



# Configuring a Malware Detection and Forensics SecurityCenter Scan

May 2, 2016

(Revision 3)

---

## Table of Contents

Introduction .....	3
Add Policy .....	3
Basic Settings .....	3
Enable Plugins.....	5
Brute Force: General Settings .....	7
Windows: Malware Files.....	8
Expanded Malware Scanning.....	8
Report: Output .....	9
Authentication: Windows .....	10
Add Credential .....	11
Add Scan .....	12
Policy and Credential .....	14
Settings: Advanced .....	15
Add Dashboard .....	16
Choose the Monitoring Related Dashboards and Components .....	16
Locate the Indicators Dashboard .....	17
Review the Details of the Indicators Dashboard .....	18
Wait for the Dashboard to be Added .....	19
Wait for the Dashboard Components to Update .....	20
Add Asset .....	21
Choose to Add an Asset List .....	21
Create Dynamic Asset List .....	21
Verify Asset List Created Successfully .....	22
Vulnerabilities (Cumulative View) .....	22
Look at the Cumulative View of Results .....	23
Filter on the Executable Code File Name that has been Identified as Malware.....	24
Review the List of Plugin Results that Contain References to the Malware .....	24
Change the View to “IP Summary” .....	25
ThreatLists and Watches: .....	25
About Tenable Network Security .....	25

## Introduction

This document offers a suggested approach to configure a malware detection and forensics credentialed scan in Tenable SecurityCenter™ that will work in most environments without modification. It also offers suggested steps to configure additional objects in SecurityCenter to help with interpreting scan results.

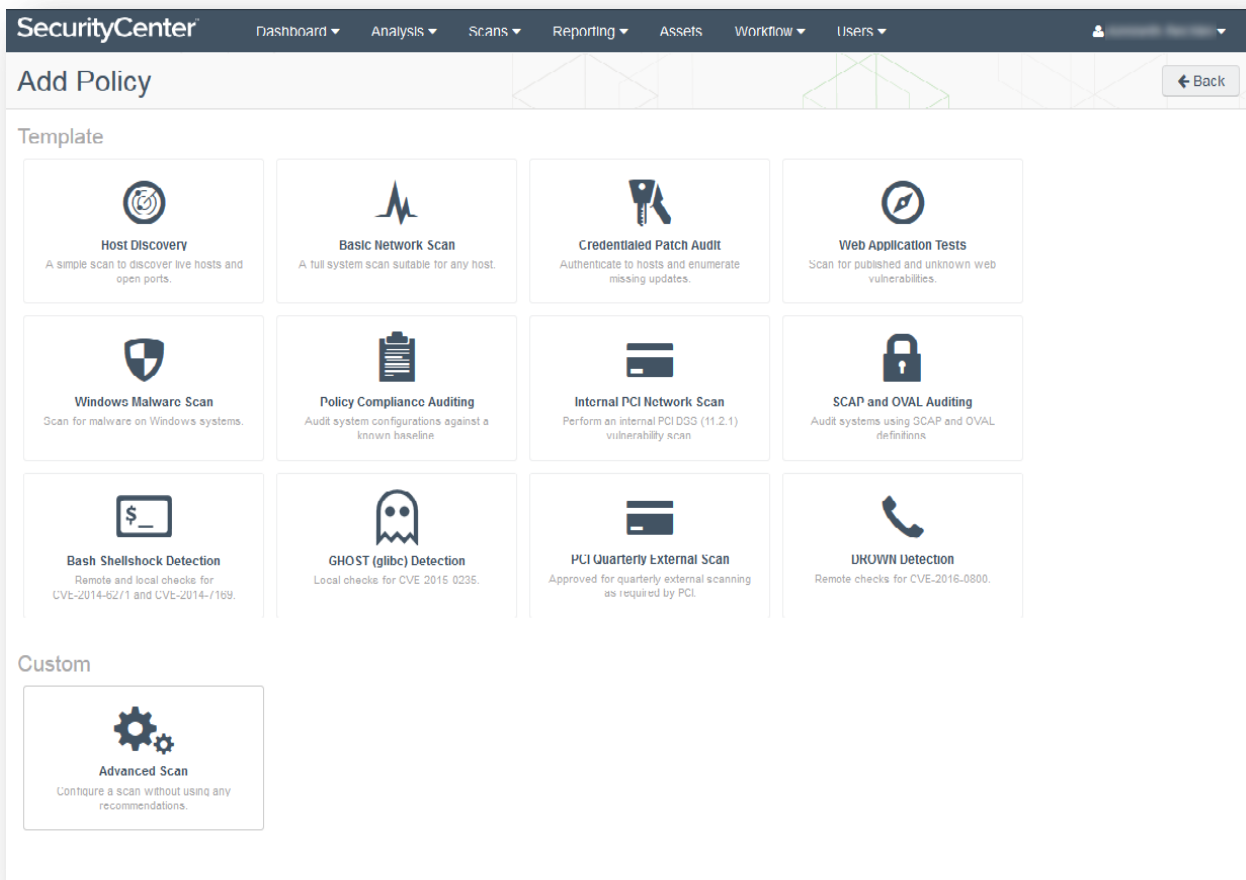
A basic understanding of the SecurityCenter GUI to find the menu options for adding objects such as repositories, policies, scans, asset lists, and performing queries is highly recommended. This document is not intended as a replacement for official Tenable training or documentation. For more details on adding objects through SecurityCenter, please refer to the [SecurityCenter User Guide](#).

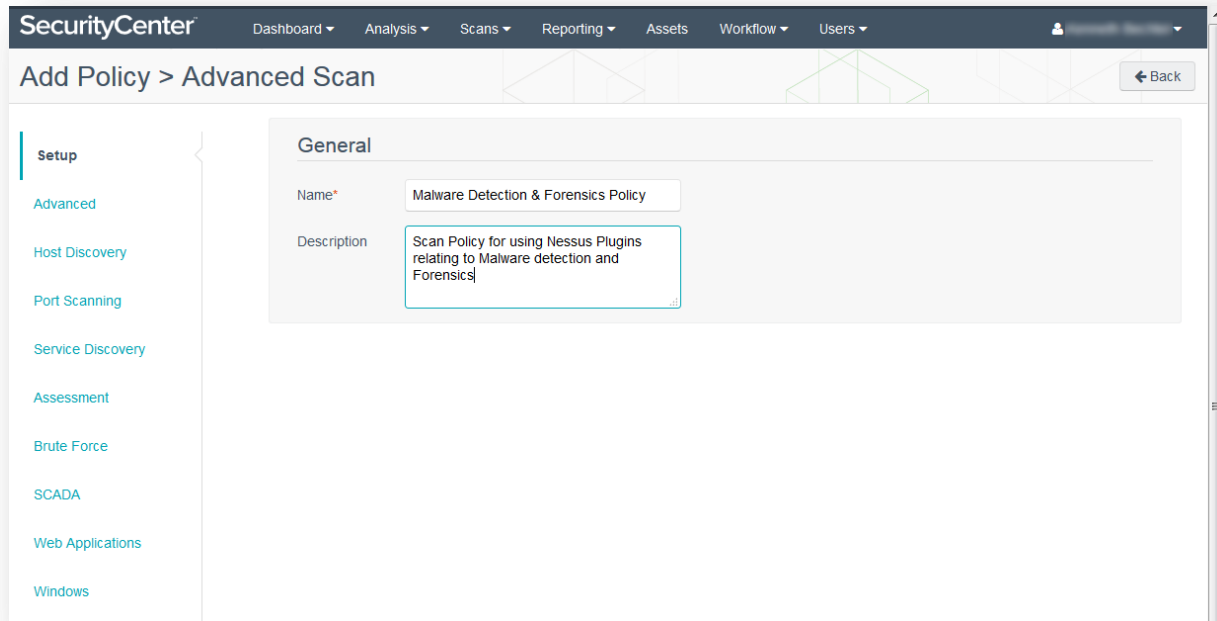
When following the configuration steps, please note that some settings may be set correctly by default, depending on the SecurityCenter version and plugin versions being used. Screenshots are provided below configuration steps to help avoid any confusion.

## Add Policy

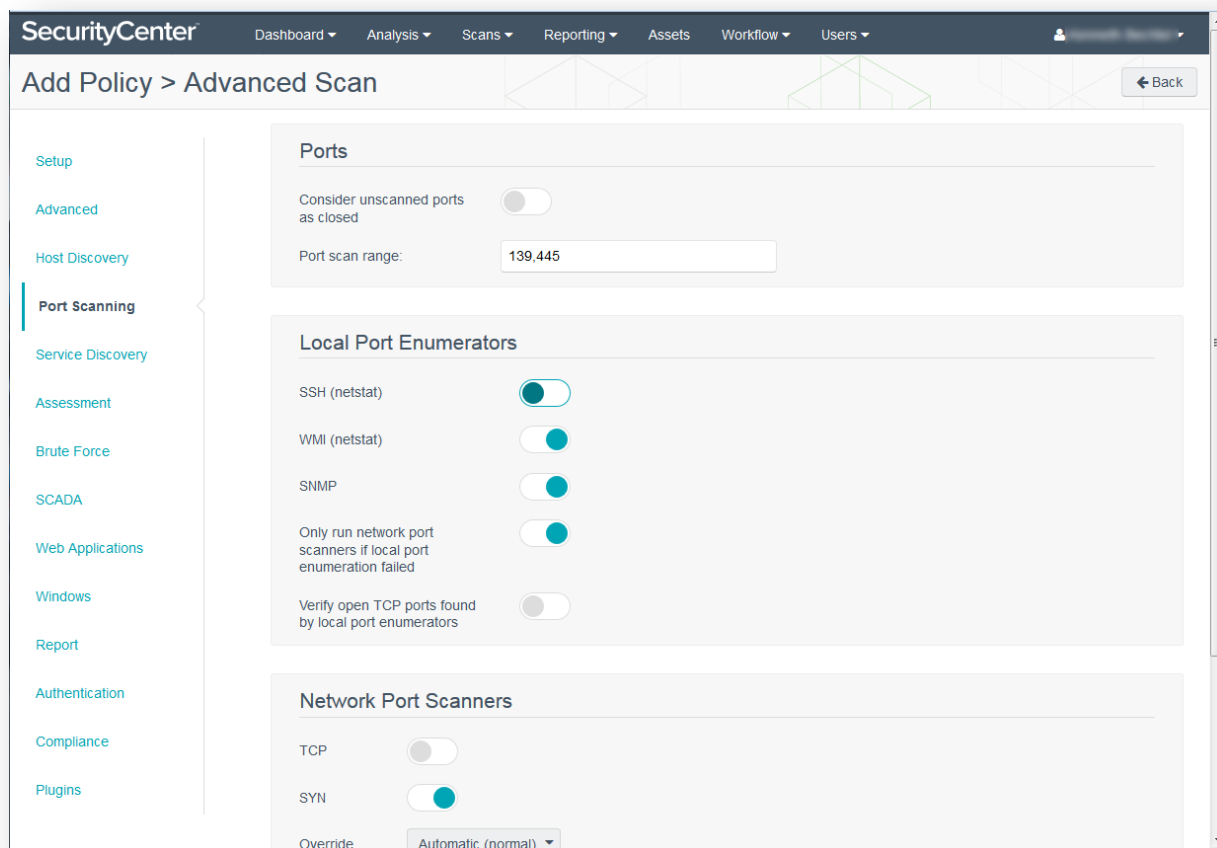
### Basic Settings

1. As a Security Manager user, add an Advanced Scan policy.





2. Under "Network Port Scanners", ensure "TCP" is disabled and enable "SYN", "WMI (netstat)", and "Ping Host".
3. Set the "Port scan range" to "139,445".



---

## Enable Plugins

Enable the following Nessus<sup>®</sup> plugins:

### Authentication Diagnostic Help

- 10919 Open Port Re-check
- 19506 Nessus Scan Information
- 21745 Authentication Failure - Local Checks Not Run
- 10394 Microsoft Windows SMB Log In Possible
- 10395 Microsoft Windows SMB Shares Enumeration
- 10400 Microsoft Windows SMB Registry Remotely Accessible
- 24269 Windows Management Instrumentation (WMI) Available
- 26917 Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

### Host Identification

- 10150 Windows NetBIOS / SMB Remote Host Information Disclosure
- 12053 Host Fully Qualified Domain Name (FQDN) Resolution
- 45590 Common Platform Enumeration (CPE)
- 55472 Device Hostname
- 35716 Ethernet Card Manufacturer Detection

### Botnet

- 52669 Host is Listed in Known Bot Database
- 58429 DNS Server Listed in Known Bot Database
- 58430 Active Outbound Connection to Host Listed in Known Bot Database
- 59713 Active Inbound Connection From Host Listed in Known Bot Database

### Malicious Processes

- 59275 Malicious Process Detection
- 59641 Malicious Process Detection: Potentially Unwanted Software
- 64687 Malicious Process Detection: APT1 Software Running
- 64788 Malicious Process Detection: Malware Signed By Stolen Bit9 Certificate
- 65548 Malicious Process Detection: User Defined Malware Running

### Windows Processes

- 70329 Window Process Information
- 70331 Window Process Module Information

### Autoruns

- 70613 Microsoft Windows AutoRuns LSA Providers
- 70614 Microsoft Windows AutoRuns Appinit DLLs
- 70615 Microsoft Windows AutoRuns Boot Execute
- 70616 Microsoft Windows AutoRuns Codecs
- 70617 Microsoft Windows AutoRuns Explorer

- 70618 Microsoft Windows AutoRuns Registry Hijack Possible Locations
- 70619 Microsoft Windows AutoRuns Internet Explorer
- 70620 Microsoft Windows AutoRuns Known DLLs
- 70621 Microsoft Windows AutoRuns Logon
- 70622 Microsoft Windows AutoRuns Network Providers
- 70623 Microsoft Windows AutoRuns Print Monitor
- 70624 Microsoft Windows AutoRuns Report
- 70625 Microsoft Windows AutoRuns Scheduled Tasks
- 70626 Microsoft Windows AutoRuns Services and Drivers
- 70627 Microsoft Windows AutoRuns Setup
- 70628 Microsoft Windows AutoRuns Unique Entries
- 70629 Microsoft Windows AutoRuns Winlogon
- 70630 Microsoft Windows AutoRuns Winsock Provider
- 74442 Microsoft Windows Known Bad AutoRuns / Scheduled Tasks

## Reputation

- 70767 Reputation of Windows Executables: Known Process(es)
- 70768 Reputation of Windows Executables: Unknown Process(es)
- 70943 Reputation of Windows Executables: Never seen process(es)
- 71262 Reputation of Linux Executables: Never seen process(es)
- 71264 Reputation of Mac OS X Executables: Never seen process(es)

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

Setup  
Advanced  
Host Discovery  
Port Scanning  
Service Discovery  
Assessment  
Brute Force  
SCADA  
Web Applications  
Windows  
Report  
Authentication  
Compliance

### Plugins

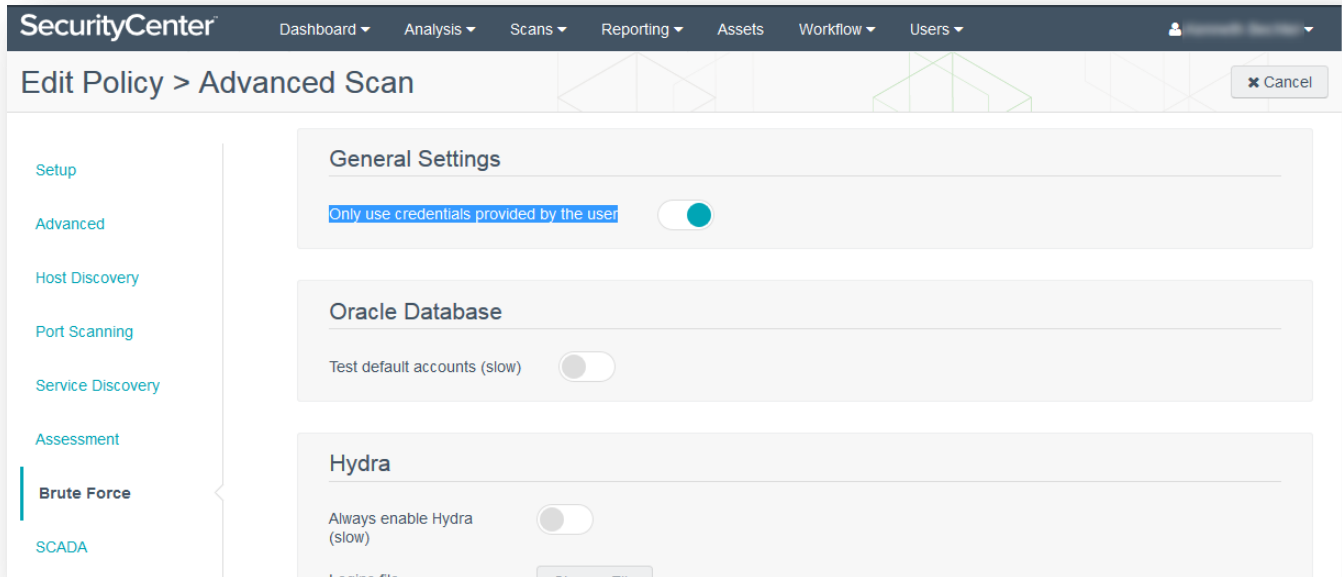
Windows Back Show Enabled / Show All

Status	Plugin Name	Plugin ID
Enabled	Malicious Process Detection	59275
Enabled	Malicious Process Detection: APT1 Software Running	64687
Enabled	Malicious Process Detection: Malware Signed By Stolen Bit9 Certificate	64788
Enabled	Malicious Process Detection: Potentially Unwanted Software	59641
Enabled	Malicious Process Detection: User Defined Malware Running	65548
Disabled	Microsoft Malicious Software Removal Tool Installed	66424
Disabled	MS Security Advisory 3074162: Vulnerability in Microsoft Malicious Software Removal Tool Could Allow Elev...	84742

Enable Selected / Disable Selected

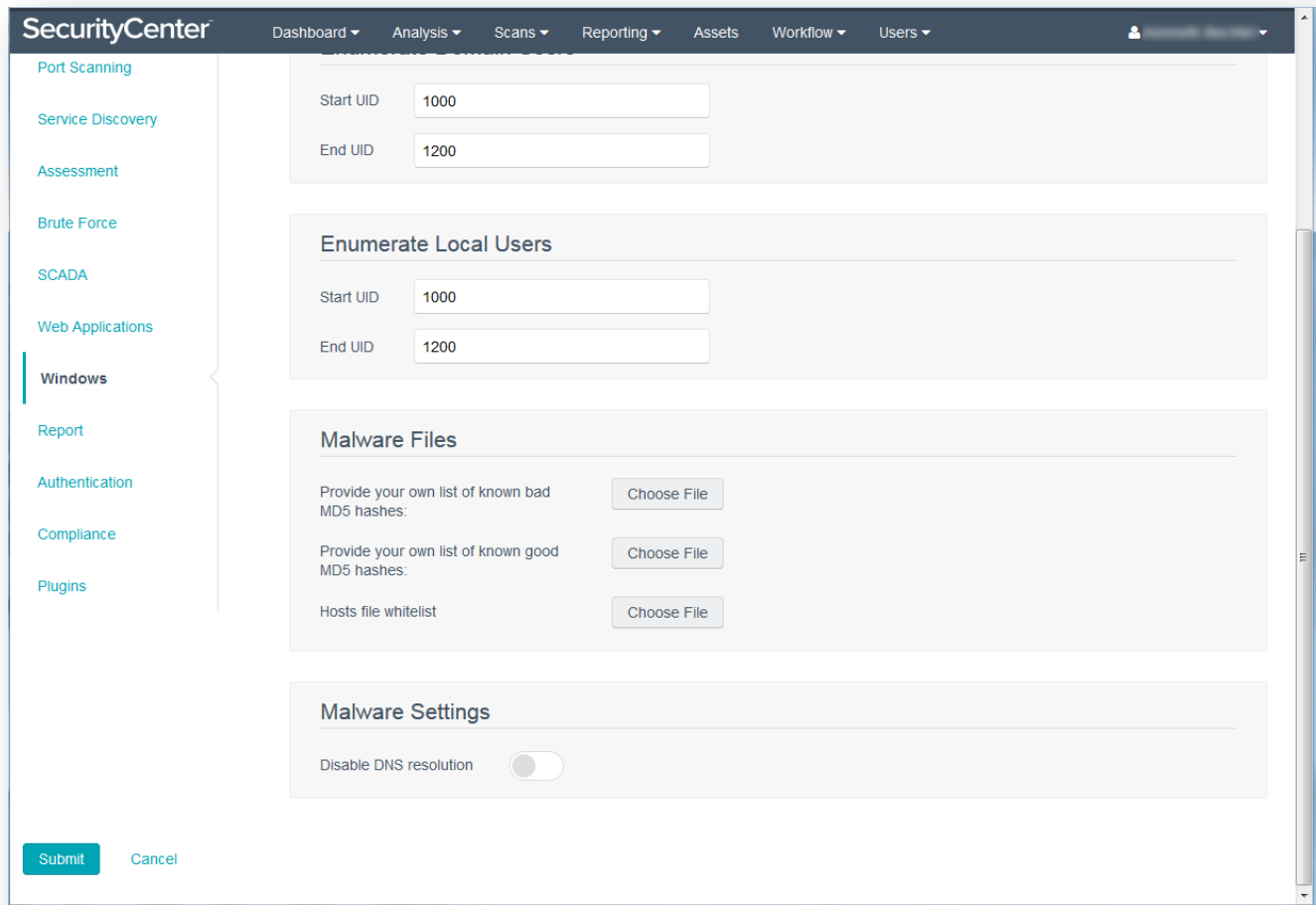
## Brute Force: General Settings

Enable “Only use credentials provided by the user”.



## Windows: Malware Files

Upload custom MD5 hashes, if any. Skip this step if you do not have any MD5 hashes to provide.



The screenshot displays the SecurityCenter web interface. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The left sidebar lists various scanning categories: 'Port Scanning', 'Service Discovery', 'Assessment', 'Brute Force', 'SCADA', 'Web Applications', 'Windows' (highlighted), 'Report', 'Authentication', 'Compliance', and 'Plugins'. The main content area is titled 'Windows' and contains several sections:

- Port Scanning:** Two input fields for 'Start UID' (value: 1000) and 'End UID' (value: 1200).
- Enumerate Local Users:** Two input fields for 'Start UID' (value: 1000) and 'End UID' (value: 1200).
- Malware Files:** Three sections, each with a 'Choose File' button:
  - 'Provide your own list of known bad MD5 hashes:'
  - 'Provide your own list of known good MD5 hashes:'
  - 'Hosts file whitelist'
- Malware Settings:** A toggle switch for 'Disable DNS resolution', which is currently turned off.

At the bottom left, there are 'Submit' and 'Cancel' buttons.

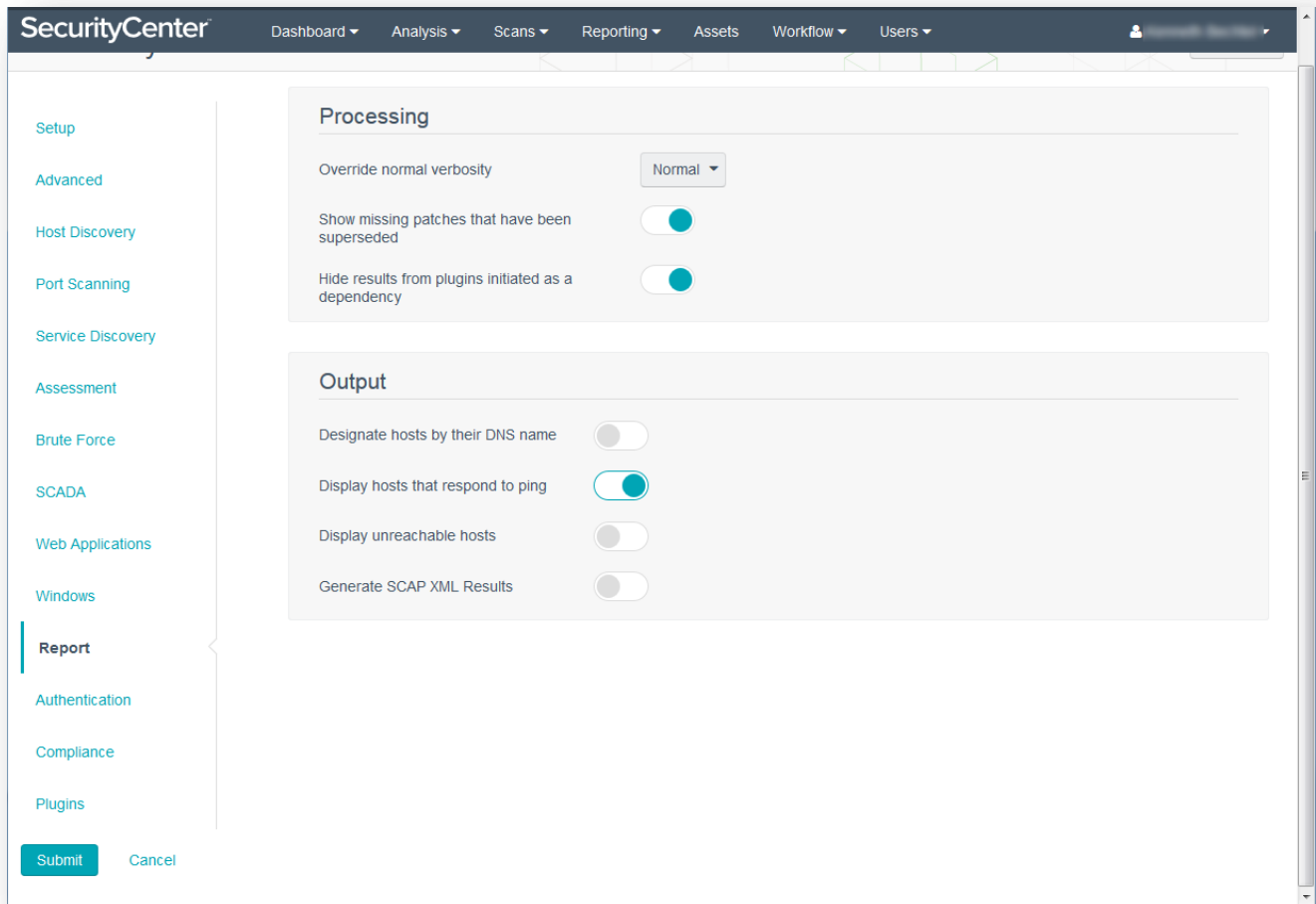
## Expanded Malware Scanning

With Nessus 6.6, malicious file detection is expanded to now scan directories of files on disk. When specific directories you want to scan are entered into a scan policy, Nessus will report any malware or suspicious files discovered in the scan.



## Report: Output

Enable “Display hosts that respond to ping”.



## Authentication: Windows

1. Enable “Start the Remote Registry service during the scan”.
2. Enable “Enable administrative shares during the scan”.

The screenshot displays the SecurityCenter web interface. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The left sidebar lists 'SCADA', 'Web Applications', 'Windows', 'Report', 'Authentication' (highlighted), 'Compliance', and 'Plugins'. The main content area is divided into several sections:

- Additional UDP port #3\***: A text input field containing the value '161'.
- SSH**: A section with three fields: 'known\_hosts file' with a 'Choose File' button, 'Preferred port' with a text input field containing '22', and 'Client version' with a text input field containing 'OpenSSH\_5.0'.
- Windows**: A section with four toggle switches, all of which are turned on (indicated by a teal circle):
  - Never send credentials in the clear
  - Do not use NTLMv1 authentication
  - Start the Remote Registry service during the scan
  - Enable administrative shares during the scan
- Plaintext Authentication**: A section with three toggle switches, all of which are turned off (indicated by a grey circle):
  - Perform patch audits over telnet
  - Perform patch audits over rsh
  - Perform patch audits over rexec

## Add Credential

Consider setting up a dedicated Active Directory domain user account for credentialed scanning. Test the account in a lab environment or on one or two hosts to ensure the account has the correct permissions.

**SecurityCenter** Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾

### Add Credential

← Back

**General**

Name\*

Description

**Credential**

Type

Authentication Method

Username\*

Password\*

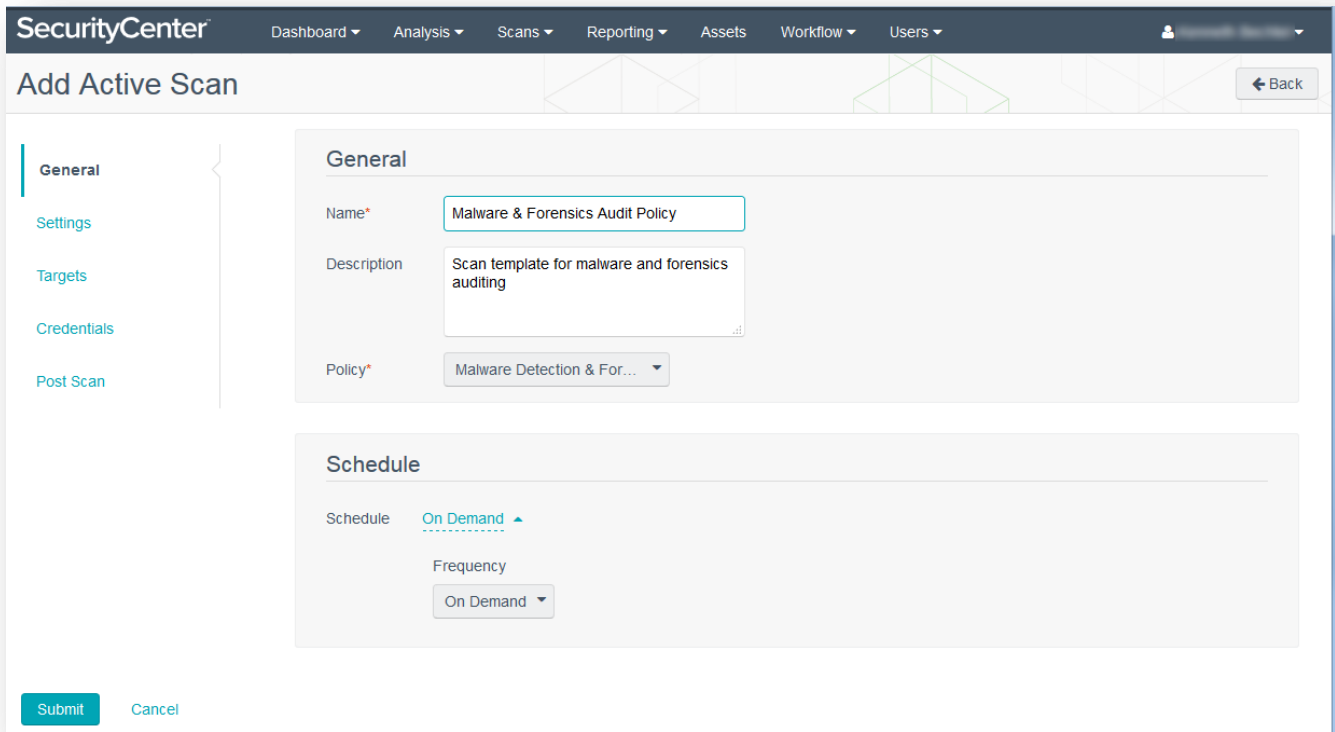
Domain  Windows login domain

[Cancel](#)

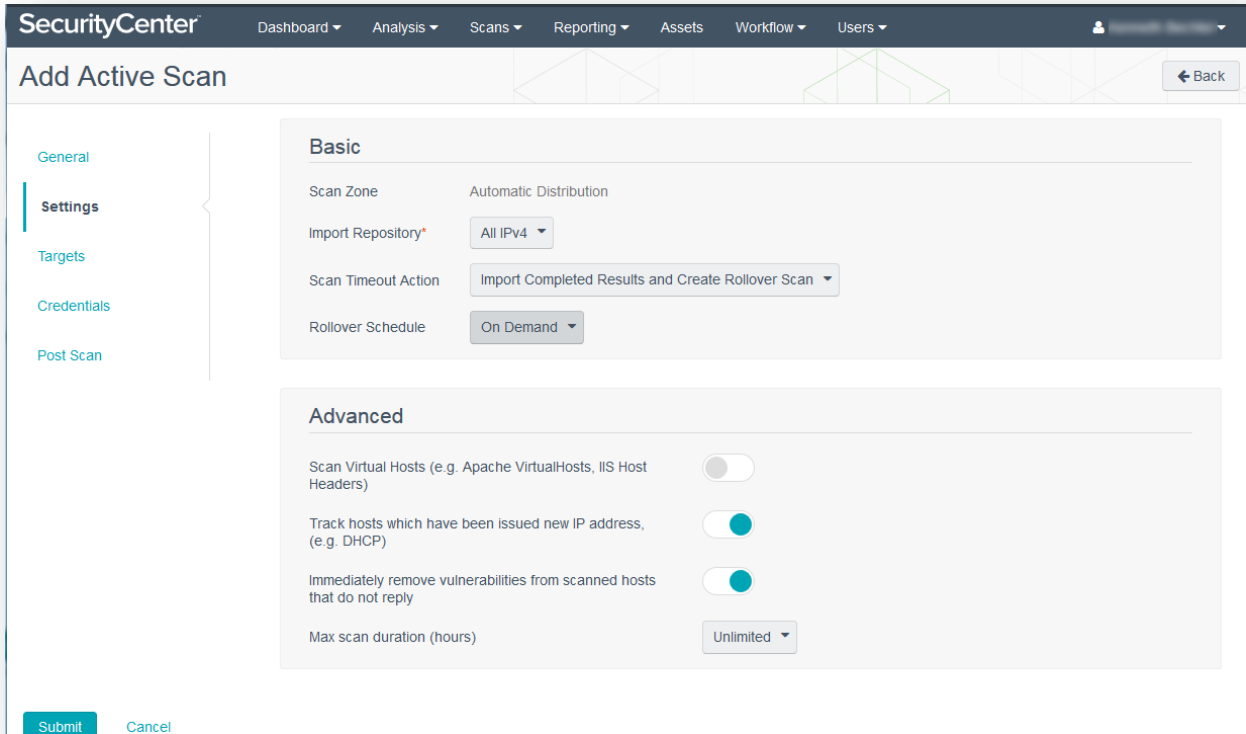
## Add Scan

Enter a scan name per your company naming policy. Include a description that informs users about the purpose of the scan.

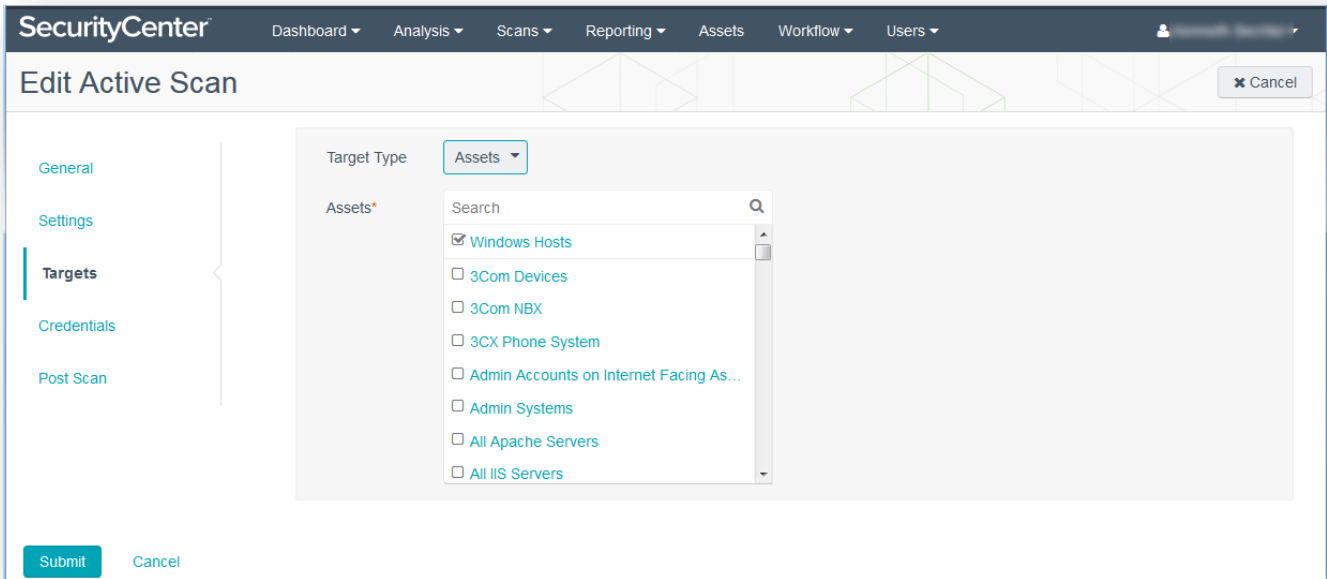
Create the scan with its schedule set to **“On Demand”**. Scans can be launched on demand, or scheduled to launch automatically at a specified time.



The screenshot shows the 'Add Active Scan' interface in SecurityCenter. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The main title is 'Add Active Scan' with a 'Back' button. A left sidebar lists 'General', 'Settings', 'Targets', 'Credentials', and 'Post Scan'. The 'General' section contains fields for 'Name\*' (Malware & Forensics Audit Policy), 'Description' (Scan template for malware and forensics auditing), and 'Policy\*' (Malware Detection & For...). The 'Schedule' section shows 'Schedule' set to 'On Demand' and 'Frequency' set to 'On Demand'. At the bottom are 'Submit' and 'Cancel' buttons.

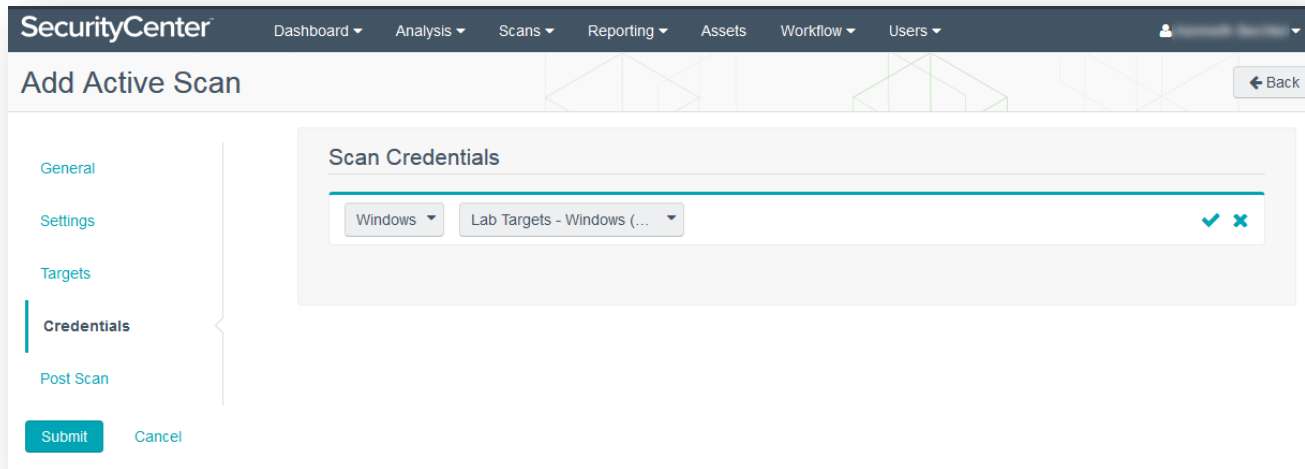


Set the targets for the scan under “**Targets**” using an asset list, IP address(es), IP range, or CIDR block.



## Policy and Credential

1. Use the scan policy created in the “Add Policy” section for the “Policy” selection.
2. Use the Windows credentials entered in the “Add Credential” section in the available “Windows Credential” selections.



## Settings: Advanced

1. Enable “Track hosts which have been issued new IP address (e.g. DHCP)”.
2. Enable “Immediately remove vulnerabilities from scanned hosts that do not reply”.

The screenshot shows the 'Add Active Scan' configuration page in the SecurityCenter interface. The page is divided into two main sections: 'Basic' and 'Advanced'. The 'Basic' section includes settings for Scan Zone (Automatic Distribution), Import Repository (All IPv4), Scan Timeout Action (Import Completed Results and Create Rollover Scan), and Rollover Schedule (On Demand). The 'Advanced' section includes settings for Scan Virtual Hosts (disabled), Track hosts which have been issued new IP address (e.g. DHCP) (enabled), Immediately remove vulnerabilities from scanned hosts that do not reply (enabled), and Max scan duration (hours) (Unlimited). The 'Settings' tab is selected in the left-hand navigation menu. At the bottom of the page, there are 'Submit' and 'Cancel' buttons.

**SecurityCenter** Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾

### Add Active Scan

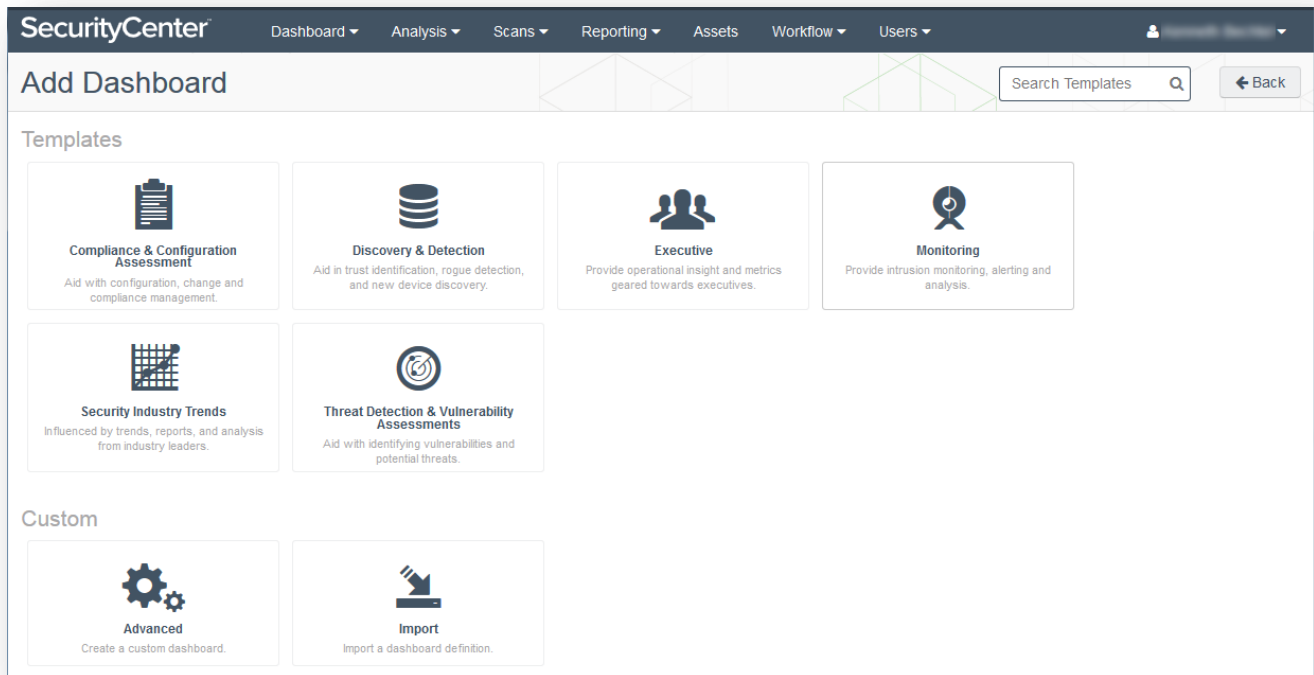
← Back

## Add Dashboard

Use the Indicators dashboard that Tenable provides as a starting point to experiment with the visual alerting of malware detection results. Please note that the Indicators dashboard covers far more than the results returned by a standard malware audit.

### Choose the Monitoring Related Dashboards and Components

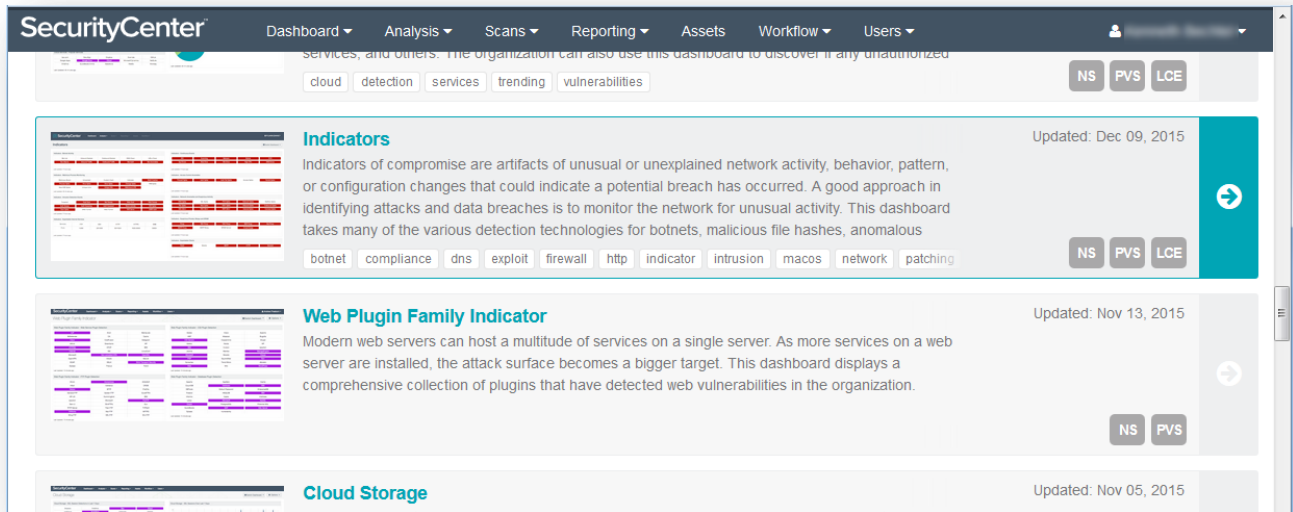
Click the “Monitoring” panel to view the selection of monitoring related dashboards and components.





## Locate the Indicators Dashboard

Filter the selection by using the word “**Indicators**” and click the “**Indicators**” dashboard.



# Review the Details of the Indicators Dashboard

Review the Indicator dashboard details and click “Add It Now”.

The screenshot shows the SecurityCenter interface with the 'Indicators' dashboard selected. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The main content area is titled 'Add Dashboard Template' and features a 'Back' button. The dashboard is divided into several sections:

- Indicators:** A grid of indicator categories, each with a red status indicator and a 'Add It Now' button. Categories include Botnet Activity, Continuous Events, Malicious Process Monitoring, Access Control Anomalies, Intrusion Detection Events, Network Anomalies and Suspicious Activity, Exploitable Internet Services, Suspicious Proxies, Relays and SPAM, and Exploitable Clients.
- Description:** A detailed text block explaining the dashboard's purpose. It states that as network complexity evolves, attackers use new methods to infiltrate organizations. The dashboard displays close to 100 different IOC and suspicious activity alerts based on malicious file hashes, anomalies in network traffic, and correlated attacks. Each element is identified with a single phrase, which turns red when that particular query has results. All time-based queries are for the last 48 hours and refresh every two hours. Indicators provide clues to unusual activity that help analysts spot attacks quickly and within the earliest stage possible.
- Components:** A list of components corresponding to the indicator categories, each with a grid icon and the category name.
- Metadata:** Information about the dashboard template, including Category (Monitoring), Created (May 10, 2015 19:01), Updated (Dec 09, 2015 16:48), Requirements (Ice 4.0.2, nessus 5.0.3, pvs 3.8.1), and Tags (botnet, compliance, dns, exploit, firewall, http, indicator, intrusion, macos, network, patching, rdp, scan, smb, ssh, ssl, web).

## Wait for the Dashboard to be Added

Click “Add” to add the dashboard to SecurityCenter, which will notify when the dashboard has successfully been added.

**SecurityCenter** Dashboard Analysis Scans Reporting Assets Workflow Users

monitoring.  
The Indicators dashboard displays close to 100 different IOC and suspicious activity alerts based on malicious file hashes, anomalies in network traffic, and correlated attacks. Each element is identified with a single phrase, which turns red when that particular query has results. All time-based queries are for the last 48 hours. All columns get refreshed every two hours.  
Indications provide clues to unusual activity that help analyst spot attacks quickly, and within the earliest stage possible. Early detection helps identify

Category: Monitoring  
Created: May 10, 2015 19:01  
Updated: Dec 09, 2015 16:48  
Requirements: Ice 4.0.2 nessus 5.0.3 pvs 3.8.1  
Tags: botnet compliance dns exploit firewall http indicator intrusion macos network patching rdp scan smb ssh ssl web

**Components**

- Indicators - Botnet Activity
- Indicators - Continuous Events
- Indicators - Malicious Process Monitoring
- Indicators - Access Control Anomalies
- Indicators - Intrusion Detection Events
- Indicators - Network Anomalies and Suspicious Activity
- Indicators - Exploitable Internet Services
- Indicators - Suspicious Proxies, Relays and SPAM
- Indicators - Exploitable Clients

**Focus**

Targets: All Systems

**Schedule**

Schedule\* Every day at 13:18 -04:00

Cancel

Dashboard Added Successfully

https://172.26.24.244/#

## Wait for the Dashboard Components to Update

In the screenshot below, a malware detection and forensics audit has already been run and the results, as highlighted by the dashboard, contain malicious process detection results.

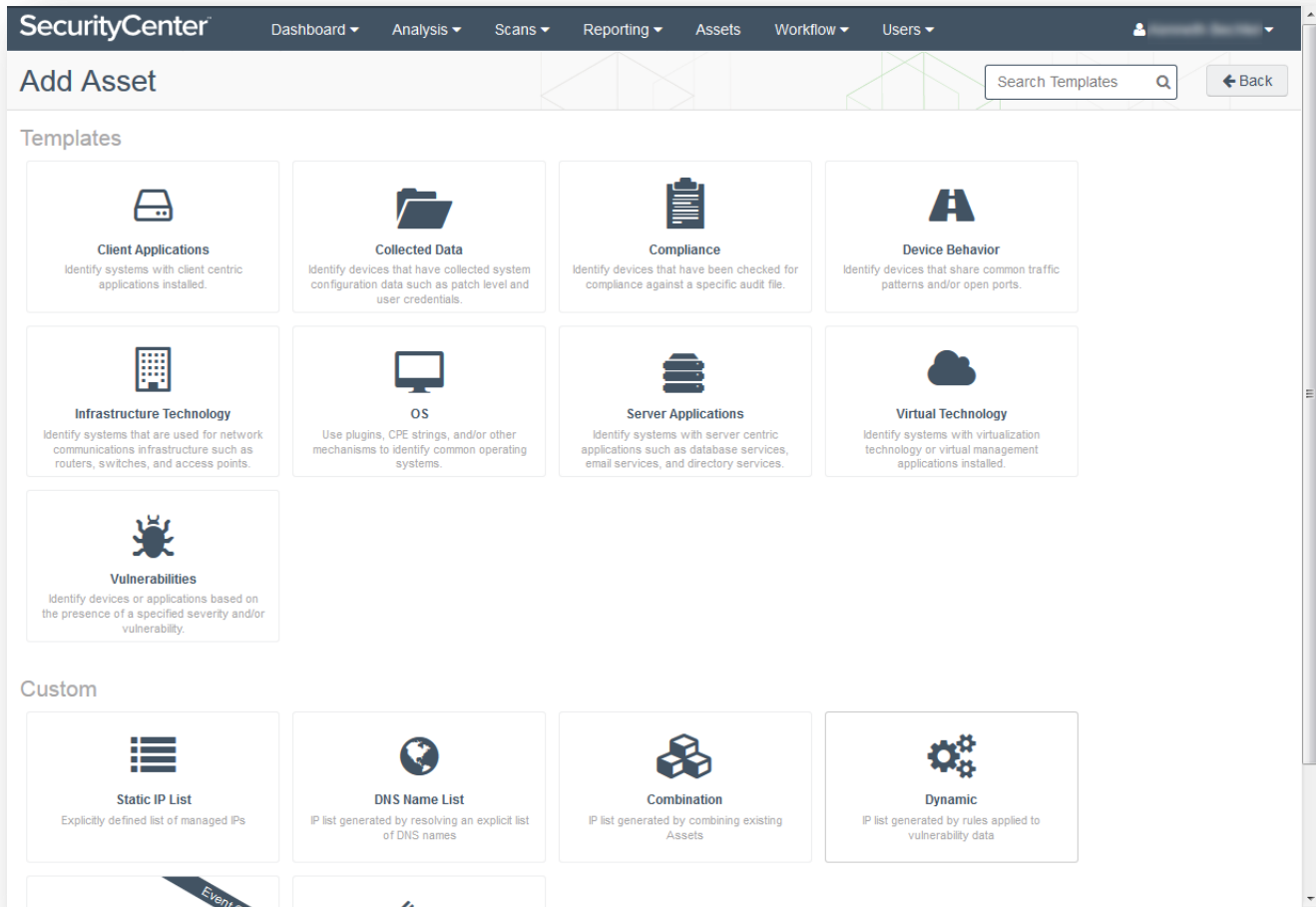
The screenshot displays the SecurityCenter dashboard with the following sections:

- Indicators - Botnet Activity:** Bot List, Inbound Netstat, Outbound Netstat, DNS Clean, URLs Clean. Bot Attacks, Inbound Traffic, Outbound Traffic, Bot Auth, Bot Anomalies. Last Updated: Less than a minute ago.
- Indicators - Malicious Process Monitoring:** Malicious (Scan), Unwanted, Custom Hash, Indicator, Multi Crashes. Process Spike, Virus Spike, Error Spike, Change Spike, FIM Spike. New EXE Spike, Unique Unix, Unique Win, Malicious (LCE). Last Updated: Less than a minute ago.
- Indicators - Intrusion Detection Events:** Targeted, Host Scan, Net Sweep, Web Scan, Web Sweep. Auth Sweep, Auth Guessing, Auth Guessed, Worm Activity, IDS Spike. Scan Spike, DNS Tunnel, Web Tunnel, EXE Serve, USER Auth. Last Updated: Less than a minute ago.
- Indicators - Exploitable Internet Services:** Services, FTP, SSH, HTTP, HTTPS, SMB. Ports, 1-200, 201-500, 501-1024, 1025-5000, 5000+. Last Updated: Less than a minute ago.
- Indicators - Continuous Events:** IDS, Scanning, Malware, Botnet, DOS. Sys Errors, Web Error, Win Error, High CPU, DNS Errors. Last Updated: Less than a minute ago.
- Indicators - Access Control Anomalies:** Firewall Spike, Auth Spike, Auth Fail Spike, Access Spike, Denial Spike. Last Updated: Less than a minute ago.
- Indicators - Network Anomalies and Suspicious Activity:** DNS Spike, SSL Spike, PVS Spike, Network Spike, Netflow Spike. File Spike, Web Spike, 404+ Spike, Inbound Spike, Outbound Spike. SSH 30m+, VNC 30m+, RDP 30m+, Internal Spike, Connect Spike. Last Updated: Less than a minute ago.
- Indicators - Suspicious Proxies, Relays and SPAM:** Proxy, SSH Proxy, VNC Proxy, RDP Proxy, Bot Proxy. SMTP Proxy, SMTP Relay, SPAM Server, Crowd Surge. Last Updated: Less than a minute ago.
- Indicators - Exploitable Clients:** (Section header visible, content not fully shown).

## Add Asset

We can build a dynamic asset list to filter in dashboards, reports, alerts, and querying on those hosts identified as running a Windows operating system but did not have credentialed checks executed. The majority of malware detection and forensic checks are credentialed checks.

### Choose to Add an Asset List



### Create Dynamic Asset List

1. Click **“Dynamic”**.
2. Enter the name and description.
3. Ensure **“All of the following are true”** is selected, and not **“Any of the following are true”**.
4. Create two clauses: the first, Plugin Text, containing the pattern **“Credentialed checks : no:”** where the plugin ID is 19506; the second, Operating System, containing the pattern **“indows”** (omitting the quotation marks in each entry).
5. Click **“Submit”** when done.

**SecurityCenter** Dashboard Analysis Scans Reporting Assets Workflow Users Kenneth Bechtel

### Edit Dynamic Asset

**General**

Name\* Windows Credential Check Failures

Description a list of Windows hosts on which credentialed checks could not be executed.

**Asset Definition**

All of the following are true:

- Operating System is equal to indows
- Plugin Text is equal to Credentialed checks : no: where plugin ID is 19506

Submit Cancel

## Verify Asset List Created Successfully

Ensure that a non-zero number is shown for the number of systems scanned for the new dynamic asset list.

Asset Name	Access	Type	Count	Last Updated	Actions
VMWare ESX Hypervisors and Related Systems	Full Access	Dynamic	13	Jul 01, 2015 14:27	⚙️
Voice or Mobile Client Devices	Full Access	Dynamic	0	Jun 08, 2015 17:03	⚙️
VoIP Servers or Voice Infrastructure	Full Access	Dynamic	3	Jun 30, 2015 17:04	⚙️
Web Server Detection	Full Access	Dynamic	462	Jul 22, 2015 13:10	⚙️
Windows Credential Check Failures	Full Access	Dynamic	0	1 minute ago	⚙️
Windows Hosts	Full Access	Dynamic	214	Jun 08, 2015 17:03	⚙️

## Vulnerabilities (Cumulative View)

The malware and botnet detection plugins follow the general policy of indicating an issue when a result has a severity rating of low, medium, high, or critical. The Indicators dashboard highlights these types of issues. We could also set up alerts and filter on the new malware repository for any plugin result with a severity rating of low, medium, high, or critical. A query can be filtered in the same fashion, as can a SecurityCenter API query.

However, in addition to potentially having malware detection plugin results, we also have a rich dataset of forensics information in the form of Windows process and auto-run plugin results. Through reviewing the results of plugin 70330, “**Window Process Unique Process Name**” and plugin 70768, “**Reputation of Windows Executables: Unknown Process(es)**” and forensic investigation, we may find some executable code that has not been flagged by the malware detection plugins but actually is malware. We could upload hashes (see “[Windows: Malware Files](#)”), and perform a new enterprise malware scan to determine how widespread a newly discovered malware infection is, or we could turn to the forensic plugin results to determine the scope of an infection.

The steps that follow offer a method for a quick search for executable code that has been identified as malware; however, there are many ways to use the filters in SecurityCenter, which are available across dashboards, reporting, alerting, and the API.

## Look at the Cumulative View of Results

The screenshot displays the SecurityCenter interface for Vulnerability Analysis. The top navigation bar includes Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. The main header shows 'Vulnerability Analysis' with an 'Options' menu. On the left, there are filter sections for Address, Plugin ID, Plugin Name, and Severity, each with an 'All' selection. Below these filters are 'Select Filters' and 'Load Query' buttons. The main content area shows a 'Vulnerability Summary' dropdown and a 'Jump to Vulnerability Detail List' link with 'Total Results: 16497'. The central table lists vulnerabilities with the following data:

Plugin ID	Name	Family	Severity	Total
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Windows	Critical	78
33850	Unsupported Unix Operating System	General	Critical	33
82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Windows	Critical	29
22024	Microsoft Internet Explorer Unsupported Version Detection	Windows	Critical	13
71458	Nessus Unsupported Version Detection	Misc.	Critical	12
72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)	DNS	Critical	10
89059	CentOS 6 / 7 : openssl (CESA-2016:0301) (DROWN)	CentOS Local Securi...	Critical	10
55883	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (remote check)	Windows	Critical	9
72704	Microsoft .NET Framework Unsupported	Windows	Critical	9

## Filter on the Executable Code File Name that has been Identified as Malware

The screenshot shows the SecurityCenter interface for Vulnerability Analysis. The left sidebar contains a 'Filters' panel with the following settings:

- Plugin ID: All
- Vulnerability Text: Contains MSADE.EXE
- Address: All
- Plugin Name: All
- Severity: All

The main content area displays a table of vulnerability results. The table has columns for Plugin ID, Plugin Name, Family, Severity, IP Address, NetBIOS, DNS, MAC Address, and Repository. One result is visible:

Plugin ID	Plugin Name	Family	Seve...	IP Address	NetBIOS	DNS	MAC Address	Repository
800040	Malware Hos...	Generi...	High	172.26.24.251		scr-ice...	00:50:56:bd:...	SCR - Lab...

## Review the List of Plugin Results that Contain References to the Malware

We could drill in further to see the individual plugin report details for the context of the malware matches.

The screenshot shows the SecurityCenter interface for Vulnerability Analysis. The left sidebar contains a 'Filters' panel with the following settings:

- Plugin ID: = 70768, 70330
- Address: All
- Plugin Name: All
- Severity: All

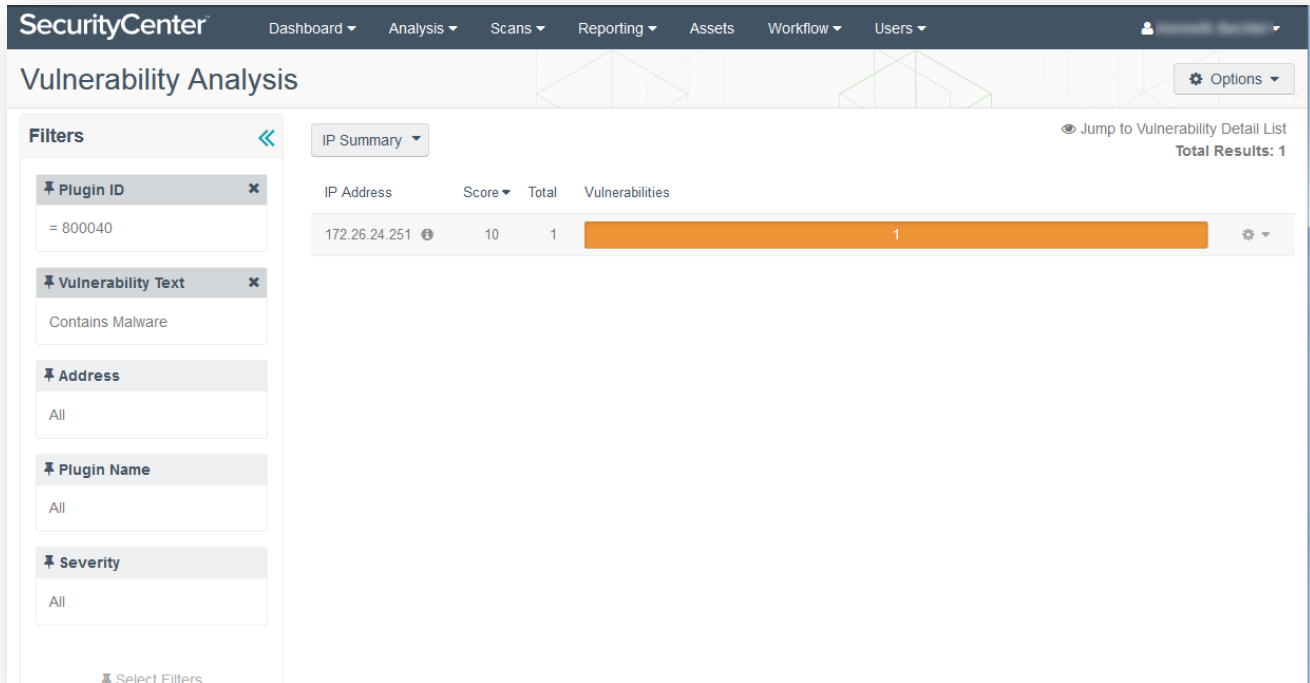
The main content area displays a table of vulnerability results. The table has columns for Plugin ID, Name, Family, Severity, and Total. One result is visible:

Plugin ID	Name	Family	Severity	Total
70768	Reputation of Windows Executables: Unknown Process(es)	Windows	Info	10



## Change the View to “IP Summary”

If we change the view to “IP Summary”, we can see the list of hosts that have plugin results with matches for the malware.



The screenshot shows the SecurityCenter interface for Vulnerability Analysis. The view is set to "IP Summary". The left sidebar contains filters for Plugin ID, Vulnerability Text, Address, Plugin Name, and Severity. The main area displays a table with columns for IP Address, Score, Total, and Vulnerabilities. A single entry is shown for IP address 172.26.24.251 with a score of 10 and 1 vulnerability. A progress bar indicates 1 vulnerability out of a total of 1. The interface also includes navigation options like "Jump to Vulnerability Detail List" and "Options".

IP Address	Score	Total	Vulnerabilities
172.26.24.251	10	1	1

## ThreatLists and Watches:

SecurityCenter integrates multiple threat intelligence feeds focusing on three areas:

- Passive Web Traffic Analysis
- Malicious Process Detection
- Botnet Detection based on IP reputation

Dashboards check against these areas and display real-time data of the results. Administrators can also leverage custom whitelists and blacklists when customizing dashboard output.

## About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting [tenable.com](https://tenable.com).