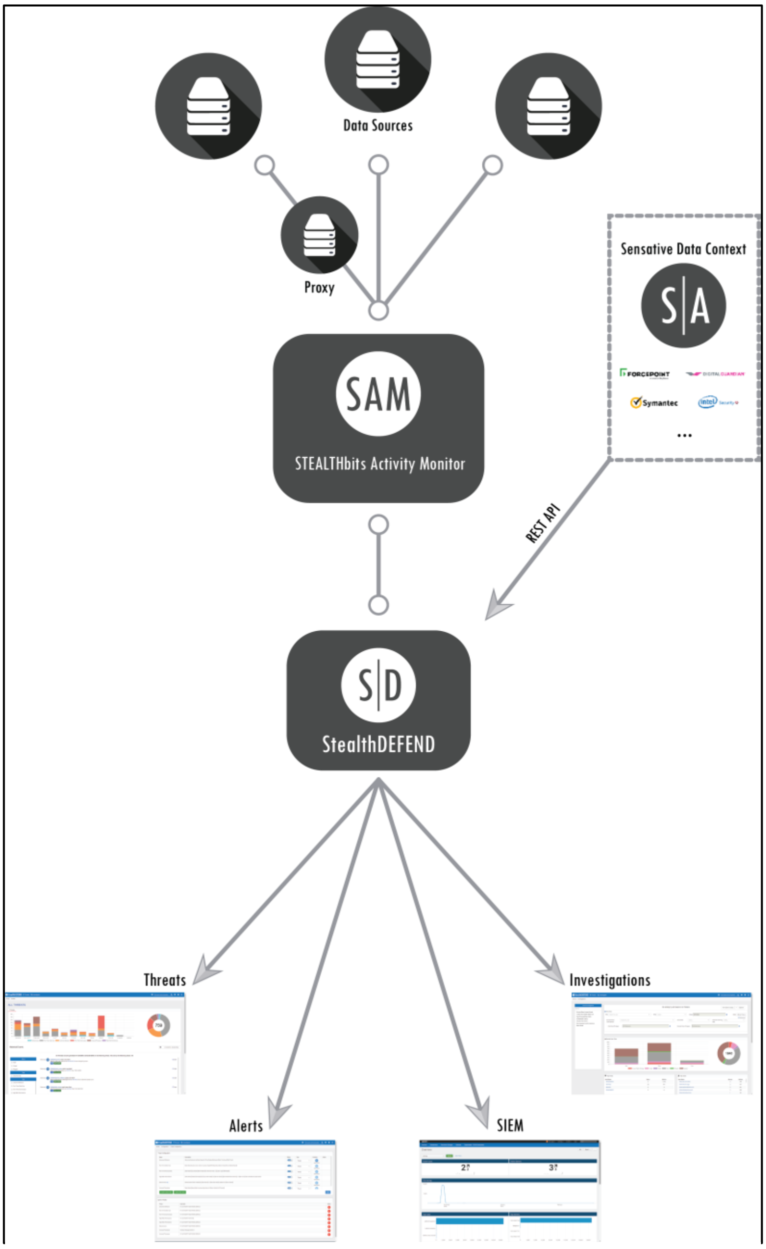

Figure 2: StealthDEFEND Architecture (reproduced with permission from STEALTHbits)

An overview of the StealthDEFEND architecture and functionality is shown in Figure 2.

StealthDEFEND Key features include:

- Unsupervised Machine Learning – StealthDEFEND incorporates Machine Learning models to evaluate, correlate, and baseline the activity and behaviour of users. This improves threat detection while reducing false positives;
- Sensitivity of Data – by focussing on files that matter most using information from data governance and threats reduces the noise while increasing effectiveness;
- Preconfigured Threat Models – StealthDEFEND includes out-of-the-box predefined threat models that align with common attack patterns. These include patterns to detect file system threats associated with Ransomware, Abnormal User Behaviour, First Time Host Access, First Time Client Use, Unusual Processes;
- User Behavioural Profiles – StealthDEFEND's threat analytics and Machine Learning models incorporate an understanding of each user's individual behaviour. This is complemented by visualizations that help the analyst to understand the normal behaviour of any user;
- Investigation Tools – enable the analyst to create, configure, investigate and save detailed reports on suspicious behaviour. These can also be used to detect and alert on future occurrences of similar behaviour;

- SIEM Integration – StealthDEFEND can automatically send data on threats it has identified to an SIEM solution in real-time for consolidated alerting. It can also help to reduce the load on SIEM tools by only sending data on identified threats;
- Real-Time Alerting – StealthDEFEND can be configured to alert any group of people to identified threats in real-time;
- Interactive, Real-Time Visualizations – threat data is streamed, processed, and visualized as it happens through a unified web presentation layer. These visualizations include dashboards with elements like heat maps that update themselves in real-time to bring data to life.
- Incident Detection Response Workflow – StealthDEFEND includes a workflow that helps to coordinate the work of the threat response team to share information and track who is working on an issue at any given time.

By incorporating file activity details in conjunction with the context of each file's sensitivity, StealthDEFEND aims to highlight abnormal behaviours that are likely to be Indicators of Compromise (IOCs) such as:

- Crypto Ransomware;
- Abnormal user behaviour;
- First-time access to data resources;
- Suspicious encryption activity
- Unusual access to sensitive data;
- Abnormal denied activity;
- Suspicious changes to permission;
- Attempts to exfiltrate data;
- Tampering with configuration files;
- Mass file deletions.

3 Strengths and Challenges

StealthDEFEND provides a useful solution to help detect cyber-threats. Unlike other solutions that focus on network traffic or on technical vulnerabilities this solution focuses on file access activity to detect and prioritize risk. This approach makes sense since most cyber-attacks eventually involve obtaining unauthorized access data through compromised user accounts. Furthermore, abuse and data theft by insiders does not normally involve suspicious network activity.

StealthDEFEND needs to be judged as part of the suite of STEALTHbits products. These provide a comprehensive set of solutions to address IT security risks covering Active Directory, Data Access Governance, Privileged Access Management (PAM), and Threat Detection. StealthDEFEND will be of interest to organizations using this suite of products.

StealthDEFEND enables the discovery of changes to permissions and specifically provides visibility into administrative file system activities. This is especially important since many external threats involve taking control over administrative accounts in addition to the threat of abuse by insiders with administrative privileges.

Monitoring user activity is increasingly important as a component of cyber-defence. Often the first sign of a cyber-attack is abnormal user behaviour. StealthDEFEND User Behaviour Analytics (UBA) exploits machine learning to enable the detection of abnormal user activities while ensuring a low level of false alarms. It also integrates with leading SIEM products out-of-the-box.

The challenge, which is similar to that for a network activity-based approach, is to calibrate what constitutes normal activity. Only then is it possible to accurately identify abnormal patterns and without this calibration the user is either overwhelmed with false alarms or real issues remain undetected. StealthDEFEND solves this problem through the use of machine learning models plus data analytics. The extent to which this can replace professional services and deep knowledge of the tools, tactics and procedures used by cyber-security teams remains to be seen.

To obtain the maximum benefits StealthDEFEND is best deployed in conjunction with other STEALTHbits products.

Strengths	**Challenges**
● Part of a comprehensive suite of solutions; ● Designed to integrate with Microsoft Active Directory as the source of user data; ● Detects suspicious activity to provide alerts in real time; ● Exploits machine learning and data science to provides UBA functionality.	● Effectiveness of machine learning approach needs to be proven for a wide range of security use cases; ● For maximum benefit needs to be deployed in conjunction with STEALTHbits Discovery & Classification solution. ● Needs to form part of a complete cyber-defence approach.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Wilhelmstraße 20-22
65185 Wiesbaden

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com