In the wake of a series of damaging insider threat incidents, the U.S. Government has issued new policies and directives aimed at more effectively countering insider threats across the U.S. Government and the supporting Defense Industrial Base (DIB). This paper discusses how several of these mandates pertain to insider threat programs. It then recommends a proven and trusted solution to help governmental and private sector organizations comply with relevant policies and directives.
Contents

1. Executive Summary 4
2. Federal Government Policies and Requirements 4
3. Common Misconceptions in Addressing the Insider Threat Challenge 4
5. Multiple Stakeholders, Multiple Business Objectives 7
6. SureView® Insider Threat Capabilities 7
7. SureView® Insider Threat Pre-Configured Hardware Platform: Rapid Implementation Package Delivered by a Dedicated Mission Partner 9
8. Pre-Configured Hardware and Storage Designed to Scale 9
9. Business Support Services 10
10. Training 10
11. Conclusion 10
12. Index 11
Executive Summary

"Today more information can be carried out the door on removable media in a matter of minutes than the sum total of what was given to our enemies in hard copy throughout U.S. history. Consequently, the damage caused by malicious insiders will likely continue to increase unless we have effective insider threat programs that can proactively identify and mitigate the threats before they fully mature."  

The following anecdotes represent some of the most common misconceptions that exist as government agencies and DIB companies consider how best to comply with government mandates regarding user activity monitoring for insider threats:

- **Endpoint Security and Configuration Management.**
  
  "I already have software in place that ensures that my endpoints are secure, configured according to our enterprise baseline, and patched consistently. It also helps us ensure that the CD burners on each box are deactivated."

  While this component is one important aspect of addressing the insider threat and it does a good job of "locking down" and controlling the actual endpoint device, it offers little visibility into what the human end-user is doing on the device. Moreover, often there is no independent auditing performed to ensure that some of these host-based information assurance controls (such as disabling a write capability on a CD burner) are actually working properly.

- **Data Leak Prevention (DLP).**
  
  "We already use DLP for ‘dirty word’ searches on email sent outside our enterprise to ensure sensitive documents are not being shared with anyone outside the agency that does not have authorization to view such information."

  While this approach is helpful for unencrypted email text and attachments, it is defeated if a malicious actor encrypts the content in order to conceal the payload. Moreover, a purely "content-centric" approach to the insider threat ignores the fact that data exfiltration is merely one of many threat vectors among a broad spectrum of risks that do not necessarily relate to "data leaks." Those risks include, among others, technical sabotage, clandestine communication, unauthorized changes to data, and workplace violence. Key requirements such as keystroke auditing, clipboard monitoring, and collection of desktop video are not met with DLP solutions.

- **Log Analysis.**
  
  "We use a prototype tool to extract existing Windows log files to detect anomalous events that may indicate malicious insider activities. This kind of capability promises the lowest cost approach to solving the insider threat detection challenge."

  Content-blind log analysis requires excessive reliance on superficial event properties described in the log that make it difficult to identify truly malicious behavior with a high degree of fidelity. And most logs are designed to assist system administrators in determining whether information systems

In the wake of a series of damaging insider threat incidents, the U.S. Government has issued new policies and directives aimed at more effectively countering insider threats across the U.S. Government and the supporting Defense Industrial Base (DIB). This paper discusses how several of these mandates pertain to insider threat programs. It then recommends a proven and trusted solution to help governmental and private sector organizations comply with relevant policies and directives.

Federal Government Policies and Requirements

Since October 7, 2011, when President Obama signed Executive Order (EO) 13587 in response to Private Manning’s theft of millions of classified records, known as "Wikileaks," there have been multiple government policies, mandates and suggestions. All getting at one thing, that organizations need to beef up their cyber security programs; specifically their insider threat programs.

The end result of these Executive and Legislative Branch actions is a new set of cascading and inter-locking policy guidance and increasingly specific technical/programmatic directives and instructions mandating adoption of critical insider threat detection and mitigation capabilities. For more details on many of these mandates please refer to the Index of this paper.

Common Misconceptions in Addressing the Insider Threat Challenge

Many security software vendors are seeking to reposition their traditional information security tools to address insider threat use cases. As a result, misconceptions have arisen around the myriad of technology solutions available to mitigate insider threats. While some organizations have characterized existing information assurance (IA) software solutions as effective tools for addressing insider threat challenges, these solutions fall short of providing the insight and context required to detect and assess the potentially malicious acts of a trusted insider.

---

1 Source: http://www.ncsc.gov/issues/ithreat/
2 Source: Executive Order (EO) 13587 "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."
are running properly. Reliance on static logs does not provide context around incidents as a means to effectively discern end-user intent, thereby inhibiting real-time, content-aware review and response to incidents while creating more, not less, work for the operator.

At its root, the insider threat challenge is about human behavior and how to effectively audit and investigate that behavior as the user interacts with a computer and its data. A policy-driven user activity monitoring approach is the most effective way to audit the comprehensive range of human interaction with IT systems. Such a solution enables visibility into possible precursor activity so that incidents can often be mitigated by the organization before damage occurs. Only by employing a configurable endpoint audit tool in conjunction with a risk management approach to insider threat detection can organizations ensure that relevant, actionable data is collected, thereby lowering false positives and reducing operator workload.

**SureView® Insider Threat: A Mature and Trusted User Activity Monitoring Solution for Insider Threat Detection**

SureView® Insider Threat, has been securing the nation’s most critical and sensitive networks from internal leaks, compromise, and malicious attacks for more than a decade. SureView Insider Threat was designed to specifically support the user activity monitoring mission through robust auditing of human behavior on computer endpoints. It was developed by a team of insider threat domain experts who have spent their careers on insider threat programs. They pioneered an active strategy to protect critical data by monitoring "technical observables" which include not only the location and movement of data, but also the actions (including precursor actions) of users who access, alter, and transport that data. The SureView Insider Threat team has been a trusted mission partner of federal and commercial customers since 2001.

The vast majority of Intelligence Community agencies and key Department of Defense organizations have invested significant resources in an operationally-proven and scalable capability that delivers a mature, standardized endpoint audit tool for insider threat detection. SureView Insider Threat offers a trusted and reliable capability already deployed to over a million classified and unclassified endpoints. SureView Insider Threat is the only user activity monitoring solution that meets Intelligence Community (ICD 503 and DCID 6/3) and DOD (DISA STIGs and DIACAP) security requirements out-of-the-box and has Authority to Operate (ATO) on NIPRNET, SIPRNET, JWICS and various TS/SCI networks.

Hence, SureView Insider Threat provides the U.S. Government and Defense Industrial Base companies with a low-risk implementation path to complying with relevant mandates.

**SureView Insider Threat**

is the only user activity monitoring solution that meets Intelligence Community (ICD 503 and DCID 6/3) and DOD (DISA STIGs and DIACAP) security requirements out-of-the-box and has Authority to Operate (ATO) on NIPRNET, SIPRNET, JWICS and various TS/SCI networks.

SureView Insider Threat uses fully validated NIST FIPS 140-2 encryption modules for all cryptographic functions, including data storage on agents, agent-to-server communication, server-to-server communication and data storage in the centralized database. The tool’s software code has been extensively reviewed by the Government for reliability, safety, maintainability, integrity and availability.

**SureView Insider Threat uses fully validated NIST FIPS 140-2 encryption.**
Key SureView Insider Threat features include:

- **Configurable, Policy-based Auditing.** Analysts have the ability to succinctly define policy-based criteria to select which behaviors are audited and what information is collected, unlike other solutions that use a one-size-fits-all approach. This flexibility enables the analyst to easily adjust the criteria for defining a high-risk behavior or a policy violation to meet organizational needs. Every adjustment by the analyst is also audited by the tool to ensure policy compliance and prevent abuse. Equally important, SureView Insider Threat enables analysts to define what sensitive information not to collect, such as user passwords, Social Security Numbers (SSNs), online bank account numbers or confidential and privileged email communication to legal counsel or inspectors general.

- **Full Context Event Replay.** SureView Insider Threat offers a unique video playback capability to provide contextual insight to discern malicious from benign activity that is easily understood by non-technical personnel. The playback capability offers unambiguous and irrefutable attribution of all computer end-user activity and can help detect concealment techniques employed by malicious insiders to cover up their activities.

- **Unobtrusive Monitoring.** SureView Insider Threat provides host-based monitoring that can audit the comprehensive range of human interaction with computer endpoints, to include all keystroke activity, communication vectors, application usage, processes, and use of removable media and peripheral devices without adversely impacting bandwidth or memory.

- **Complements Existing Information Assurance (IA), Advanced Persistent Threat (APT) and Computer Network Defense (CND) Tools.** SureView Insider Threat can be used to establish "ground truth" for established IA controls to ensure they are properly configured and functioning per compliance standards. It also supports specific CND use cases such as malware detection and blocking downloads of unauthorized software and it complements existing APT tools.

- **Creates IT Efficiency and Provides High Return on Investment (ROI).** SureView Insider Threat reduces management costs and agent footprints on enterprise endpoints by combining multiple analytical functions into a single tool, thereby providing quick ROI for IT. It quickly detects internal and external threats, monitors human behaviors to expose internal threats, and identifies external threats that traditional anti-malware security tools miss.

SureView Insider Threat includes:

- **Enterprise Administration.** The Administration Workbench improves the management of users, agents and groups in large-scale deployments, and supports hundreds of thousands of clients.

- **Universal Security Information and Event Management (SIEM) Integration.** SureView Insider Threat’s alerts can be forwarded to SIEM systems that support the Common Event Format to enhance situational awareness across the enterprise.

- **Role-Based Access Controls (RBAC).** SureView Insider Threat access controls provide role-based restrictions, allowing access only to functions required for the user’s role. SureView Insider Threat also provides self-auditing features that enable independent oversight to prevent abuse by analysts.

- **Data Aggregation.** SureView Insider Threat allows for the ingestion of external data sources such as ID badge and Human Resources records, phone logs, data from CND tools and other related personnel security information to enhance an investigator’s operational situational awareness.

- **Analytics API.** SureView Insider Threat provides an analytics framework that enables seamless integration with best-of-breed analytical tools including risk assessment algorithms, anomaly detection, and user trend analysis, in support of the insider threat mission.

- **Targeted Policies.** SureView Insider Threat Policy Packs are based on business policies and best practices for detecting and deterring insider threats. They span a broad range of policies that target specific business problems such as privileged user abuse, PCI compliance, HIPAA compliance, etc.
Multiple Stakeholders, Multiple Business Objectives
While originally designed to support the cyber counterintelligence mission through robust auditing of human behavior on computer endpoints, SureView* Insider Threat offers a reliable, stable and unobtrusive host-based agent that also supports other key stakeholder business objectives. Examples of use cases that SureView Insider Threat supports include:

- **Information Assurance**
  - Monitoring effectiveness of IA controls (e.g., disabling the write function on CD drives, blocking the introduction of unapproved software or applications, etc.) to ensure that they are working properly.
  - Host-based discovery and detection of malware through registry analysis and on-demand searching of registries for the presence of particular keys/values.
  - Video playback to provide context and detail around incidents described in Help Desk trouble tickets.

- **Business Analytics**
  - Auditing end-user access to agency intranets and portals to discern usage trends.
  - Software license auditing (e.g., capturing the number of copies of Microsoft Project that are installed and actively used across the enterprise).

- **Personnel Security**
  - Continuous evaluation for end-users holding an active security clearance with respect to Adjudicative Criteria M: Use of Information Systems described in Intelligence Community Policy Guidance (ICPG) 704.1, Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information.³
  - Evidentiary support for inquiries or investigations relating to workplace threats or Operations Security (OPSEC) violations.

SureView Insider Threat policy group mappings and role-based access provide stakeholder groups with the appropriate individual control over policy development and deployment. In addition to controlling access to collected audit data based on a user’s role and permissions, SureView Insider Threat creates efficiencies across the IT enterprise by reducing management costs and agent footprints on enterprise endpoints and combining multiple analytical functions into a single tool.

**SureView Insider Threat Capabilities**
SureView Insider Threat’s capabilities are enabled by the deployment of tamper-resistant agents onto workstations across the enterprise. These agents observe and analyze user behavior and activity through rules and policies as defined by the operator. Agents are able to collect on a multitude of applications, processes and behaviors, including but not limited to those listed in Figure 1.

---


---

**MONITORING VECTORS OF COMMUNICATION**

![Monitoring Vectors of Communication](image)
The highly stable agent has been specifically designed to minimize adverse impact to endpoint bandwidth and storage by means of configurable throttling mechanisms that regulate CPU usage and offloading and transfer of collected data back to collector nodes. These throttling mechanisms also have been tested and proven, when configured, to transmit data from remote OCONUS (Outside the Continental United States) locations utilizing as little as 56 kbps of bandwidth. SureView® Insider Threat agents are able to collect in a persistent manner even when laptops or workstations are disconnected from the network by transmitting collected data once the network connection is restored.

From a performance standpoint, the SureView Insider Threat agent is rigorously tested to minimize its impact to the host machine user's experience. While the agent can actively disengage the user from the host machine when certain behaviors are detected, such as introduction of classified data onto an unclassified system, the default behavior of the agent is to "quietly" monitor user behavior and collect requested data.

For role-based access control, SureView Insider Threat implements a fully-configurable access matrix that restricts operator access to only those functions required by their role. For example, investigators can be restricted to only viewing collected data with no access to policy creation or other system administration functions. In addition to allowing or denying access, SureView Insider Threat offers two-person authorization enforcement for gaining access to customer-selected system functions. For example, creating new operators or altering policies could be configured to require two-person controls. SureView Insider Threat's management controls can be used to segregate access to audit policies and collected auditable events according to each individual stakeholder group within an organization. Analysts can review auditable events and utilize the “DVR” play-back functionality with the SureView Insider Threat Investigator Workbench. (See Figure 2.)

Figure 2 - SureView Insider Threat Investigator Workbench.
SureView® Insider Threat Pre-Configured Hardware Platform: Rapid Implementation Package Delivered by a Dedicated Mission Partner

Speed to implementation is a vital consideration for any insider threat detection tool. As a trusted mission partner, we offer organizations our proven and effective user activity monitoring capability with a low total cost of ownership (TCO) by bundling together a pre-configured hardware and software solution with expert deployment and support services that ensure rapid implementation and efficient ongoing management of the tool. The rapid implementation of a user activity monitoring capability with SureView® Insider Threat is enabled by several key factors:

- **SureView Insider Threat Pre-Configured Hardware Platform** ensures that the customer has properly configured hardware delivered pre-installed with the SureView Insider Threat software. This pre-configured system approach significantly reduces risk and speeds implementation, while providing a solid foundation with a scalable path to a fully operational program.

- **Lessons Learned and Institutional Knowledge** derived from over a decade of past Federal Government and Fortune 100 deployments are injected into the pre-configured hardware platform project plans and schedules, providing for continuous improvement of the processes while greatly reducing the risks of deployment. Implementation activities are designed to be executed in parallel to streamline the process.

- **The Pre-Configured Hardware Platform** package is delivered with certification and accreditation templates for ICD 503⁴ (formerly DCID 6/3) and DIACAP⁵ processes that can be tailored and modified to support each unique deployment. Additionally, these templates expedite approvals by Designated Accrediting Authorities (DAA) in granting Authority to Operate (ATO).

- **SureView Insider Threat** is fully integrated as a plug-in to McAfee ePolicy Orchestrator (ePO). As a result, agent command and control for functions such as installation, start/stop of agents and monitoring health and wellness can be accomplished through existing ePO implementations.

- **SureView Insider Threat** fully integrates with ArcSight and other Security Information and Event Management (SIEM) tools utilizing the Common Event Format (CEF).

This includes the ability to pass auditable event alerts to the SIEM in order to augment the enterprise’s overall situational awareness picture.

- **SureView Insider Threat’s** pre-configured and standardized library of over 600 audit policies can be rapidly deployed, tested, tuned and implemented using trusted and repeatable processes and techniques that leverage best practices from existing deployments.

Pre-Configured Hardware and Storage Designed to Scale

SureView Insider Threat has standardized on Oracle Enterprise Database Software and EMC Storage Arrays for its back-end database and storage solution. With a building block approach, the solution scales from a small configuration to a larger configuration while maintaining application integrity and performance. This allows organizations to achieve the proper level of reliability and scalability while minimizing cost and impact on IT resources. The Pre-configured Hardware Platform delivers a cost-effective, standardized and rapidly deployable capability that will scale to support expansion to a full enterprise. (See Table 1.)

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower total cost of ownership (TCO)</td>
<td>Reduces acquisition, administration, and maintenance costs</td>
</tr>
<tr>
<td>High availability</td>
<td>Can implement a clustering architecture that provides very high levels of data availability</td>
</tr>
<tr>
<td>Increased flexibility and scalability</td>
<td>Easily expand capacity as customer needs grow</td>
</tr>
<tr>
<td>Standard environment</td>
<td>More reliable and better-tested environment reduces the likelihood of problems with the product</td>
</tr>
</tbody>
</table>

Table 1 - SureView Insider Threat’s Pre-configured Hardware Platform Benefits

---


⁵ Source: https://en.wikipedia.org/wiki/Department_of_Defense_Information_Assurance_Certification_and_Accreditation_Process
Business Support Services
SureView® Insider Threat is supported by a team of dedicated professionals, many of whom are cleared at the TS/SCI level and support existing insider threat audit programs. Supporting the first line of subject matter experts is our team of engineering, development, quality assurance, and customer support staff that have refined SureView Insider Threat to the exceptionally stable and reliable solution it is today.

A full spectrum of on-site and off-site product support services is provided to support the operation of the SureView Insider Threat system, and these services are configurable according to customer needs. The professional services staff possesses a wealth of institutional knowledge and deep understanding of best practices based on their support for existing insider threat programs, reducing overall implementation risk for organizations.

Training
One of the key strengths of SureView Insider Threat is the tool’s ease-of-use and the fact that it does not require a significant amount of training or a technical background for analysts to use and understand. SureView Insider Threat analysts are typically trained in a three-day class.

Training can be delivered onsite at customer facilities and can also be customized based on the customer’s needs and specific business processes. The curriculum can be tailored to support the various stakeholder roles within the organization’s user activity monitoring program:

- Technical security analysts and administrators
- Investigators and incident response specialists
- Compliance officers and non-technical management

Our unique combination of technical experts and world-class investigators can train personnel to become competent in both enterprise auditing and targeted investigations. The following training curriculum is provided in support of SureView Insider Threat:

- Policy Creation and Tuning
- Investigations and Forensics
- Enterprise Monitoring Best Practices
- Policies for Regulatory Compliance
- System Configuration and Optimization

Conclusion
The WikiLeaks and Snowden incidents were watershed events that have dramatically changed the policy landscape with regard to detecting and mitigating insider threats across the U.S. Government and supporting organizations such as DIB companies. Recent policy changes and technical/programmatic directives have underscored the importance of effective and cost-efficient solutions to insider threats. As noted above, SureView Insider Threat is the only user activity monitoring solution that meets Intelligence Community (ICD 5036 and DCID 6/37) and DoD (DISA STIGs8 and DIACAP) security requirements out of the box and that has Authority to Operate (ATO) on NIPRNET, SIPRNET, JWICS and other TS/SCI networks. SureView Insider Threat uses fully validated NIST FIPS 140-29 encryption modules.

We are committed to working with the United States government and DIB companies as a trusted partner to address the challenges presented to its classified and unclassified IT systems by potential insider threats. With well over a decade supporting insider threat programs, we are in a unique position to deliver a proven, scalable and mature capability with the lowest total cost of ownership available that will address all stakeholder missions described in Intelligence Community Standard 500-2710.

---

7 Source: http://fas.org/irp/offdocs/DCID_6-3_20Manual.htm
8 Source: http://iase.disa.mil/stigs/Pages/index.aspx
9 Source: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
Index

1. Order (EO) 13587 structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information
   • Established a Senior Information Sharing and Safeguarding Steering Committee to develop government-wide policies and standards for safeguarding classified data on computer networks.
   • Established an inter-agency National Insider Threat Task Force (NITTF) to develop a government-wide insider threat program to deter, detect, and mitigate insider threats. The Task Force is co-chaired by the U.S. Attorney General and the Director of the Federal Bureau of Investigation (FBI). They, in turn, designated the FBI and the National Counterintelligence Executive (NCIX) to co-direct the daily activities of the NITTF.

2. November 12, 2012, President Obama signed a memorandum outlining U.S. national insider threat policy and minimum standards for Executive Branch insider threat programs. The memorandum provides Federal departments and agencies with the minimum elements necessary to establish effective insider threat programs. According to the memorandum, “These elements include the capabilities to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.”

3. November of 2013, the NITTF released the “Guide to Accompany the National Insider Threat Policy and Minimum Standards,” which included guidelines on establishing and implementing an integrated capability to monitor and audit information for insider threat detection and mitigation – also known as User Activity Monitoring (UAM). The NITTF also made clear that log analysis is not the same as UAM, and that UAM includes monitoring file activity, keystrokes, clipboard use, video captures, and other endpoint activities.

4. November 18, 2013, the Department of Defense published a Final Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to address requirements for safeguarding unclassified controlled technical information from unauthorized access and disclosure and to prescribe reporting to DOD with regard to certain cyber intrusion events. The final rule is mandatory for all contracts and solicitations, including for commercial items, and must flow down to all subcontractors. For Defense Industrial Base (DIB) companies, the Final Rule will clearly impact operations.

5. September 30, 2014, the Deputy Secretary of Defense signed Directive Number 5205.16 entitled “The DOD Insider Threat Program.” The program covers all components of the Defense Department as well as DIB contractors and other non-DOD entities that have authorized access to DOD resources. It sets policies and assigns responsibilities for preventing, detecting and mitigating damaging actions by trusted insiders. The program seeks to implement the Presidential Memorandum from November 2012 and directs that “Through an integrated capability to monitor and audit information for insider threat detection and mitigation, the DOD Insider Threat Program will gather, integrate, review, assess, and respond to information derived from counter-intelligence (CI), security cybersecurity, civilian and military personnel management, workplace violence, AT risk management, law enforcement (LE), the monitoring of user activity on DOD information networks, and other sources as necessary and appropriate to identify, mitigate and counter insider threats.”

6. The United States Congress also has moved aggressively to enact statutory requirements, provide clear programmatic guidance and direction, and authorize and appropriate funding to enable federal agencies and organizations to deploy proven and effective insider threat detection and end-user auditing tools as well as adopt best practices. For example, Section 922 of the National Defense Authorization Act for Fiscal Year 2012 directed the Secretary of Defense to establish a program for information sharing protection and insider threat mitigation for the information systems

13 Source: http://www.fas.org/sgp/obama/insider.pdf
of the DoD to detect unauthorized access to, or use and transmission of, classified information. It also directed the Secretary to ensure that the program achieve an Initial Operational Capability (IOC) no later than October 1, 2012, and achieve a Full Operational Capability (FOC) no later than October 1, 2013. Likewise, the Intelligence Authorization Act for Fiscal Year 2011\(^{17}\) required the Director of National Intelligence (DNI) to also implement an insider threat detection program and achieve Initial Operating Capability (IOC) for the program by October 1, 2012 and Full Operating Capability (FOC) by October 1, 2013.

\(^{17}\) Source: https://www.govtrack.us/congress/bills/112/hr754