RapidFireTools®
A Kaseya COMPANY

DETECTING AND PROTECTING:
IT Security Discovery Checklists

Everything you need to know to achieve cyber resiliency

On average, it takes an organization 277 days or NINE MONTHS to detect a breach due to low threat awareness and visibility of the network (IBM). When it happens to you, your business is at critical risk. You can combat this with tools that give you an **"X-ray vision" of your network to build a robust IT environment.**

We've developed a set of checklists that you can use to ensure you have visibility into every threat your organization faces. These checklists will show you the industry standard discovery procedures you should be implementing to identify hidden IT issues and weaknesses so you can prevent your network from being exploited.

DISCOVER IT VULNERABILITIES BEFORE THE HACKERS DO

Vulnerability management can be a relatively simple process that can be set up as a part of your day-to-day IT routine.

Pro tip: With VulScan, you can automate a lot of the heavy lifting after the initial setup.

- □ Set up and configure the scanner(s) on each managed network. It takes less than an hour to set up the first scanner, and the more scanners that are set up, the quicker the process. On average, it takes about 10 minutes to set up a new scanner

- □ Bind the scanner to a specific client site and schedule the scan; also, scan tasks can be changed at any time.

- □ Review the alerts for new vulnerabilities as they come in — if there is nothing new since the last scan, there is nothing to do until the next security hygiene SLA window.

- □ Review the dashboard based on the designated SLA frequency and drill into the issues that need addressing and create rules for any false positive alerts.

- □ Remediate all high and medium risks.

DISCOVER HIDDEN IT RISKS AND ISSUES BEFORE THEY BECOME BIG PROBLEMS

Conduct regular IT security assessments — on prem, in the cloud and remote computers.

Pro tip: With a powerful IT assessment tool like **Network Detective Pro**, you can automatically scan networks and individual endpoints, to collect the data, analyze the assessment results and generate a wide range of professionally designed reports.

- □ Collect security data from all environments — on-premises networks/satellite offices/remote/work-from-home users/cloud assets.

- □ Review the schedule of your data collectors to ensure the frequency is commensurate with the cadence of typical changes to identify issues before they become risks.

- □ Generate specialized IT security assessment reports that cover the entire IT risk assessment:

  - ✓ The Consolidated Risk Report
  - ✓ The Data Breach Liability Report
  - ✓ The Dark Web Credential Compromise Report
  - ✓ The MS Cloud Security Report

- □ Focus on the most important risks and issues with dynamically generated management plans.

- □ Identify remediation opportunities to enhance security.

- □ Generate executive infographic summary reports to demonstrate value to your organization’s leadership and justify increased resource needs.

DISCOVER INTERNAL THREATS BEFORE THEY TAKE YOU DOWN

More than 70% of all cybersecurity incidents today are the result of internal security issues inside the network firewall.

Pro tip: With **Cyber Hawk**, you can automatically scan your networks on a regular basis to identify insider threats and obtain alerts with guidance on how to address them.

□ Install a simple software appliance on each network that's designed to run regularly to pick up unauthorized changes and suspicious end-user behaviors.

□ Run automated daily scans and get alerted to:

- potential new threats
- anomalous user behaviors
- misconfigurations that create risk.

□ Ensure daily alerts are sent with a list of anomalies, changes and threats to catch security issues as they arise.

□ Sort issues by high to low priority or by issue type.

□ Resolve issues by following the step-by-step-remediation suggestions provided by your software.

□ Integrate alerts into service tickets with PSA software solutions to increase efficiency.

□ Utilize smart tags to enrich the detection system and increase the quality of the alerts

Know IT All

Discover issues
Identify risks
Detect threats

RapidFire Tools offers a suite of software modules that give IT professionals the network visibility they need to “Know IT All.” Each module is complete, automated and priced right for any organization.

They work alone or as a powerful stack that is tightly integrated through a common web-based portal, shared users and sites, and deep workflow integrations that reduce risk and drive improved IT management efficiency.

NETWORK DETECTIVE PRO

for IT Assessments and Documentation

Discover hidden user and system issues before they cause problems

Learn more

VULSCAN

for Network Vulnerability Scanning

Identify risks by discovering hidden internal and external network vulnerabilities

Learn more

CYBER HAWK

for Internal Threat Detection

Detect hidden internal threats caused by unauthorized network changes and susppicious user activity

Learn more

Request a demo with one of our specialists to understand how our suite of solutions can ensure nothing about your network ever catches you off guard.

REQUEST A DEMO