CYBER HAWK

THE CRITICAL IT CHANGE DETECTION SOLUTION

Cyber Hawk is a powerful IT change detection solution designed to give you an extra layer of risk management. With its advanced features and intelligent algorithms, Cyber Hawk identifies unauthorized or malicious changes in your IT environment – as well as suspicious end-user behavior that represents potential indications of a network breach.

Expose unauthorized logins or attempts to restricted computers

Identify a new user profile suddenly added to the business owner's computer

Find an application just installed on a locked-down system

Get alerted to unauthorized wireless connections to the network

Get notified when new users are granted administrative rights

Detect an unusual midnight login for the first time by a daytime worker

Find personal Information (PII) stored on machines where it doesn't belong

Detect when new users or new profiles are added

Alert when critical patches are no longer applied in a timely manner

Key IT CHANGE DETECTION Features

Automated scans with minimum configuration

- Ongoing adjustments are automated for effortless IT change detection.
- Get started immediately with minimal setup.

Smart tags

- Easily configure Cyber Hawk to your specific IT environment using an intuitive asset tagging system called "smart tags."
- Simplify and streamline the configuration process through asset tagging.

Scanning engine

- Cyber Hawk goes beyond traditional monitoring systems to scan user, asset and configuration data.
- Discover threats that antivirus, anti-spyware and firewalls may miss.
- It's always "on patrol" by scanning the network at pre-set scheduled times.

Pre-built and custom plans for MSPs

- Choose from four pre-configured service plans based on your needs.
- Customize plans to meet your specific needs or create new plans from scratch.
- Complete flexibility to create the perfect balance of risk versus cost and effort.

Sort IT changes based on severity

- Group changes by type and then severity for easier issue filtering.
- Allows users the flexibility to see the higher severity items first.

Direct PSA integration

- Use the "action links" included with Cyber Hawk to turn individual (or grouped) alerts into service tickets within BMS, Autotask, ConnectWise or Tigerpaw One.
- Improve productivity and efficiency with automatic ticket creation in leading professional service automation (PSA) tools of your choice.

Be on the lookout for these **CRITICAL IT CHANGES**

Category	Change Alert
Wireless	New connection to unauthorized wireless access point
Access Control	New profile (business owner's computer)
Computers	New application installed on locked-down system
Computers	New removable drive added to locked-down system
Access Control	New administrative rights granted
Access Control	New unauthorized access to IT-restricted computer
Network Security	New device on restricted network
Access Control	New unauthorized access to accounting computer
Access Control	New unauthorized access to CDE
Access Control	New unauthorized access to ePHI
Access Control	New unauthorized printer on network
Access Control	New suspicious user logins by single desktop user
Computers	Internet access changed from restricted to not enforced
Computers	Critical patches no longer applied timely on DMZ computer
Computers	Critical patches no longer applied timely
Access Control	New profile added
Access Control	New user added
Access Control	New unusual login to computer by user
Access Control	New unusual login time by user
Network Security	New high severity internal vulnerability (with VulScan)
Network Security	New medium severity internal vulnerability (with VulScan)
Access Control	Local user admin user added

BENEFITS OF CRITICAL IT CHANGE
detection with Cyber Hawk

Reduced risk and increased compliance

- Demonstrate compliance with industry-specific IT regulatory requirements that mandate change detection.
- Maintain accurate documentation and properly configure systems for scalability and disaster recovery.

Early identification of "unforced errors"

- Identify unintentional or unauthorized changes that could disrupt services or impact system stability.
- Acts as a "second set of eyes" that you can use to provide an extra layer of risk management for your network.

Easier troubleshooting and root cause identification

- Leverage Cyber Hawk's detailed alerts to troubleshoot network issues and identify root causes.
- Compare current and previous known states to isolate and pinpoint recent changes contributing to problems.

Manage configurations more efficiently

- Quickly triage discovered changes to dismiss those that are benign in nature and rapidly address critical insider threats.
- Automatically create service tickets for changes that need remediation for faster resolution of critical issues.

Greater peace of mind

- Go to bed at night knowing that Cyber Hawk is on the case, scanning your network environments and alerting you when critical IT changes are detected.

Request a demo and see how easy critical IT change detection can be

Do you need a solution for identifying unauthorized or malicious changes in your IT environment that represent potential threats? Contact us to set up a custom demo and we'll show you how simple it is to automatically detect anomalous user activity, unauthorized network changes and threats caused by misconfigurations.

Get a demo

of Cyber Hawk today.