Data Sheet

StealthINTERCEPT®

Security Information and Event Management (SIEM) Adapter

Security Information and Event Management (SIEM) Adapter

The StealthINTERCEPT® SIEM Adapter provides the ability to feed concise detail regarding change and access events across an organization's Active Directory, Exchange, and file systems to SIEM tool vendors in real time. By distilling change and access activities into individual, complete, self-contained access events, this integration efficiently collects and delivers critical activity information for easy consumption and correlation by SIEM tools. These events are often impractical to collect and make sense of using standard Windows EventLog technology, as they can be extremely disjointed and in some cases incomplete. Additionally, high volume EventLog traffic historically introduces unacceptable overhead to servers that are configured to collect everything. The StealthINTERCEPT® (SI) event collection approach brings to bear deep introspection that has been specifically geared for completeness and efficiency for the specific event types that it collects.

Active Directory Monitoring

Windows Active Directory (AD) is fundamental to controlling access to resources in Windows domains, as well as other environments that have consolidated on AD as a source of managing accounts that are referenced to grant access to critical data resources and applications, as well as key security and configuration settings propagated throughout the environment as Group Policies. By collecting details on changes made to AD as they are made, the SI SIEM Adapter makes available the information of who is changing AD objects that can control critical Group Policies as well as group membership that controls access to critical resources throughout the environment. Additionally, the SI SIEM Adapter tracks direct LDAP (and LDAPS) access to AD to allow identification of non-secure credential exchange, denial of service exposure, directory attacks, and non-Windows application and user access activities.

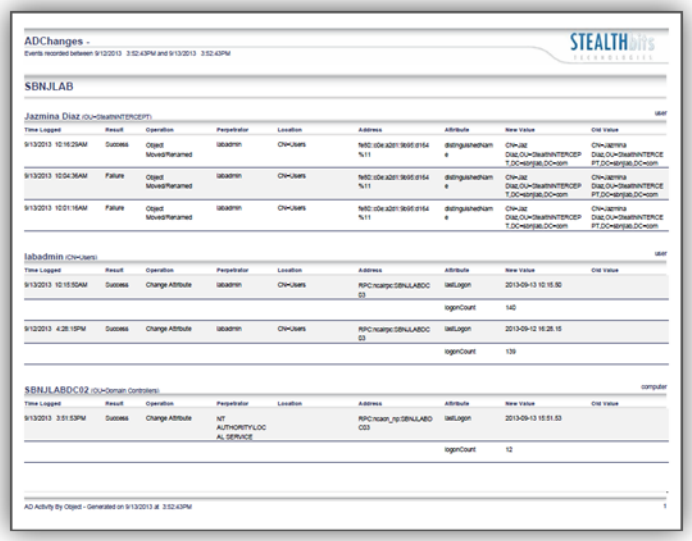
Exchange Monitoring

Access to mailboxes and changes to Microsoft Exchange configuration represent a significant potential for security breaches and organizational issues stemming from visibility to, and redistribution of confidential data. In addition to StealthINTERCEPT®'s capabilities to monitor and prevent configuration changes and access to mailboxes, especially non-owner mailbox access, the SIEM integration relays all information on such activities (allowed and blocked) to the SIEM feed for additional investigation and context.

File System Monitoring

Controlling and auditing access to unstructured data is a constant and growing challenge in industry today. Examples of theft and unauthorized distribution of sensitive data are seen in the press with growing frequency. The StealthINTERCEPT® SIEM Adapter provides insight into user data access patterns and an audit trail to allow early detection of unauthorized and inappropriate accessing of sensitive data. This event detail is of particular interest with the increasingly heightened sensitivity to Privileged Identity Management (PIM) and access control and provides strong synergies in combination with other tools used for control in this space. The monitoring rules

implementation of StealthINTERCEPT® allows simplified and flexible configuration to focus on users, applications, and content of interest without overwhelming the infrastructure with extraneous data.



Integration Features

StealthINTERCEPT® utilizes the industry standard SysLog approach to feed events to SIEM tools. It also provides the ability to further customize to SIEM vendors' formats using a straightforward template approach.

For AD, the Events Detail:

- The user account initiating the change
- The IP address from which the request was made
- The "before and after" values of the object/ attribute being changed
- Changes to Group Policy settings including detail of changed values
- LDAP queries that are run against AD. These include the credentials under which the query was performed and the objects requested by the query. These queries may be generated by applications for multiple purposes and therefore prove to be valuable in filling in the big picture regarding access and control for applications that may run in non-Windows environments, but still utilize AD for configuration or access control. This facility also identifies whether these queries are secured by SSL.
- Advanced use of the tool also provides the ability to block access to specific areas of the tree for specific users. Events are generated for all blocked requests as well as those permitted to complete.

For Exchange, the Events Detail:

- Non-owner mailbox access monitoring and blocking
- Configuration change monitoring and blocking
- Access rights change monitoring and blocking

For Windows File Server and a Variety of NAS systems, the File System Events details:

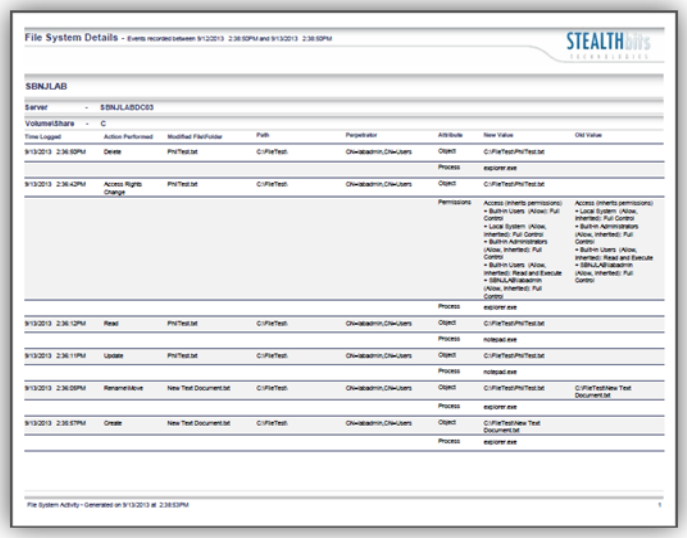
- Read/Write/Create/Delete Permissions Changes on any/all files and folders in scope
- The file or folder on which access as performed and its path
- The process through which the access is accomplished
- The account (user) for which these accesses were performed
- The "before and after" settings with respect to permissions changes on file system objects (on Windows file servers)

Integration Benefits

By extending monitoring visibility for applications and data access configuration changes and file system contents and permissions access, the StealthINTERCEPT® integration provides real savings in terms of identifying and mitigating unauthorized or potentially risky activities in the environment. These savings are realized through expediting awareness (early detection and detailed reporting) of potentially costly issues of inadvertent or malicious changes in access rights (based on groups), global configuration (in the form of GPOs) or access to sensitive data. By identifying and alerting on these situations, appropriate remediation steps can be taken as soon as possible to

prevent or mitigate resultant security fallout or interruption of service to critical applications. This information can also be correlated with network access activity data from the SIEM systems to further pinpoint the source of malicious activities for a more definitive picture of exposures and remediation options.

In addition, this integration facilitates the visualization of Active Directory, Exchange and file systems usage patterns, enabling the formulation of steps to minimize costs that could be incurred when these repositories are moved, migrated, or otherwise caused to become unavailable to critical applications or individuals that rely on them.


File System Details - Events recorded between 9/12/2013 2:38:50PM and 9/13/2013 2:38:50PM

STEALTHbits TECHNOLOGIES

SBNJLAB

Server - SBNJLABDC03

Volume\Share - C

Time Logged	Action Performed	Modified File\Folder	Path	Perpetrator	Attribute	New Value	Old Value
9/13/2013 2:36:50PM	Delete	PhiTest.txt	C:\FileTest\	CN=sbcadmin,CN=Users	Object	C:\FileTest\PhiTest.txt	
					Process	explorer.exe	
9/13/2013 2:36:42PM	Access Rights Change	PhiTest.txt	C:\FileTest\	CN=sbcadmin,CN=Users	Object	C:\FileTest\PhiTest.txt	
					Permissions	Access (inherits permissions): • Built-in Users (Allow): Full Control • Local System (Allow, Inherited): Full Control • Built-in Administrators (Allow, Inherited): Full Control • Built-in Users (Allow, Inherited): Read and Execute • SBNJLAB\sbcadmin (Allow, Inherited): Full Control	Access (inherits permissions): • Local System (Allow, Inherited): Full Control • Built-in Administrators (Allow, Inherited): Full Control • Built-in Users (Allow, Inherited): Read and Execute • SBNJLAB\sbcadmin (Allow, Inherited): Full Control
					Process	explorer.exe	
9/13/2013 2:36:12PM	Read	PhiTest.txt	C:\FileTest\	CN=sbcadmin,CN=Users	Object	C:\FileTest\PhiTest.txt	
					Process	notepad.exe	
9/13/2013 2:36:11PM	Update	PhiTest.txt	C:\FileTest\	CN=sbcadmin,CN=Users	Object	C:\FileTest\PhiTest.txt	
					Process	notepad.exe	
9/13/2013 2:36:08PM	Rename\Move	New Text Document.txt	C:\FileTest\	CN=sbcadmin,CN=Users	Object	C:\FileTest\PhiTest.txt	C:\FileTest\New Text Document.txt
					Process	explorer.exe	
9/13/2013 2:35:57PM	Create	New Text Document.txt	C:\FileTest\	CN=sbcadmin,CN=Users	Object	C:\FileTest\New Text Document.txt	
					Process	explorer.exe	

File System Activity - Generated on 9/13/2013 at 2:38:53PM 1

About STEALTHbits Technologies

STEALTHbits is a data security software company. We help organizations ensure the right people have the right access to the right information. By giving our customers insight into who has access and ownership of their unstructured data, and protecting against malicious access, we reduce security risk, fulfill compliance requirements and decrease operations expense.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com