DIOSTRUX
INSIDER THREAT TOOL

HIGHLIGHTS

- Monitoring behavioral analysis of privileged user activity is critical in fighting Insider Threat.

- Automated solutions that monitor data transfer activity help reduce the strain on human resources, and provides real-time actionable alerts to leadership.

- Solutions that leverage tools already native to the Operating Systems reduce the cost, maintenance, and compatibility concerns that arise with third party products.

- DioStrux provides the DoD community with a flexible option to meet today's complex requirements in a time of constrained budgets and sequestration.

INSIDER THREAT AUTOMATED SOLUTION

BACKGROUND

Unlawful disclosures of classified information have substantially impacted our national security and have required leadership to take a harder look at policies and oversight mechanisms for protecting our nation's most sensitive data. Employees and contractors with boundless privilege to access sensitive data present greater risk of intentionally, accidentally, or indirectly misusing that privilege and potentially stealing, deleting, or modifying data. Humans are often the weakest link in the intersection of people, process, and technology, the three tenants of security.

Privileged users with malicious intent can cripple a closed system faster and more effectively than the external expert could on an open system. The Insider has more time and knowledge of the system and its controls, and is usually not under any suspicion. The Insider often has a network loaded with information that may be stored on removable media. The anonymous misuse of the Insider activities many times goes unnoticed without the presence of effective audit tools, especially those that can detect removal of large data quantities to removable media.

Since 2009, and more recently in July of 2014, United States Cyber Command (USCYBERCOM) mandated multiple requirements for the control of classified data placed on any type of removable device in a directive geared towards Insider Threat Mitigation. The directive addresses both authorized and unauthorized users who attempt to copy or move data from a classified system to a removable device. Removable devices can be optical disks such as CD and DVD, storage memory such as USB Devices, and PCMCIA Cards. For this paper, only storage memory is considered because optical disks require a different operating system process to "burn" the optical device versus other storage media. Optical disks will be considered in the near future.

THE CHALLENGE

When it comes to user behavior, the threats that organizations typically face fall into the categories of either policy violations or specific malicious activities. Event management logs are typically focused on who is accessing the system and what they are doing during access; however, further analytics must focus on privileged users to detect anomalies in behavior. USCYBERCOM directives have established clearer policies around established user patterns.

THE SOLUTION

For Window Operating Systems, SecureStrux has developed a unique and flexible solution combining powerful built in tools and techniques already native to the operating system to capture file creation, deletion and change events for all removable storage memory. All of the information collected is easily recorded and sent to Syslog collectors for further analysis and monitoring. The following features are used and executed within the native Windows Operating Systems:

- Auto detection of removable device
- Capture all file creation, deletion and update events
- For each file action, capture the following meta data:
    - File name, to include file path and logical drive
    - Time stamp
    - Action [create, delete, update]
    - User Account
    - System Name
    - Amount of data in bytes (could be negative for deletions and updates)
- Record Meta data to windows event file of choice
- Process runs quietly in the background
- Startup the script on boot up
- Maintain one instance of the process running at all times
- Protected process from shutdown using HBSS HIP signatures or other similar method

DioStrux allows leadership to monitor and subsequently control the amount of sensitive or classified data moved to removable devices by authorized users to detect the possibility of security violations and reduce the risk of insider threat. Additionally, **DioStrux** demonstrates adequate and consistent compliance with the requirements and intention of USCYBERCOM Directives.

SUMMARY

With sequestration in full effect and despite the growing need for cyber innovation, USCYBERCOM will take a 7% hit in spending in 2016, meaning the Command as a whole, will have to do more with less. Most agencies and organizations are understaffed; therefore, effective automation can reduce the strain on human resources, and yet still provide valuable actionable information to reach leadership quickly. **DioStrux** can also enhance an organization's security posture by providing more rapid detection and response capabilities that minimize insider threat and prevent future breaches. Research has shown that increased response time reduces the impact and recovery cost of breaches.

Third party Data Loss Prevention (DLP) solutions are available, but are costly and require extensive training and tuning. For most organizations, these products introduce additional cost of procurement and maintenance. By utilizing our unique solution, we leverage the built-in Windows Operating System and the tools that are already inherently native to the OS kernel. With no additional software installation, **DioStrux** seamlessly integrates with the underlying OS making it more cost effective and less complex than standard add-ons in meeting the intents of USCYBERCOM requirements.

Our team is continuing to enhance and automate cybersecurity within the Department of Defense (DoD). **DioStrux** has wide spread applicability throughout the DoD and the federal government as a whole. Our team has extensive security experience within the DoD and brings an enormous amount of creativity and technical skills to this environment. Our SecureStrux team is well balanced among multiple disciplines and is well integrated into the existing DoD security realm.

Our DioStrux Insider Threat automated solution is just the first in many innovations being developed at SecureStrux to enhance our nation's cybersecurity posture against our global adversaries.

www.securestrux.com   717.262.2672   info@securestrux.com

ABOUT US

SecureStrux provides a wide range of specialized cyber services in the areas of compliance, vulnerability management, cybersecurity strategies and engineering