RAPIDFIRE TOOLS
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 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 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.

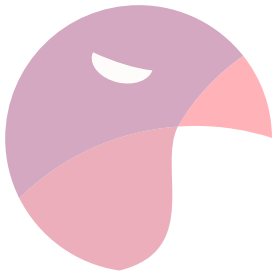
- [ ] Set up and configure the scanner(s) on each managed network. It takes less than an hour to set up the first scanner, and the more scanners that are set up, the quicker the process. On average, it takes about 10 minutes to set up a new scanner
- [ ] Bind the scanner to a specific client site and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

DETECT CRITICAL IT CHANGES BEFORE THEY TAKE YOU DOWN

More than 70% of cybersecurity incidents today are the result of undetected changes or activities that no firewall or antivirus could have prevented.

Pro tip: With Cyber Hawk, you can automatically scan your networks on a regular basis to identify hidden threats caused by critical changes 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.



PROVE YOUR INFOSEC AND COMPLIANCE PROGRAMS ARE WORKING.

86% of organizations are our of compliance with their own IT policies

Pro tip: With a tool like Compliance Manager GRC you can reduce risk and meet ANY industry, regulatory or internal security requirements without adding staff or stretching your budget.

- [ ] Pick your standards
  - Select one of the government or industry cybersecurity standard templates.
- [ ] Generate the cyber security policies & procedures manual(s)
- [ ] Run a rapid baseline assessment (first time only)
  - Answer a guided series of questions that directly tie in with the requirements of the cybersecurity standard(s) you have selected.
- [ ] Perform a full technical security assessment & controls assessment.
- [ ] Generate a set of technical assessment reports based on the discovery process.
- [ ] Quantify and prioritize the relative risk of each issue discovered.
- [ ] Assign individuals or groups to each task and set a due date for the task to be completed.
- [ ] Generate evidence of compliance for all your requirements.
- [ ] Engage your employees in compliance
  - Provide all end-users with digital access to all company policies and procedures and require them to attest to the fact that they have reviewed them and agree to them.
  - Record the responses.
  - Provide all end-users with a basic security awareness training course and monitor who has completed the training and passed a post-training quiz.

- [ ] Manage your vendor risk
  - Make sure your strategic vendors are meeting any IT security requirements that you impose on them using a branded, self-serve Vendor Risk Management portal.

- [ ] Perform periodic reassessments and compliance confirmation.
- [ ] Use stored values for previous assessments for any standard.
- [ ] Generate an Auditor's checklist and identify any changes that may move you out of compliance.
- [ ] Address any new gaps, and upload current evidence of compliance.

RAPIDFIRE TOOLS
A Kaseya COMPANY

YOUR COMPLETE
IT Risk Management Toolkit

**REDUCE RISK.
ACROSS EVERY DEVICE.
EVERY USER.
EVERYWHERE.**

You can't protect what you can't see, analyze and document. Even with the most sophisticated IT security stack, things go wrong. End users get spoofed by phishing attacks. Software updates don't complete. Time-constrained IT technicians make honest mistakes.

Our risk management platform gives you the power to discover hidden issues that can take your network down. You and your stakeholders can rest assured that all your IT security requirements are being met.

Four Products. One Integrated Platform.

Network Detective Pro

Network Scanning and IT Assessments

Identify, measure and manage network issues and risks.

VulScan

Vulnerability Management

Discover network threats & vulnerabilities.

Cyber Hawk

Change Detection

Detect unauthorized network changes and suspicious activity.

Compliance Manager GRC

IT Governance, Risk and Compliance

Demonstrate your InfoSec and compliance programs are working.

Request a Demo

Discover how our suite of solutions can ensure nothing about your network ever catches you off guard.