

Cybersecurity Open Source Tools

U.S. Embassy Suva

Political/Economic Section



Overview

- Pillars of Cybersecurity
 - Cybersecurity Fundamentals
- Introduction to Open Source Tools
 - What are they?
- Overview of Key Players
- Types of Open Source Tools
- SWOT Analysis of Open Source Tools

Please keep in mind this presentation is a high-level introduction – most topics will not be covered in depth.

Pillars of Cybersecurity: What We're Trying to Accomplish



Confidentiality - Protection of information from disclosure to unauthorized individuals, systems, or entities. Confidentiality is **data** oriented.



Integrity - Protection of information, systems, and services from unauthorized modification or destruction. Integrity is **data** oriented.



Availability - Timely, reliable access to data and information services by authorized users. Availability is **service** oriented.



Non-repudiation - The ability to correlate, with high certainty, a recorded action with its originating individual or entity. Non-repudiation is **entity** oriented.



Authentication - The ability to verify the identity of an individual or entity. Authentication is **entity** oriented.

Cyber Defense Principles: How we're trying to accomplish it

Least Privilege

- Know who has access to systems and data, and minimize the level of access to only what is required

Defense in Depth

- Know what your critical assets are, and protect them with multiple overlapping security controls

Management and Monitoring

- Know how your assets should be performing, and how they are performing currently

Cybersecurity Fundamentals: Good Cyber Hygiene

1. Risk Identification

- Know your assets & identify what's critical
- Know your network & data
- Know your applications & application versions
- Know the common vulnerabilities

2. Vulnerability Reduction

- Secure network endpoints
- Install asset protection/intrusion detection tools
- Apply principle of least privilege and defense in depth
- Apply mitigations to known vulnerabilities

3. Threat Reduction

4. Consequence Mitigation

5. Enable Cybersecurity Outcomes



Where to Start (Cyber Hygiene)

Next Steps: Holistic Cybersecurity Practices

- 1. Risk Identification**
- 2. Vulnerability Reduction**
- 3. Threat Reduction**
 - Threat Assessments
- 4. Consequence Mitigation**
 - Defensive Cyber Operations
- 5. Enable Cybersecurity Outcomes**
 - Holistic Risk Assessments



Where to Go Next

Definition of Open Source Tools

The software is freely available without cost. It is developed and maintained as a cooperative effort. If you have something to contribute, you may submit your code for inclusion.



Introduction to Open Source Tools

- Open Source tools can be cost effective.
- Many individuals and organizations develop software tools for their own use before there is a commercial equivalent.
- Some go on to become commercial products.
- Some are made freely available.
- Tools are often adapted to:
 - changing needs and requirements
 - use evolving technology

Considerations for Selecting Open-Source Tools

Requirements - Identify your need and then choose your tool.

Skillset - Does your staff have the skills to deploy and maintain the tool?

Support - What support is available? Are patches provided?

User Community Size - Better tools typically have larger/more active user communities

Documentation - What documentation is available for deployment/upkeep?

Source Code Assessment - Open-source code can be reviewed for vulnerabilities by anyone.

Licensing - are there any restrictions on using/changing the source code?

Cost - Calculate total ownership cost or ROI; include deployment cost, staffing support cost, data transfer costs, education and training, etc.

Who are the Key Players in this Space?

Government organizations include:

- U.S. Department of Homeland Security (DHS)
- Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. Computer Emergency Readiness Team (U.S.-CERT)

Non-governmental organizations include:

- MITRE
- Open-Audit
- nMap
- AlienVault
- SIEMonster
- Elastic
- OSSEC
- WAZUH
- Snort
- McAfee
- Microsoft
- Sophos
- F-Secure
- Software Engineering Institute

CISA

- The Cybersecurity and Infrastructure Security Agency is the U.S.'s risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.



U.S.-CERT

- The United States Computer Emergency Readiness Team is an organization within CISA.
- US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.



MITRE

- MITRE has worked closely with government to strengthen U.S. cyber defenses for more than four decades.
- MITRE advocates a balanced security posture that combines classic cyber defense approaches with a new emphasis on leveraging cyber threat intelligence to respond and adapt quickly to a cyber attack.

The MITRE logo is displayed in a large, bold, blue sans-serif font. The letters are thick and closely spaced, with a clean, modern aesthetic. The logo is positioned on the right side of the slide, centered vertically relative to the text area.

What Do Open Source Tools Do?

Network Discovery Tools

Log Aggregation and Analysis

Intrusion Detection Systems (IDS)

Network Monitoring Systems

Risk Assessments

Threat Assessments



Network discovery tools enable you to automatically discover exactly what devices are on your network at any given time, which helps you keep your network's devices organized, ensure they're working well, and get informed when issues arise.

Network Discovery Tools

Open-Audit v4.1.1 (Windows)/v4.1.2 (Linux)

Strengths

- Open Source
- A reporting framework on information such as software licensing, configuration changes, non-authorized devices, capacity utilization and hardware warranty status.
- Agentless Discovery (all editions)
- Community edition is free
- Enterprise edition is free for up to 20 devices

Weaknesses

- Not compatible with windows 10
- 12-month subscription licenses
- Professional edition starts at \$1,449 US for 500 devices, and Enterprise edition starts at \$1,149 US for 100 devices

Opportunities

- Community, Professional, Enterprise, and Cloud editions offer increasing levels of features and support

Threats

- Professional support only on paid versions

Accessing Open-AuditIT



The Open-AuditIT tool is available with **free and paid** options



Get started by downloading the tool at <https://www.open-audit.org/downloads.php>



To learn more about the tool visit <https://community.opmantek.com/display/OA/Home>

NMAP 7.90



Strengths

- Runs on all major computer operating systems
- Official binary packages are available for Linux, Windows, and Mac OS X
- Options for command line or advanced GUI with results viewer (Zenmap)
- Free to download

Weaknesses

- No warranty
- No support

Opportunities

- Flexible data transfer, redirection
- Debugging tool (Ncat), a utility for comparing scan results (Ndiff)
- Packet generation and response analysis tool (Nping)

Threats

- N/A

Accessing NMAP



The NMAP tool is available at **no cost** to users



Get started by downloading the tool at <https://nmap.org/download.html>



To learn more about the tool visit <https://nmap.org/book/man.html>



- A software function that consolidates log data from throughout the IT infrastructure into a single centralized platform where it can be reviewed and analyzed.

Log Aggregation and Analysis

OSSIM 4.1 (Released September 2019)



Strengths

- Open Source
- Security Information and Event Management (SIEM), provides event collection, normalization and correlation
- SIEM event correlation
- On-premises Physical & Virtual Environments
- Windows and Linux distributions

Weaknesses

- Lacks log management features
- Lacks Azure / AWS integration
- Support via community forums
- Limited Product Documentation

Opportunities

- Asset discovery
- Vulnerability assessment
- Intrusion detection
- Behavioral monitoring
- Upgrade path to Alienvault USM (paid), which resolves some feature limitations

Threats

- Single server only (lacks redundancy)
- Professional support only on paid versions

Accessing OSSIM



The OSSIM tool is available with **free and low-cost** options



Get started by downloading the tool at <https://cybersecurity.att.com/products/ossim/download>



To learn more about the tool visit <https://cybersecurity.att.com/products/ossim>

SIEMonster v4.4



Strengths

- “Built on” Open Source
- Virtual Server / Bare-Metal installation options
- Wazuh integration used to collect, aggregate, index and analyze security data, to detect intrusions, threats and behavioral anomalies.
- MITRE ATT&CK framework integrations

Weaknesses

- Community Edition not upgradeable or scalable
- Limit 100 endpoints
- Invitation required for Community Edition
- Paid editions can be quite expensive
- Community version not upgradeable, does not support Cloud data sources

Opportunities

- Community (free, 1-100 endpoints)
- Professional (\$125/mo US, 1-200 endpoints)
- Enterprise (\$1,200/mo US, 1-10,000 endpoints)
- MSSP versions (\$3,275/mo US, unlimited endpoints)

Threats

- Professional support only on paid versions

Accessing SIEMonster



The SIEMonster tool is available with **free and low-cost** options



Get started by downloading the tool at <https://siemonster.com/download-community-edition/>



To learn more about the tool visit <https://siemonster.com/community-edition/>

Elastic-Logstash-Kibana (ELK) 7.13.3 , Rel 07/07/2021



Strengths

- Has wide adoption in industry (*Graylog is built on top of the Elastic base*)
- Loading Data: Elastic has inputs, extractors, data shippers (beats), etc.
- Search & Visual Analytics: Flexible controls and "drill-down analysis" via the Kibana dashboard
- Elastic is open-source

Weaknesses

- Complex data loading occurs via scripted Logstash pipelines
- Making full use of data index features requires custom mappings
- Implementing enterprise security will require purchasing licenses

Opportunities

- Due to wide adoption, large user community exists
- Documentation is extensive, training classes are also available

Threats

- Elastic stack is seemingly low-cost, but enterprise features come with a price
- Platform and hardware maintenance issues are also a factor

Accessing the Elastic (ELK) Stack Tools



The Elastic (ELK) Tool is available with **low-cost** options



Get started by downloading the tool at <https://www.elastic.co/downloads/>



To learn more about the tool and additional Elastic resources visit <https://www.elastic.co/products/>



An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.

Intrusion Detection Systems (IDS)

OSSEC 3.6.0 (Released Feb. 2020)



Strengths

- Runs on all major Operating Systems
- Includes client & server-based management options
- Low CPU usage
- Active response options
- User manual available
- Community support via google mailing list & GitHub

Weaknesses

- Enterprise OSSEC option not open source
- Limit to 256 agents per manager

Opportunities

- Host-based intrusion detection
- Log monitoring & analysis
- Compliance audits
- System inventory
- File integrity monitoring

Threats

- CVE-2021-28040 – Uncontrolled Recursion Vulnerability

Accessing OSSEC



The OSSEC tool is available at **no cost** to users



Get started by downloading the tool at <https://www.ossec.net/ossec-downloads/>



To learn more about the tool visit <https://www.ossec.net/products/>

Wazuh 4.1.5



Strengths

- Free
- Open Source
- Based on OSSEC framework
- Wazuh agents run on Windows, Linux, Mac OS X, AIX, Solaris and HP-UX
- Alerts generated by Wazuh are sent to Elastic Stack, where they are indexed and stored

Weaknesses

- User interface can be difficult to use

Opportunities

- Threat detection, integrity monitoring, incident response and compliance
- Cloud version (paid) offers Software as a Service Endpoint Detection and Response capabilities

Threats

- Professional support only on paid versions
- Standard (starts at \$500 US / annual)
- Premium (starts at \$725 US/ annual) maintenance packages

Accessing WAZUH



The WAZUH tool is available at **free**
and low-cost options to users



Get started by downloading the tool
at <https://wazuh.com/start/>



To learn more about the tool visit
<https://documentation.wazuh.com/current/index.html/>

Snort 3.1.6 (Released June 2021)



Strengths

- Open Source
- Linux and Windows distributions
- Source code updated every 2 weeks via GitHub
- Installation, configuration, and rule writing video walkthroughs

Weaknesses

- Lacks GUI / Admin console
- Relatively high false positive rate (particularly if not well configured)
- Requires frequent upgrading
- Lack of prepackaged logging and reporting methods

Opportunities

- Packet Sniffer, Packet logger, Intrusion Prevention System (IPS) functionality
- Personal subscriptions for students or home network environment users (\$29.99 US / annual)

Threats

- Business subscriptions for companies, non-profits, universities, government agencies, etc. that need to deploy Snort across a wide variety of devices and need to protect a large network (\$399 US per sensor / annual)

Accessing Snort



The Snort tool is available at **low-cost** options



Get started by downloading the tool at <https://www.snort.org/>



To learn more about the tool visit <https://www.snort.org/documents>

Next Steps: Holistic Cybersecurity Tool Types

- Risk Assessments
 - Cyber Security Assessment Tool(s)
- Defensive Cyber Operations
 - Symson (including configuration)
 - Windows Event Logger
 - Custom Analysis

Threat Reduction

Consequence Mitigation

Tools in these categories require significant time and skill to configure and implement but can be considered once Fundamental Tools are in place.



Identifies the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets.

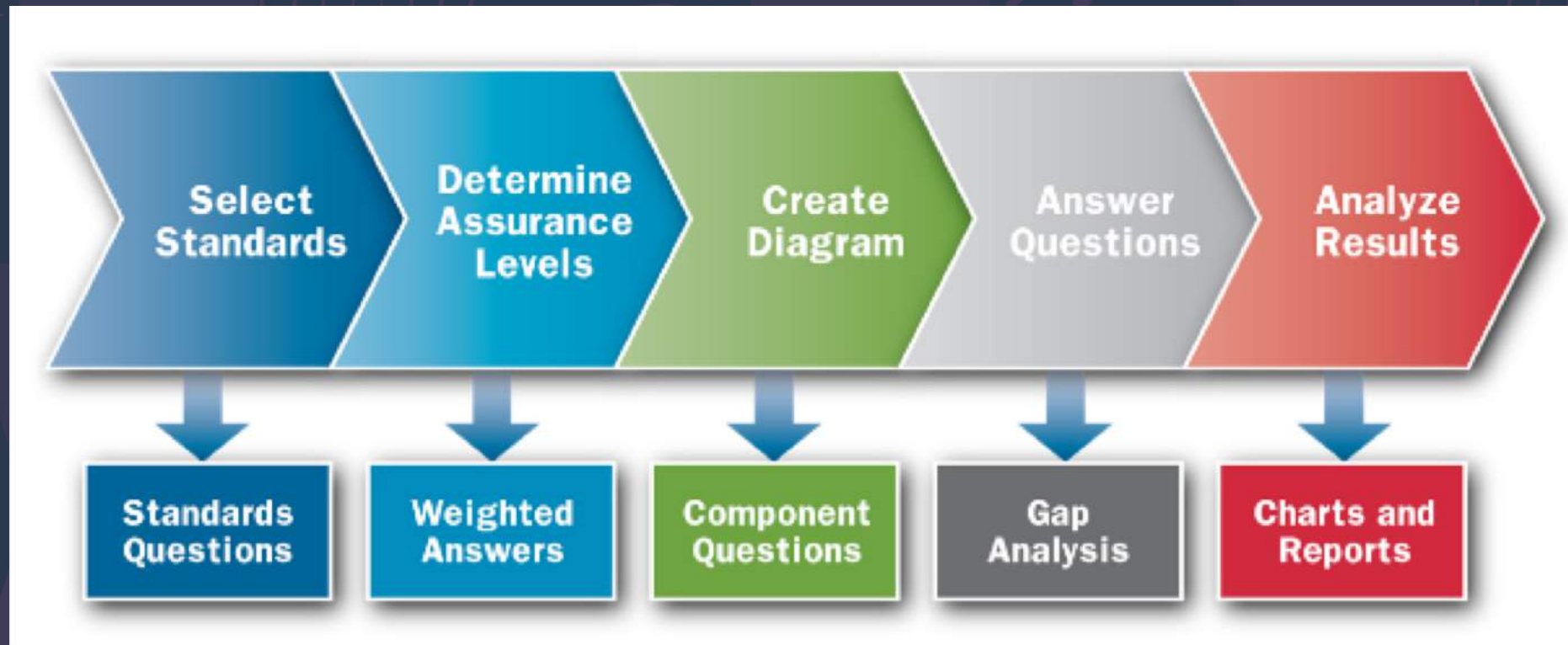
Risk Assessments

Cyber Security Evaluation Tool (CSET®)

- CSET® provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture.
- Desktop software tool that guides asset owners and operators through a step-by-step process to evaluate their industrial control system (ICS) and information technology (IT) network security practices.
- Users evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.



CSET[®] Assessment Process



Accessing CSET®



The CSET application is available at **no cost** to end users.



Get started by downloading CSET at <https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET>



To learn more about CSET or to request a physical copy of the software, contact cset@dhs.gov

Working Towards a Holistic Risk Management Approach

- A Risk Management Approach:
 - acknowledges that it is impossible to prevent cyber incidents;
 - asks "*What's the worst that can happen?*" if a cyberattack was successful;
 - assigns financial, human, and technical resources to the assets and data that are the most critical to your overall business mission;
 - calculates how to prioritize the assignment of resources by:
 - examining the vulnerabilities in networks, systems, and the data you process;
 - determining the threat profile of malicious actors and the likelihood those actors will take advantage of the vulnerabilities you have;
 - factoring in the consequences that would happen if the threat actor executed a successful attack.



- Questions?

Thank you!



Cyber threat analysis is the process of assessing the cyber activities and capabilities of unknown intelligence entities or criminals. Threats posed by cyber-attacks include denial of service attacks (DoS), computer viruses, malware, phishing emails, and others.

Threat Assessment


What is Malware?

Short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device.

The software is then used, usually covertly, to compromise the integrity of your device.

US-CERT AMAC Malware Analysis

- Cyber analysis and warning capabilities are critical to thwarting computer-based threats and attacks.
- DHS established the United States Computer Emergency Readiness Team (US-CERT) to coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks.



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT AMAC Malware Analysis Submissions

Web Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

Completing Your Submission

- Navigate to <https://www.malware.us-cert.gov/>
- Complete the fields in the form in order initiate contact with DHS to have a malware analysis conducted.

(All fields are optional)

Agree to Terms:

First Name:

Last Name:

Organization:

Incident ID:

Phone Number:

Email Address:

Please enter context regarding this submission:

Select file (100MB Limit):

Browse...

No file selected.

Submit

Privacy Act Statement:

Authority: 5 U.S.C. § 301 and 44 U.S.C § 3101 authorize the collection of this information.

Purpose: The primary purpose for the collection of this information is to allow the Department of Homeland Security to contact you regarding your request.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

Disclosure: Providing this information is voluntary, however, failure to provide this information will prevent DHS from contacting you in the event there are questions regarding your request.

[Privacy Policy](#)

Accessing US-CERT AMAC Malware Analysis



The AMAC Malware Analysis tool is available at **no cost** to end users.



Get started by accessing the tool at <https://www.malware.us-cert.gov/>



To learn more about US-CERT or the Malware Analysis Tool, contact : info@us-cert.org or call (888) 282-0870

If Your System Has Been Compromised...

- There are legitimate, low-cost tools available to help detect and eliminate malware infections.
- These mainstream options are established by:
 - Sophos
 - F-Secure
 - McAfee
 - Microsoft

Sophos Virus Removal Tool

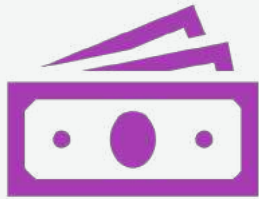
- This tool detects all types of malicious software on your computer and returns it to a working state.
- This includes:
 - Viruses
 - Spyware
 - Rootkits
 - Conficker

The image shows the Sophos logo, which consists of the word "SOPHOS" in a bold, blue, sans-serif font. The logo is centered within a white rectangular box that has a subtle drop shadow, making it stand out against the light gray background of the slide.

Sophos Tool Functions

- The tool is a self-contained, on-demand malware scanner with the following features:
 - Automatic updating before a scan
 - Scans all connected drives
 - Rootkit scanning
 - User memory scanning
 - Kernel memory scanning

Accessing the Sophos Virus Removal Tool



The Sophos Virus Removal tool is available at **no cost** to end users.



Get started by downloading the tool at <https://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx>



To learn more about the tool and additional Sophos Cloud Security Topics visit <https://community.sophos.com/free-antivirus-tools-for-desktops>

F-Secure Online Scanner

- Scan and clean your Windows system at no cost.
- Online Scanner finds and removes viruses, malware, and spyware.
- Works in-conjunction with any other security software already installed.



Accessing F-Secure Online Scanner



The F-Secure Online Scanner tool is available at **no cost** to end users.



Get started by downloading the tool at <https://www.f-secure.com/en/home/free-tools/online-scanner>



To learn more about the tool and additional F-Secure resources visit <https://www.f-secure.com/en/business/support-and-downloads>

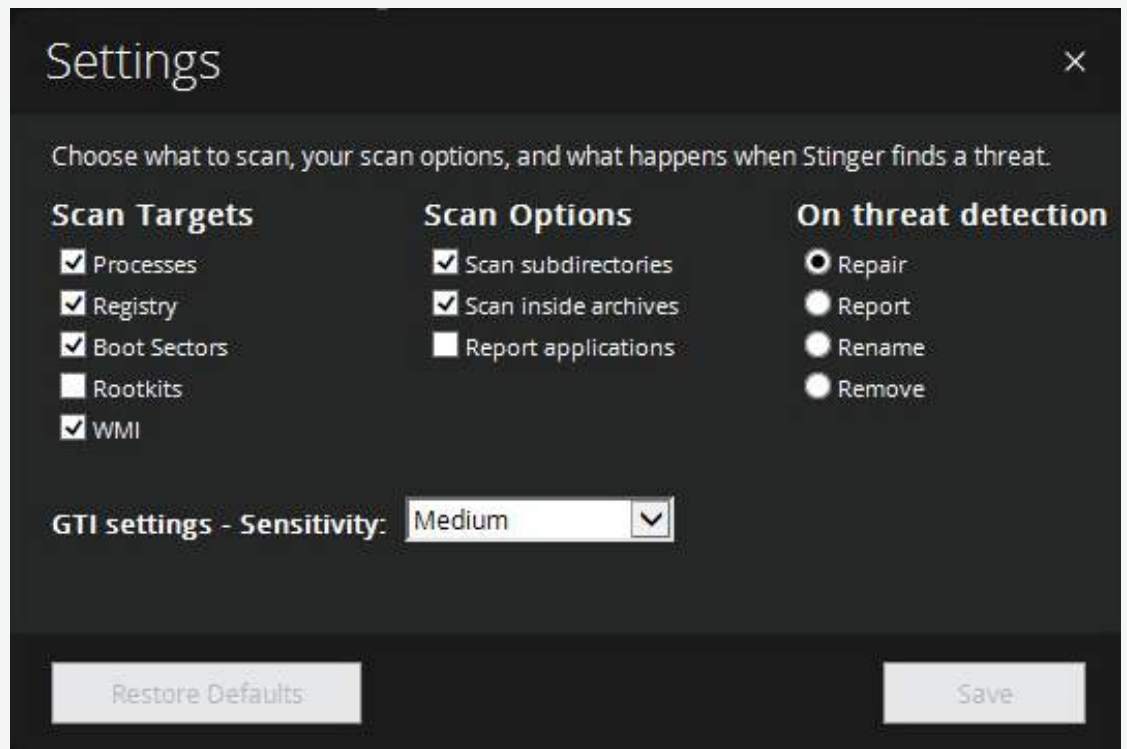
McAfee Stinger

- McAfee Stinger is a standalone utility tool used to detect and remove specific viruses.
- Marketed as not a substitute for complete antivirus protection.
- Utilizes scan technology, including rootkit scanning, and scan performance optimizations.



McAfee Stinger Settings

- The Stinger tool allows users to choose what to scan, configure scan options, and what occurs when Stinger finds a threat



Accessing McAfee Stinger



The McAfee Stinger tool is available at **no cost** to end users.



Get started by downloading the tool at <https://www.mcafee.com/enterprise/en-us/downloads/free-tools/stinger.html>



To learn more about McAfee Stinger visit <https://www.mcafee.com/enterprise/en-us/downloads/free-tools/how-to-use-stinger.html>

Microsoft Safety Scanner

- Microsoft Safety Scanner is a scan tool designed to find and remove malware from Windows computers.
- After scanning to find malware, the tool attempts to reverse changes by identified threats.



Microsoft Safety Scanner

- Safety Scanner only scans when manually triggered and is available for use 10 days after being downloaded.
- Microsoft recommends that you always download the latest version of the Safety Scanner tool before each scan.
- Microsoft indicates that this tool does not replace any existing anti-malware product.

Accessing Microsoft Safety Scanner



The Microsoft Safety Scanner tool is available at **no cost** to end users.



Get started by downloading the tool at <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download>



To learn more about Microsoft Safety Scanner visit <https://support.microsoft.com/en-us/topic/how-to-troubleshoot-an-error-when-you-run-the-microsoft-safety-scanner-6cd5faa1-f7b4-afd2-85c7-9bed02860f1c>