



USER GUIDE

Cyber Hawk (previously known as Detector)

Detecting and Responding to IT Security Policy Violations

Contents

Introduction to Cyber Hawk	9
<u>Cyber Hawk Overview</u>	9
<u>Cyber Hawk Components</u>	11
Setting Up Cyber Hawk	13
<u>Initial Cyber Hawk Set Up</u>	13
Step 1 — Provision Cyber Hawk Appliance ID in Network Detective	13
Step 2 — Install Cyber Hawk and Create a New Site	14
Step 3 — Associate Cyber Hawk with a Site and Access Cyber Hawk Settings	15
<u>Configure Cyber Hawk Using the Setup Wizard (Virtual Appliance)</u>	18
Step 1 — Configure Scan Settings	19
Step 2 — Schedule Scans and Alert Notifications	29
Tips for Scheduling the Level 2 Scan	30
Step 3 — Configure Tech Email Groups	31
Step 4 — Configure End User Email Groups	34
Step 5 — Perform Pre-Scan Analysis	35
Step 6 — Perform Initial Cyber Hawk Scan	38
Step 7 — Configure Policies	38
Step 8 — Configure Notifications	41
Step 9 — Configure Smart Tags	42
Step 10 — Set Up RapidFire Tools Portal	44
<u>Provisioning Additional Cyber Hawk Appliances for Deployment</u>	45
<u>Provisioning Additional Cyber Hawk Appliances for Deployment (Classic)</u>	47
<u>Provisioning Additional Detector Legacy Appliances for Deployment</u>	50
Cyber Hawk Security Policy Violation Alerts	52
<u>Security Policy Violation Alert Notification Rule Actions</u>	52
<u>Set Up End User Alert Notifications</u>	53
More about End User Security Policy Violation Alert Notifications	55
<u>Set Up Tech Group Alert Notifications</u>	56

<u>Managing and Deleting “Ignore” Alert Rules</u>	58
<u>Cyber Hawk Security Alert Email Summaries</u>	59
<u>Security Policy Details</u>	63
Cyber Hawk Alert Response Workflows	68
<u>Create a Ticket from an Alert</u>	68
<u>Respond to an Alert Investigation Request (Tech Group)</u>	69
Three Alert Response Scenarios using Cyber Hawk	72
#1: "Attempted access of system restricted to IT administrators only by a non-IT admin"	73
#2: "Unauthorized access to a computer in the Cardholder Data Environment (CDE)"	73
#3: "New medium severity internal vulnerabilities were found"	74
<u>Send the Tech Group an Alert Investigation Request (End User)</u>	76
<u>Request that the Tech Group Ignore an Alert (End User)</u>	78
<u>Process an Ignore Alert Request (Tech Group)</u>	80
Using the RapidFire Tools Portal	84
<u>Alerts</u>	84
How Long Do Alerts Last in the Portal?	85
View and Process Alerts	85
Alert Item Statuses	87
Filter Alert Queue by Status	88
Revert Completed Alerts Back to the To Do Items	89
<u>To Dos</u>	93
How Long Do To Do Items Last in the Portal?	94
View and Process To Dos	94
Create To Do Items from Alerts	94
<u>Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk</u>	97
Step 1 — Gather Credentials and Set Up your PSA System	97
Step 2 — Set Up a Connection to your Ticketing System/PSA	98
Step 3 — Map your Cyber Hawk’s Site to a Ticketing System/PSA Connection	103
Set Up Autotask Integration	105

Set Up ConnectWise REST Integration	108
Step 1 — Download and Install the ConnectWise Manage Internet Client Application	109
Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with	109
Create Minimum Permissions Security Role for API Member	110
Step 3 — Create an API Key in the ConnectWise Ticketing System	110
Step 4 — Configure Service Tables in ConnectWise	111
Set Up ConnectWise SOAP Integration	112
Set Up Kaseya BMS Integration	114
<u>Set Up RapidFire Tools Portal Branding</u>	115
Set Custom Portal Theme	117
Set Custom Portal Subdomain	118
Set Custom Company Name	119
Set Custom Company Logo	120
<u>Set Up a Custom Subdomain to Access the RapidFire Tools Portal</u>	121
<u>Set Up Custom SMTP Server Support</u>	124
<u>Allow Clients to Access Portal and Manage Tickets</u>	127
Step 1 — Create Site Restricted User in Portal	127
Step 2 — Assign User to Site	128
Step 3 — Assign User to Technician Role	129
<u>Manage Users (Global Level)</u>	130
Users and Global Access Roles	130
Add User at Global Level	132
Edit User at Global Level	134
<u>RapidFire Tools Portal Site Roles</u>	136
<u>Manage Site Data Collectors</u>	138
Data Collector Commands	139
Smart Tags	142
<u>Defining Smart Tags</u>	142
<u>Using Smart Tags</u>	146
<u>Add and Configure Smart Tags</u>	147

Step 1 — Select the Site	147
Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings	147
Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded	148
Step 4 — Select and Apply Recommended Tags	150
Step 5 — View Applied Tags	152
Step 6 — Select and Apply Additional Smart Tags from the Available Tags Window	152
<u>Export and Import Smart Tags</u>	156
Export Smart Tags	156
Step 1 — Select the Site	156
Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings	157
Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded	157
Step 4 — Export Smart Tags	158
Import Smart Tags	159
Step 1 — Select the Site	159
Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings	159
Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded	160
Step 4 — Import a Smart Tags Configuration File	160
<u>Delete Smart Tags</u>	162
Step 1 — Open the Applied Tags Window and Select the Tag for Deletion	162
Step 2 — Select the Tag and Delete	162
Service Plans and Catalogs	164
<u>Using the Service Plan Creator</u>	164
<u>Create Service Plans and Service Catalogs</u>	165
Step 1 — Create a New Service Plan	165
Step 2 — Assign Security Policies to Your Service Plan	167
Step 3 — Define Reports Deliverables to be Included in the Service Plan	170
Step 4 — Create a Service Catalog	173
<u>Generate a Service Catalog Document</u>	176
<u>Generate a Service Plan Matrix Document</u>	177
<u>Generate a Sample Master Services Agreement for a Service Plan</u>	180

Step 1 — Opening Existing Network Detective Site that is Associated with your Cyber Hawk	180
Step 2 — Access the Cyber Hawk Settings	181
Step 3 — Select the Policy Configuration Option	181
Step 4 — Generate Master Service Agreement Option	182
Step 5 — Enter the MSP information, Customer information, and Service Plan Cost Details	183
Step 6 — Confirm Acceptance of the Disclaimer and Generate the Sample MSA	184
<u>Managing Service Plans</u>	185
Edit a Service a Plan	185
Delete a Service Plan	186
<u>Managing Service Catalogs</u>	188
Add Service Plans to a Catalog	188
Edit a Service Catalog	190
Remove (Delete) a Service Catalog from the List of Catalogs	191
Delete (Exclude) Service Plans from a Catalog	193
<u>Default Cyber Hawk Service Plans</u>	194
Appendices	198
<u>Configure Cyber Hawk Using the Setup Wizard (RapidFire Tools Server)</u>	200
Step 1 — Configure Scan Settings	201
Step 2 — Schedule Scans and Alert Notifications	209
Step 3 — Configure Tech Email Groups	210
Step 4 — Configure End User Email Groups	213
Step 5 — Perform Pre-Scan Analysis	215
Step 6 — Perform Initial Cyber Hawk Scan	218
Step 7 — Configure Policies	218
Step 8 — Configure Notifications	221
Step 9 — Configure Smart Tags	222
Step 10 — Set Up RapidFire Tools Portal	224
<u>Additional Scan Host Configuration Options and Requirements</u>	226
Scan Host Diagram	226
Scan Host Requirements	227
Assigning Scan Hosts in a Domain Environment	227

<u>Pre-Scan Network Configuration Checklist</u>	229
Checklist for Domain Environments	229
Checklist for Workgroup Environments	231
<u>RapidFire Tools Server vs. Virtual Appliance</u>	233
<u>Sample Daily Alerts and Weekly Notices</u>	235
Sample Tech Alert	235
Sample End User Alert	235
Sample Weekly Notice	236
<u>Edit Policies Enforced at a Site</u>	237
<u>Unitrends Backup Alerts</u>	238
Requirements for Unitrends Backup Alerts	238
How to enable Unitrends Backup Alerts (Web Console)	239
How to enable Unitrends Backup Alerts (Network Detective)	240
<u>Cyber Hawk Basic and Advanced Breach Detection System</u>	243
Breach Detection: Basic vs. Advanced Scanning and Alerting	243
Breach Detection Scan Setup Prerequisites	244
Enable Breach Detection and Alerting with Cyber Hawk	244
Step 1 — Purchase ABDS Add-on in RapidFire Tools Portal	245
Using an ABDS Subscription with another Cyber Hawk Site	247
Step 2 — Configure Breach Detection Policy in Network Detective	247
Step 3 — Configure Schedule for Breach Scan and Alerts in Network Detective	249
Breach Detection Security Alerts	251
Basic: NO ABDS Add-On Subscription	251
Advanced: WITH ABDS Add-On Subscription	252
How Does Breach Detection Work?	253
What does Breach Detection Look For?	255
Why go with Advanced Breach Detection?	255
Example #1: Basic Alert for Potential Malware	255
Example #2: Advanced Alert for Potential Malware	256
<u>Setting up Automatic Report Generation Using the Reporter Appliance</u>	258
Step 1 – Set up a Connector for the Site	258
Step 2 – Associate a Reporter with the Site	259

Step 3 – Set the Cyber Hawk Scan to Upload the Scan Data to Reporter 260

Step 4 – Set up Reporter to Automatically Generate Reports 261

Audit Log 261

Two-Factor Authentication for RapidFire Tools Portal 262

 Enable Two-Factor Authentication 262

 Disable 2FA 265

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.

In the RapidFire Tools Portal you can:

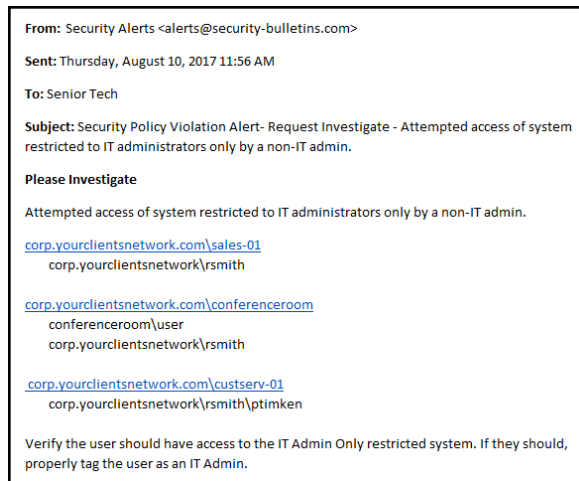
- review the issue’s forensics
- automatically generate a service ticket in your favorite Ticketing System/PSA
- configure a **Smart-Tag** to change Cyber Hawk’s behavior
- issue an **Ignore Rule** to ignore the alert and prevent the same “false-positive” from being generated again in the future

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	<p>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.</p> <p>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.</p>

Cyber Hawk Component	Description
<p>RapidFire Tools Portal</p>	<p>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:</p> <ul style="list-style-type: none"> • 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 <p>To access the RapidFire Tools Portal, visit the default web site URL of https://www.youritportal.com.</p>
<p>Portal Integration with Ticketing Systems/PSAs</p>	<p>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.</p>