Protecting DoD organizations from insider threats

Syteca

The possibility of espionage, fraud, and other malicious activities in the Department of Defense carries critical risks to the well-being and safety of the entire country. Therefore, safeguarding sensitive information against insider threats is paramount for DoD organizations.

Required by CNSS Directive 504 and other cybersecurity regulations for the Department of Defense, user activity monitoring (UAM) emerges as a powerful tool for detecting and preventing insider threats, ultimately protecting critical and classified data.

As a full-cycle insider risk management platform, Syteca offers user activity monitoring, privileged access management, and incident response capabilities to protect data at multiple levels of security.

Meeting the requirements of CNSS Directive 504 with Syteca

CNSS Directive 504 requires DoD organizations to implement UAM as a part of their insider threat programs. Here's how you can meet the directive's requirements with Syteca's capabilities:

CNSSD 504 requirements for UAM capabilities	Syteca's offer				
Keystroke monitoring	Track all keystrokes typed by a user.	Record clipboard text content (copy and paste operations).	Receive alerts on users typing specific keywords.	Start user activity monitoring upon user typing a specific keyword.	Apply keystroke filtering by defining applications for which keystroke data will be captured to reduce the amount of data collected.
Application content capture	Track the names of applications and titles of active windows a user launches.	Track URLs visited by a user in standard browsers (Firefox, Chrome, Microsoft Edge Opera, and Internet Explorer).	Record on-screen user activity in applications.	Record input and output audio streams in common browsers and communication platforms.	Apply application filtering to monitor user activity only in specific applications.
Screen capture	Create high-quality screen capture recordings of user activity along with informative metadata.	View videos of on-screen user activity and read metadata in real time.	Continue to take screenshots of user activity and capture metadata if the server connection goes down.	Define the frequency and quality of screen captures to meet your needs and storage capabilities.	Enable an option to create a screen capture recording each time a user clicks a mouse or presses a key on the keyboard.
File shadowing	Record on-screen user actions with files.	Track and receive alerts on file upload operations performed on the monitored endpoint.			
Alerting	Receive real-time notifications on suspicious user activity by using a system of granular alert rules.	Use predefined alerts to detect threats that may lead to cyber incidents such as fraud or data leakage.	Create your own custom alerts for detecting suspicious user actions like launching a specific application, visiting a particular URL, or typing certain words, etc.	View risk scores of each user session to prioritize assessment.	Customize your experience for viewing enabled alerts: using the Alerts tab, generating informative alert reports, and pipelining your data to Microsoft Power BI.
Ability to attribute collected data to a specific user	View user details in the monitored session, including user name, remote IP address, remote host name, etc.	Leverage Syteca's secondary authentication feature to identify users and distinguish their activity under shared accounts.	Pseudonymize personally identifiable data of users for privacy purposes and then de-anonymize it if needed for investigation purposes.	Benefit from Active Directory integration and link user activity data with individual user identities.	

CNSS Directive 504 requires DoD organizations to implement an insider threat program in addition to UAM. Effective insider threat mitigation requires a comprehensive approach that addresses the human element. You can take such an approach by leveraging Syteca's cybersecurity capabilities:

Elements of an insider threat program	Syteca's offer			
Risk assessment	Monitor user activity in real time and review recorded user sessions to identify security risks.	Streamline your risk assessment process with the help of user activity alerts that prioritize events according to their risk level.	Aggregate information on security events collected by Syteca in SIEM systems to enable swift and full-spectrum analysis.	Generate reports on user activity to speed up your risk assessment process.
Threat detection and response	Receive live notifications on suspicious user behavior and security violations.	Manually block users performing potentially malicious actions or configure rules for automatic incident response.	Block unauthorized USB devices used by employees in your IT infrastructure.	Leverage Syteca's dashboards for a convenient overview of your security events and employee productivity.
Access management	Verify user identity with the help of two-factor authentication (2FA).	Control access to sensitive endpoints and implement the principle of least privilege with Syteca's privileged access management (PAM).	Leverage password and identity management capabilities to establish secure access request and approval workflows and enhance authentication methods in your organization.	Streamline just-in-time access management with the help of one-time passwords, time-based user access restrictions, and integration with ticketing systems.
Incident investigation	Record user sessions to collect evidence in case a security incident happens.	Leverage Syteca's offline monitoring feature to continue collecting cybersecurity evidence even if the server connection goes down.	Export user sessions in a tamper-proof format for the purpose of external forensic investigations.	Investigate security incidents caused by insiders and establish context by reviewing screen capture recordings along with detailed metadata on user activity.
Training and cyber awareness	Get visibility into user actions and behaviors to identify and address any lapses in basic cyber hygiene practices and detect policy violations.	Use recorded user sessions to develop materials and case studies for cybersecurity awareness training initiatives.	Foster positive cybersecurity habits and de-incentivize negative ones by displaying warning messages in response to prohibited actions.	Monitor user actions during penetration testing to provide targeted feedback to users and promote adherence to cybersecurity best practices.

Why Syteca?

Complete server and desktop OS support

Syteca supports a majority of operating systems, including Windows, macOS, Linux, and Citrix. Our platform also supports jump servers, allowing you to secure almost any network architecture.

Scalable solution

Our platform is designed to monitor thousands of endpoints while retaining performance and stability. Syteca is suitable for large heterogeneous infrastructures thanks to its High Availability and Multi-Tenant Modes, system health monitoring, and automation processes.

Cloud and VDI monitoring

Syteca allows you to monitor user activity in cloud infrastructures including AWS, Microsoft Azure, and Amazon Workspaces. Similarly, Syteca works well in virtual environments like VMware Horizon, Microsoft Hyper-V, and Citrix.

IT compliance simplified

Leverage Syteca's extensive functionality to comply with key IT security requirements of the GDPR, HIPAA, PCI DSS, NIST 800-53, ISO 27001, SOX, FISMA, NIS2, and other cybersecurity standards, laws, and regulations.

Full-cycle privileged user management and monitoring

Syteca takes a holistic, multi-layered approach to managing privileged user risks. This approach includes managing privileged access, monitoring privileged user activity, and responding to potential threats.

Comprehensive integration capabilities

Syteca seamlessly integrates with existing tools and services that our customers rely on: SIEM systems, ticketing systems, Active Directory, Power BI, and SSO. Integration eliminates the need for manual data transfer and fosters a more unified workflow.

Fast deployment and painless maintenance

Thanks to remote client installation, Syteca is quick to deploy. Our support team is available 24/7 if you need assistance or help with maintenance. With the SaaS version of Syteca, maintenance is performed entirely on our side.

Lightweight software agent and highly optimized data storage formats

The lightweight agent does not interfere with your systems and does not affect user performance. Collected data is saved in searchable and highly optimized file formats for compact log storage and easy reporting. All data is encrypted and protected from unauthorized access.

2,000+ Clients

300+ Partners

70+ Countries

7,000+ Protected servers

120,000+ Protected workstations

Explore how Syteca helped a US-based defense company secure sensitive data from insider threats and comply with cybersecurity requirements:

Customer success story

US-Based Defense Organization Enhances Insider Threat Protection with Syteca

Request a free 30-day trial of Syteca to see if it meets your cybersecurity needs.