CYBER HAWK™
by RapidFireTools®

USER GUIDE

Cyber Hawk (previously known as Detector)

Detecting and Responding to IT Security Policy Violations

10/29/2021 10:12 AM

Contents

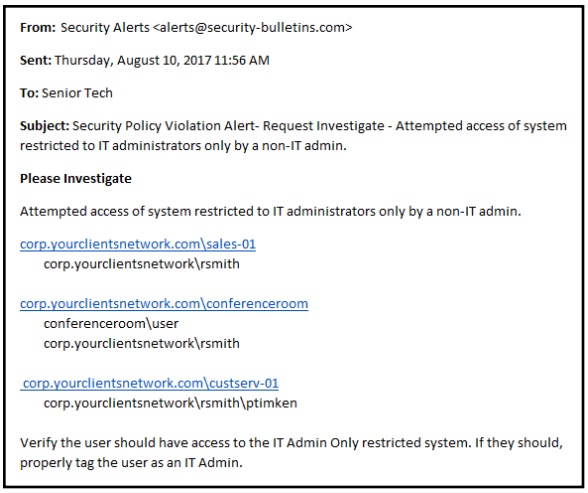
Introduction to Cyber Hawk

This section contains everything you need to know before getting started with Cyber Hawk.

Cyber Hawk Overview

Cyber Hawk prowls an entire network each day at whatever time you determine and then sends out daily **Security Policy Violation Alerts** to notify you of any suspicious activity.

Each discovered issue listed in a Security Policy Violation Alert contains an “Alert Link” to the **RapidFire Tools Portal**. The Portal automates the process of responding to security issues by enabling your technicians to **Investigate** or **Ignore** the Alert item.



From: Security Alerts <alerts@security-bulletins.com>

Sent: Thursday, August 10, 2017 11:56 AM

To: Senior Tech

Subject: Security Policy Violation Alert- Request Investigate - Attempted access of system restricted to IT administrators only by a non-IT admin.

Please Investigate

Attempted access of system restricted to IT administrators only by a non-IT admin.

corp.yourclientsnetwork.com\sales-01
corp.yourclientsnetwork\rsmith

corp.yourclientsnetwork.com\conferenceroom
conferenceroom\user
corp.yourclientsnetwork\rsmith

corp.yourclientsnetwork.com\custserv-01
corp.yourclientsnetwork\rsmith\ptimken

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

In the RapidFire Tools Portal you can:

- review the issue’s forensics
- automatically generate a service ticket in your favorite Ticketing System/PSA
- configure a **Smart-Tag** to change Cyber Hawk's behavior
- issue an **Ignore Rule** to ignore the alert and prevent the same “false-positive” from being generated again in the future

Cyber Hawk performs scheduled IT network assessment scans on a daily and/or weekly basis. When *Anomalies*, *Changes*, or *Threats* (ACT) are identified on the network, Cyber Hawk issues Security Policy Violation Alerts according to rules that you configure.

Anomalies, Changes, and Threats

Each time Cyber Hawk executes a pre-scheduled scan, it’s on the look-out for three classifications of internal network security issues: Anomalies, Changes, and Threats.

- **Anomalies** are suspicious activities and findings that are out of the ordinary and unexpected and that should be investigated. Examples of anomalies are users logging in at times outside their historical patterns, or a USB drive plugged into a

computer that has been tagged as being "locked down."

- **Changes** are recorded variances from previous scans linked to specific aspects of the network environment that could represent a threat. Examples of suspicious changes are a user's security permission promoted to administrative, or a new device added to the network that wasn't there before.
- **Threats** are defined as clear and recognizable dangers to the network environment that need fast attention. Examples of threats would be a critical security hole or a machine in the "DMZ" that hasn't been patched in 30 days.

Every day Cyber Hawk looks at a broad range of assets and configurations in search of anomalies, changes and threats, including: Wireless Networks, Network Devices, User Behavior, Computers, Printers, DNS entries, Switch Port Connections (Layer 2/3), and Internal Network Vulnerabilities. It also looks at issues specifically for environments subject to HIPAA and PCI compliance.

And, on a weekly basis, Cyber Hawk will also notify you of changes in the large categories of: Access Control, Computer Security, Wireless Access, and Network Security.

Cyber Hawk Components

In order to use and get the most out of Cyber Hawk, you will need the following components:

Cyber Hawk Component	Description
Cyber Hawk Appliance	This is the Cyber Hawk Appliance software application installed on the target network. You have two install options. These include 1) installing the **RapidFire Tools Server** Windows Service, or 2) a **Virtual Appliance** that requires a user supplied Microsoft Hyper-V based system or a VMware based system.
Optional Small Form Factor Server Computer	This is an optional hardware component that can be purchased from RapidFire Tools to host and operate the Cyber Hawk Appliance. It is a small, portable server computer which plugs into the target network through an Ethernet connection.
Diagnostic Tool	This tool is used for configuring and troubleshooting the Cyber Hawk Appliance. The Diagnostic Tool should be run on the same network as the Cyber Hawk Appliance to perform diagnostics checks such as for Cyber Hawk Appliance connectivity.
Network Detective Application	This is the same Network Detective desktop application and report generator that is used with any other Network Detective modules. This application contains additional features to manage the Cyber Hawk Appliance remotely.
The Network Detective Service Plan Creator and the Service Catalog	Cyber Hawk users have access to Network Detective's unique "Service Plan Creator" tool that gives you the ability to modify our starter Service Plans, or create your own plans from scratch. You define and name the offerings based on the security policies that you want to enforce, and the tool automatically generates a "Service Plan Catalog" (or catalogs), and "Service Plan Matrix" sheet that compares your plans to help you sell them to your clients and prospects Once you sell one of your plans to your client, simply "apply" the plan to the Cyber Hawk assigned to that client and its Service Policy Violation detection capability is then automatically configured to deliver that exact plan.

Cyber Hawk Component	Description
RapidFire Tools Portal	The RapidFire Tools Portal is used to process Investigate Alert Action Requests and Ignore Alert Action Requests created in response to Anomalies, Changes, or Threats (ACT) detected by the Cyber Hawk Appliance. The Portal acts as an ACT “triage center” that enables technicians to view a “To-Do” list of Investigate Alert Action Requests and Ignore Alert Action Requests and to enable processing of these requests by: • transferring the requests to Ticketing/PSA Systems such as Autotask, ConnectWise, and Tigerpaw • using the Portal to modify Cyber Hawk Smart-Tags to configure the Cyber Hawk Appliance to more effectively detect Security Policy violations and address False Positives • creating Ignore Rules to address Alert False Positives • completing a given Action Request To access the RapidFire Tools Portal, visit the default web site URL of https://www.youritportal.com.
Portal Integration with Ticketing Systems/PSAs	To set up Cyber Hawk integration of the Autotask, ConnectWise, or Tigerpaw ticketing/PSA systems with the RapidFire Tools Portal, please refer to "Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk" on page 97.