netwrix

CSPi

Technology Solutions

Top 5 Network Device Incidents You Need Visibility Into

Table of Contents

#1: Configuration Changes 3

#2: Repeated Failed Logon Attempts 4

#3: VPN Logon Attempts 5

#4: Hardware Malfunctions 6

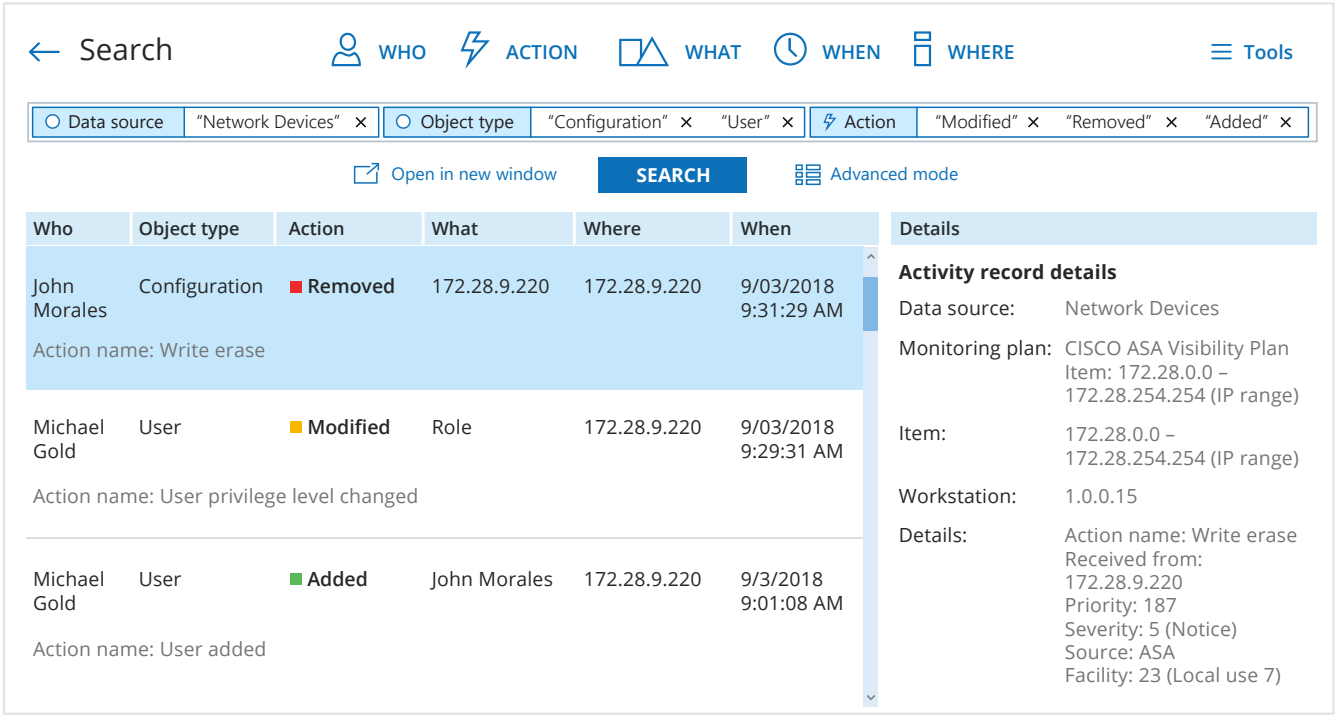
#5: Scanning Threats 7

About Netwrix Corporation 8

#1: Configuration Changes

You need to stay on top of all changes to the configuration of your network devices, such as their protocols, ports and connection limits, since any unauthorized or improper modification could lead to connectivity issues — including the entire network becoming unreachable. You also need to know quickly if someone modifies a Group Policy or creates a new user, since that could be a sign of an insider attack or privilege abuse. Netwrix Auditor tracks both successful and failed configuration changes, enabling you to easily answer questions like these:

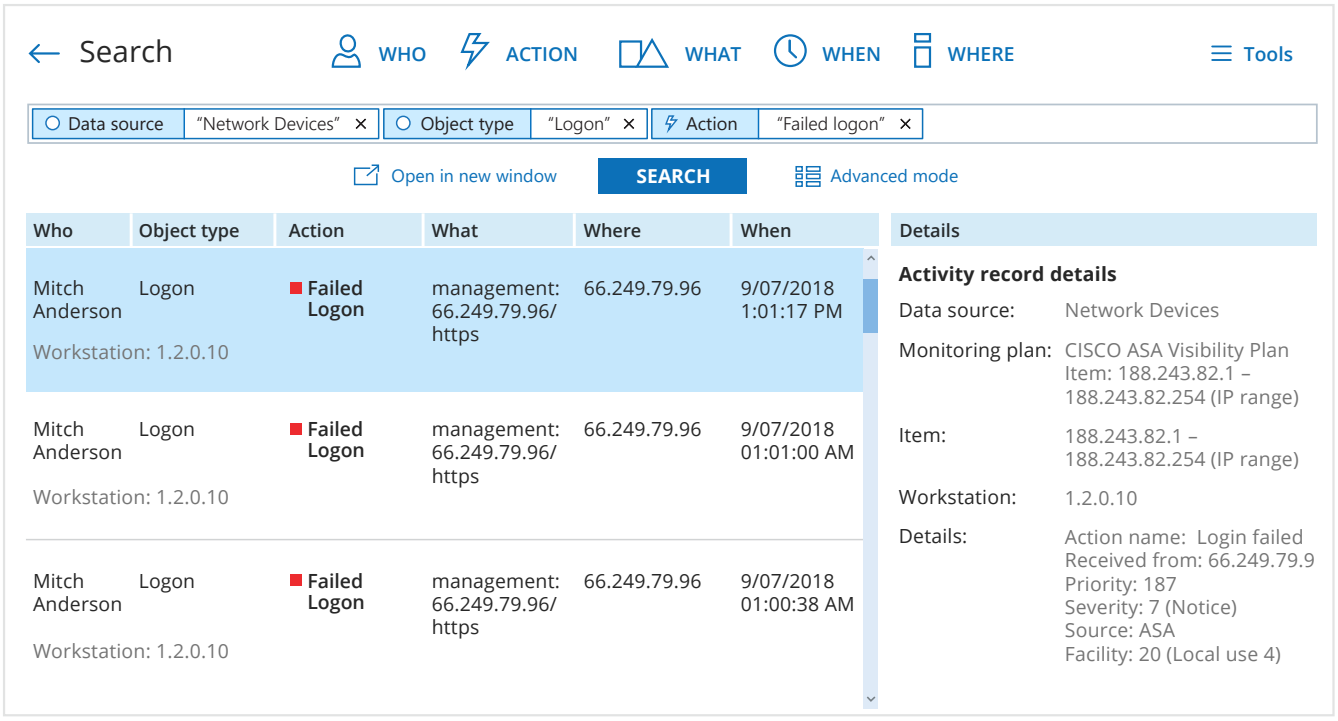
- Who erased the configuration of a particular network appliance?
- What specific settings were changed in the firewall?
- Which IP address was the reload command initiated from?
- When was the router password reset?



#2: Repeated Failed Logon Attempts

It is critical to monitor successful logons to network devices to make sure that they are fully authorized. However, you also need to watch for multiple failed logon attempts, which could indicate that someone is trying to brute-force administrative credentials. If attackers get access to your network device, they'll be able to gain control over your network traffic and steal sensitive data. Netwrix Auditor tracks both successful and failed logon attempts, helping you promptly detect potential brute-force attacks and quickly answer questions like these:

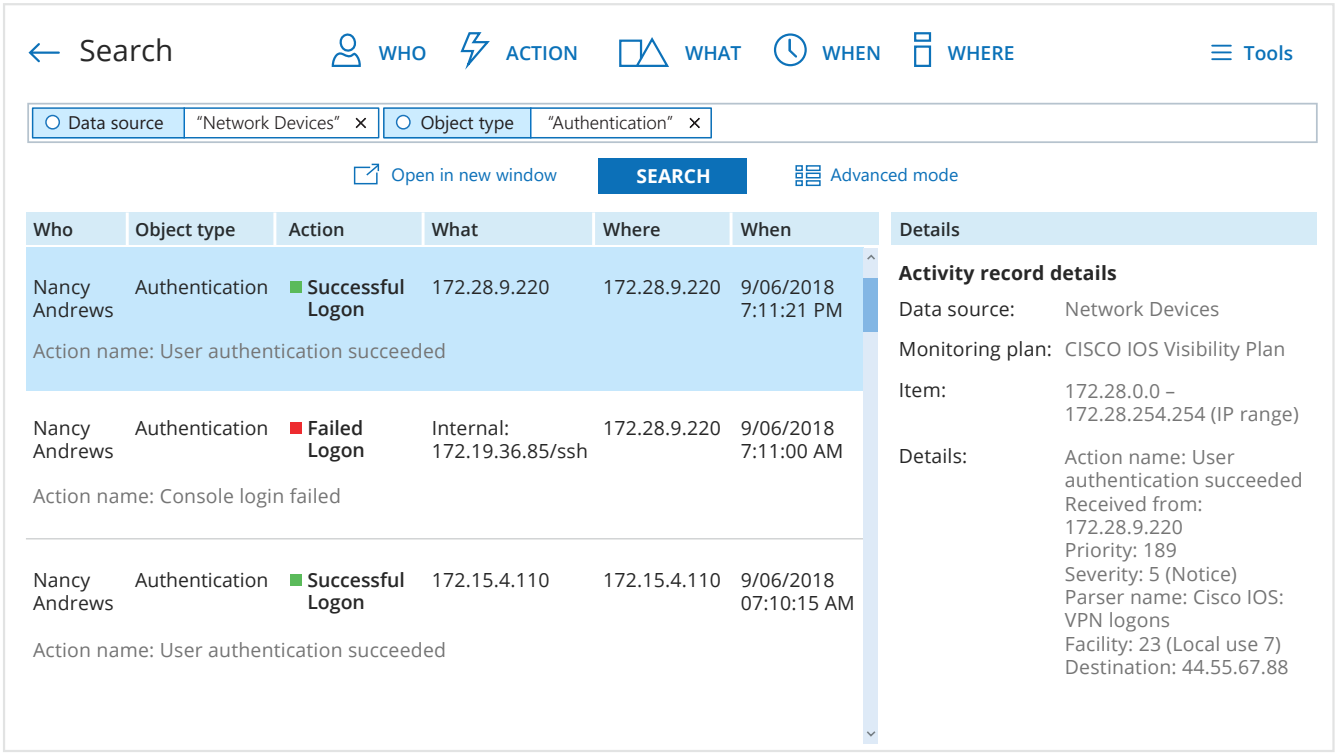
- Who exceeded the maximum number of consecutive authentication failures?
- What was the cause of each failed logon?
- Which IP address was the connection made from?
- How many logons were attempted?
- When was each failed authentication request made?
- What device was the user trying to log on to?



#3: VPN Logon Attempts

Administrators rarely have to log into network devices remotely, so it is important to keep track of each VPN logon attempt. Moreover, even an authorized device with a secure connection to the corporate network can be hacked and used to gain access to sensitive files. Netwrix Auditor helps you monitor both successful and failed VPN attempts to log on to your network devices and answer questions like the following:

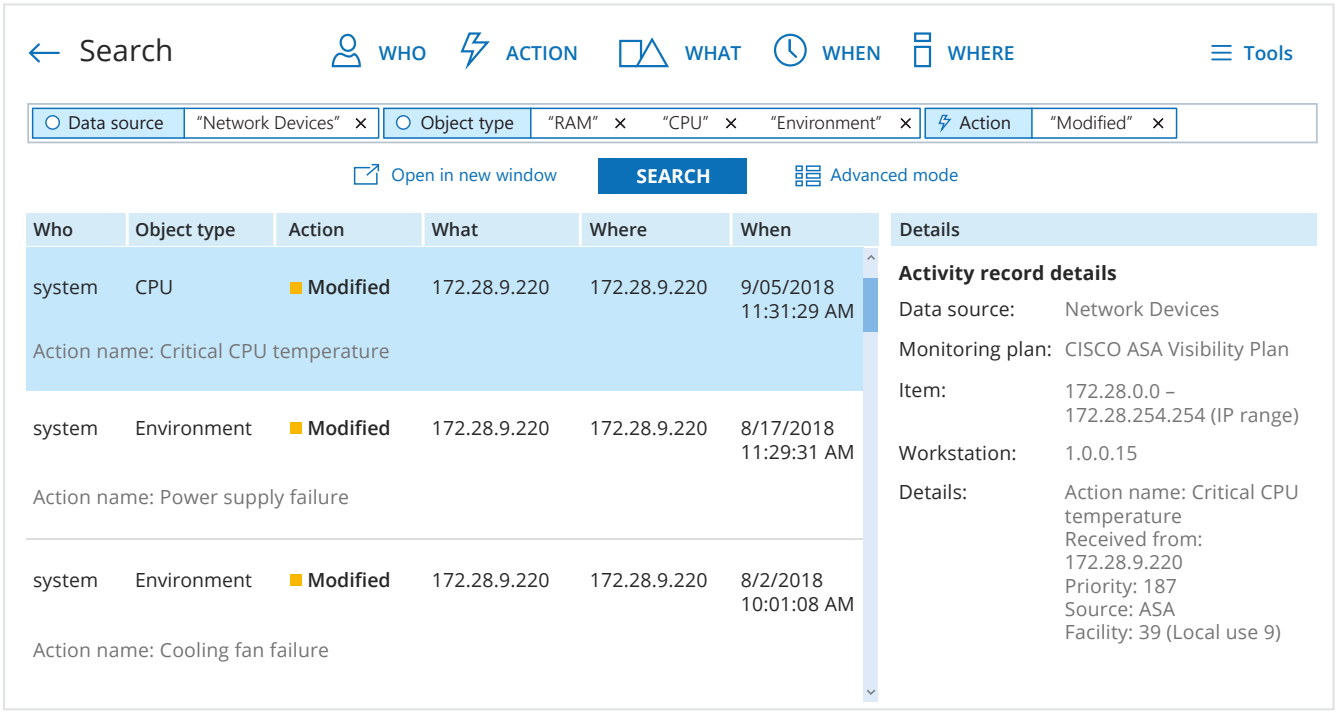
- Who tried to access network devices over a VPN?
- Which IP address was the authentication attempt made from?
- What was the cause of each failed VPN logon?
- When was each VPN logon attempt initiated?
- What device was the user attempting to log on to?



#4: Hardware Malfunctions

In addition to tracking changes to the configuration of your network devices, you should also keep a close eye on the state of your hardware. If a network device encounters environmental or power conditions that violate its specifications, it can overheat, suffer ventilation failures or lose power, which lead to underperformance or even complete shutdown of your network. Network Auditor monitors and alerts on critical hardware failures and helps you answer questions like these:

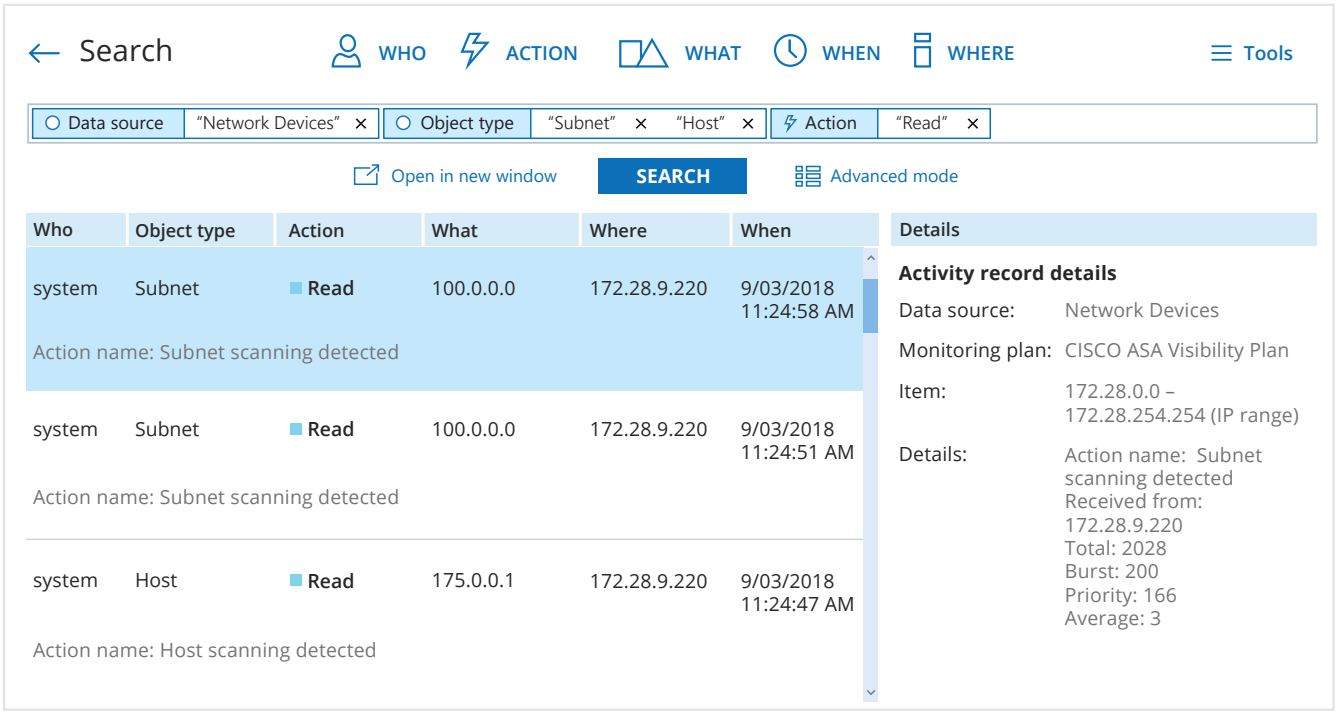
- What actions happened before the network device shutdown?
- Which part of the network device got damaged?
- When did the temperature reach critical level?



#5: Scanning Threats

Subnet scanning and host scanning are not inherently hostile processes for learning about a network's structure and behavior, but attackers often use them to conduct reconnaissance before trying to breach a network and steal sensitive data. Netwrix Auditor tracks these actions and helps you investigate potential incidents by answering questions such as:

- Which host and subnet were scanned?
- When was each scanning attempt performed?
- Which IP address was the scanning initiated from?
- How many scanning attempts were made from each IP address?



About Netwrix Corporation

Netwrix Corporation is a software company focused exclusively on providing IT security and operations teams with pervasive visibility into user behavior, system configurations and data sensitivity across hybrid IT infrastructures to protect data regardless of its location. Over 9,000 organizations worldwide rely on Netwrix to detect and proactively mitigate data security threats, pass compliance audits with less effort and expense, and increase the productivity of their IT teams. Founded in 2006, Netwrix has earned more than 140 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security intelligence to identify security holes, detect anomalies in user behavior and investigate threat patterns in time to prevent real damage.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, Windows Server and Network Devices. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises and cloud-based IT systems in a unified way.

For more information, visit www.netwrix.com.

On-Premises Deployment

Download a free 20-day trial

netwrix.com/go/freetrial

Virtual Appliance

Download our virtual machine image

netwrix.com/go/appliance

Cloud Deployment

Deploy Netwrix Auditor in the cloud

netwrix.com/go/cloud

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social