Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency

In February 2022, CISA launched an update to their website outline free cyber security services and tools.

Information Source: https://www.cisa.gov/free-cybersecurity-services-and-tools

Provided below are a few key areas of the CISA website that may be of interest.

Reducing the Likelihood of a Damaging Cyber Incident

Service	Skill Level	Owner	Description	Link
CISA Cybersecurity Publications	Basic	CISA	CISA provides automatic updates to subscribers via email, RSS feeds, and social media. Subscribe to be notified of CISA publications upon release.	https://www.cisa.gov/subscribe-updates-cisa
CISA Vulnerability Scanning	Basic	CISA	This service evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. It provides weekly vulnerability reports and ad-hoc alerts. See https://www.cisa.gov/cyber-resource-hub for details.	Email: vulnerability@cisa.dhs.gov
CISA Web Application Scanning	Basic	CISA	This service evaluates known and discovered publicly accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks. See https://www.cis	Email: vulnerability@cisa.dhs.gov

Free Cyber Security Services and Tools
From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
			a.gov/cyber-resource-hub for details.	
CISA Phishing Campaign Assessment	Basic	CISA	This service provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training. See https://www.cisa.gov/cyber-resource-hub for details.	Email: vulnerability@cisa.dhs.gov
CISA Remote Penetration Test	Basic	CISA	This test simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open source information. See https://www.cisa.gov/cyber-resource-hub for details.	Email: vulnerability@cisa.dhs.gov
Immunet Antivirus	Basic	Cisco	Immunet is a malware and antivirus protection system for Microsoft Windows that utilizes	https://www.immunet.com/

Service	Skill Level	Owner	Description	Link
			cloud computing to provide enhanced community-based security.	
Cloudflare Unmetered Distributed Denial of Service Protection	Basic	Cloudflare	Cloudflare DDoS protection secures websites, applications, and entire networks while ensuring the performance of legitimate traffic is not compromised.	https://www.cloudflare.com/plans/free/
Cloudflare Universal Secure Socket Layer Certificate	Basic	Cloudflare	SSL (Secure Socket Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. Cloudflare allows any internet property to use SSL with the click of a button.	https://www.cloudflare.com/plans/free/
Microsoft Defender Application Guard	Basic	Microsoft	This capability offers isolated browsing by opening Microsoft Edge in an isolated browsing environment to better protect the device and data from malware.	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview
Controlled folder access/Ransomware	Basic	Microsoft	Controlled folder access in Windows helps protect against threats like ransomware by protecting folders, files,	https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders

Service	Skill Level	Owner	Description	Link
protection in Windows			and memory areas on the device from unauthorized changes by unfriendly applications.	
Microsoft Defender Antivirus	Basic	Microsoft	This tool is used to protect and detect endpoint threats including file-based and fileless malware. Built into Windows 10 and 11 and in versions of Windows Server.	https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows
Cybersecurity Evaluation Tool (CSET) and On-Site Cybersecurity Consulting	Basic	CISA	This tool assists organizations in protecting their key national cyber assets. The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.	https://github.com/cisagov/cset
CIS Hardware and Software Asset Tracker	Basic	Center for Internet Security	This tool is designed to help identify devices and applications. The spreadsheet can be used to track hardware, software, and sensitive information.	https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/

Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
PGP	Basic	Open Source	This tool encrypts emails with public key cryptography.	https://www.openpgp.org/
BitLocker for Microsoft Windows	Basic	Microsoft	This tool encrypts Microsoft Windows systems.	https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server
AdBlock	Basic	Open Source	This tool blocks pop-up ads, videos and other unwanted content whilst browsing.	https://gcatoolkit.org/tool/adblock/
Quad9 for Android	Basic	Open Source	This tool for Android devices is designed to help block users from accessing known sites that have viruses or other malware.	https://www.quad9.net/news/blog/quad9-connect-now-available-on-google-play/
Quad9	Basic	Open Source	This tool is designed to prevent computers and devices from connecting to malware or phishing sites.	https://quad9.net/
Google Safe Browsing	Basic	Google	This toolset identifies known phishing and malware across the web and helps notify users and website owners of potential harm. It is integrated into many major products and	https://safebrowsing.google.com

Service	Skill Level	Owner	Description	Link
			provides tools to webmasters.	
Project Shield	Basic	Google Jigsaw	Project Shield is a free service that defends news, human rights, and election monitoring sites from DDoS attacks	https://projectshield.withgoogle.com/landing
Google reCAPTCHA	Basic	Google	reCAPTCHA uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on a user's website.	https://www.google.com/recaptcha/about/
Web Risk	Basic	Google	Web Risk API is a User Protection Service from Google Cloud designed to reduce the risk of threats targeting user generated content. Web Risk API lets organizations compare URLs in their environment against a repository of over 1 million unsafe URLs.	https://cloud.google.com/web-risk
Google Security Command Center	Basic	Google	This tool helps users strengthen their security posture by evaluating their security and data attack surface; providing asset inventory and discovery; identifying	https://cloud.google.com/security-command-center

Service	Skill Level	Owner	Description	Link
			misconfigurations, vulnerabilities and threats; and helping them mitigate and remediate risks.	
Google OSS-Fuzz	Basic	Google	OSS-Fuzz aims to make common open source software more secure and stable by combining modern fuzzing techniques with scalable, distributed execution.	https://google.github.io/oss-fuzz/
Santa	Basic	Open Source	Santa is a binary authorization system for macOS.	https://santa.dev/
Go Safe Web	Basic	Open Source	Go Safe Web is a collection of libraries for writing secure-by-default HTTP servers in Go.	https://github.com/google/go-safeweb
Open Source Vulnerabilities (OSV)	Basic	Open Source	OSV is a vulnerability database and triage infrastructure for open source projects aimed at helping both open source maintainers and consumers of open source.	https://osv.dev/
Open Source Insights	Basic	Open Source	Open Source Insights is a searchable dependency graph with vulnerability information.	https://deps.dev/

Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
AllStar	Basic	Open Source	AllStar is a GitHub application for enforcing security policies and permissions.	https://github.com/ossf/allstar
Security Scorecards	Basic	Open Source	Security Scorecards is a collection of security health metrics for open source, allowing users to evaluate the security practices of an open source package before use. Results available publicly as a Google Cloud Big Query Dataset.	https://github.com/ossf/scorecard
Tink	Basic	Open Source	Tink is a multi-language, cross-platform, open-source library that provides cryptographic APIs that are secure, easy to use correctly, and hard(er) to misuse.	https://github.com/google/tink
Google Cybersecurity Action Team	Basic	Google	This service provides a number of security resources including security blueprints, whitepapers, threat reports, and information regarding recent vulnerabilities.	https://cloud.google.com/security/gcat
Tsunami Security Scanner	Basic	Open Source	Tsunami is a general purpose network security scanner with an extensible plugin system for detecting high	https://github.com/google/tsunami-security-scanner

Service	Skill Level	Owner	Description	Link
			severity vulnerabilities with high confidence.	
OpenDNS Home	Basic	Cisco	OpenDNS blocks phishing websites that try to steal your identity and login information by pretending to be a legitimate website.	https://signup.opendns.com/homefree/
CrowdStrike CRT	Advanced	CrowdStrike	CRT is a free community tool designed to help organizations quickly and easily review excessive permissions in their Azure AD environments. CRT helps determine configuration weaknesses and provides advice to mitigate this risk.	https://www.crowdstrike.com/resources/community-tools/crt-crowdstrike-reporting-tool-for-azure/
Tenable Nessus Essentials	Advanced	Tenable	This free version of a vulnerability assessment solution includes remote and local (authenticated) security checks, a client/server architecture with a web-based interface, and an embedded scripting language for writing your own plugins or understanding existing ones. Limited by default to 16 hosts.	https://www.tenable.com/products/nessus/nessus-essentials

Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
Alien Labs Open Threat Exchange (OTX) Endpoint Security	Advanced	AT&T Cybersecurity	This tool leverages data from Alien Labs OTX to help identify if endpoints have been compromised in major cyberattacks. Provides quick visibility into threats on all endpoints by scanning IOCs using OTX.	https://cybersecurity.att.com/open-threat-exchange
Alien Labs Open Threat Exchange (OTX)	Advanced	AT&T Cybersecurity	OTX provides open access to a global community of threat researchers and security professionals. It delivers community-generated threat data, enables collaborative research, and automates the process of updating security infrastructure with threat data from any source. OTX enables anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques.	https://cybersecurity.att.com/open-threat-exchange
ClamAV	Advanced	Cisco	ClamAV is an open-source (general public license [GPL]) antivirus engine used in a variety of situations, including email and web scanning, and endpoint security. It provides many utilities for users, including a flexible and scalable multi-	http://www.clamav.net/

Service	Skill Level	Owner	Description	Link
			threaded daemon, a command-line scanner, and an advanced tool for automatic database updates.	
Kali Linux Penetration Testing Platform	Advanced	Kali Linux Project	Kali Linux contains several hundred tools targeted toward various information security tasks, such as penetration testing, security research, computer forensics, and reverse engineering.	https://www.kali.org/
Cloudflare Zero Trust Services	Advanced	Cloudflare	Cloudflare Zero Trust Services are essential security controls to keep employees and apps protected online across 3 network locations and up to 50 users. Services include: Zero Trust Network Access; Secure Web Gateway, Private Routing to IP/Hosts; HTTP/S Inspection and Filters; Network Firewall as a Service; DNS Resolution and Filters; and Cloud Access Security Broker.	https://www.cloudflare.com/plans/free/
Microsoft Sysinternals Security Utilities	Advanced	Microsoft	Sysinternals Security Utilities are free, downloadable tools for diagnosing, troubleshooting, and	https://docs.microsoft.com/en-us/sysinternals/downloads/security-utilities

Service	Skill Level	Owner	Description	Link
			deeply understanding the Windows platform.	
Memory integrity	Advanced	Microsoft	Memory integrity in Windows—also known as Hypervisor-protected code integrity (HVCI)—is a Windows security feature that makes it difficult for malicious programs to use low-level drivers to hijack computers.	https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/enable-virtualization-based-protection-of-code-integrity
RiskIQ Community	Advanced	Microsoft	The RiskIQ community offers free access to internet intelligence, including thousands of OSINT articles and artifacts. Community users can investigate threats by pivoting through attacker infrastructure data, understand what digital assets are internet-exposed, and map and monitor their external attack surface.	https://community.riskiq.com/home
IBM X-Force Exchange	Advanced	IBM	IBM X-Force Exchange is a cloud-based threat intelligence platform that allows users to consume, share, and act on threat intelligence. It enables users to conduct rapid research of the latest global security threats,	https://www.ibm.com/products/xforce-exchange

Service	Skill Level	Owner	Description	Link
			aggregate actionable intelligence, consult with experts, and collaborate with peers.	
Mandiant Attack Surface Management	Advanced	Mandiant	This early warning system for information security allows you to: create comprehensive visibility through graph-based mapping; know when assets change to stay ahead of the threat; and empower security operations to mitigate real-world threats.	https://www.mandiant.com/advantage/attack-surface-management/get-started
Mandiant Threat Intelligence	Advanced	Mandiant	Free access to the Mandiant Threat Intelligence Portal helps users understand recent security trends, proactively hunt threat actors, and prioritize response activities.	https://www.mandiant.com/advantage/threat-intelligence/free-version
Splunk Synthetic Adversarial Log Objects (SALO)	Advanced	Splunk	SALO is a framework for generating synthetic log events without the need for infrastructure or actions to initiate the event that causes a log event.	https://github.com/splunk/salo
Splunk Attack Detection	Advanced	Splunk	This tool simplifies the process of collecting MITRE ATT&CK® techniques	https://github.com/splunk/attack-detections-collector

Service	Skill Level	Owner	Description	Link
Collector (ADC)			from blogs or PDFs and mapping ATT&CK TTPs to Splunk detection content.	
Splunk Attack Range	Advanced	Splunk	This tool enables simulated attacks in a repeatable cloud-enabled (or on-premises) lab with a focus on Atomic Red Team integration.	https://github.com/splunk/attack_range
Splunk Training	Advanced	Splunk	Splunk Training is a free, hosted platform for on-demand training with hands-on practice addressing specific attacks and realistic scenarios.	https://bots.splunk.com
VMware Carbon Black User Exchange	Advanced	VMware	Carbon Black User Exchange provides access to real-time threat research data shared by a global community of security professionals.	https://community.carbonblack.com/
Carbon Black TAU Excel 4 Macro Analysis	Advanced	VMware	This tool tests endpoint security solutions against Excel 4.0 macro techniques.	https://github.com/carbonblack/excel4-tests
Paros Proxy	Advanced	Open Source	This Java-based tool is used to find vulnerabilities in web applications. It includes a web traffic recorder, web	https://www.parosproxy.org/

Service	Skill Level	Owner	Description	Link
			spider, hash calculator, and a scanner for testing common web application attacks, such as SQL injection and cross-site scripting.	
Cyber Security Tools by SANS Instructors	Advanced	SANS	This website includes links to an array of open-source tools built by cybersecurity instructors.	https://www.sans.org/tools/
Windows Management Instrumentation Command-line	Advanced	Microsoft	The WMI command-line (WMIC) utility provides a command-line interface for Windows Management Instrumentation (WMI). WMIC is compatible with existing shells and utility commands.	https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmic
Let's Encrypt	Advanced	Open Source	This tool provides a free digital certificate to enable HTTPS (SSL/TLS) for websites.	https://letsencrypt.org/getting-started/
Hping	Advanced	Open Source	This tool assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It can be useful for performing security assessments.	http://www.hping.org/

Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
Aircrack	Advanced	Open Source	Aircrack is a suite of tools for testing the strength of passwords used for wireless networks.	https://www.aircrack-ng.org/
Nikto	Advanced	Open Source	Nikto is an open source (GPL) web server scanner that performs vulnerability scanning against web servers for multiple items, including dangerous files and programs. Nitko checks for outdated versions of web server software. It also checks for server configuration errors and any possible vulnerabilities they might have introduced.	https://cirt.net/nikto2
w3af	Advanced	Open Source	W3af is a flexible framework for finding and exploiting web application vulnerabilities, featuring dozens of web assessment and exploitation plugins.	http://w3af.org/
VMware Fusion Player	Advanced	VMware	This tool allows Mac users to run Windows, Linux, containers, Kubernetes, and more in virtual machines without rebooting.	https://customerconnect.vmware.com/web/vmware/evalcenter?p=fusion-player-personal

Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
Secureworks PhishInSuits	Advanced	Secureworks	The PhishInSuits (pis.py) tool conducts security assessments and tests control frameworks against scenarios, such as BEC attacks. It combines this variation of illicit consent attacks with SMS-based phishing to emulate BEC campaigns and includes automated data-exfiltration capabilities.	https://github.com/secureworks/PhishInSuits
Secureworks WhiskeySAML	Advanced	Secureworks	The WhiskeySAML tool automates the remote extraction of an ADFS signing certificate. WhiskeySAML then uses this signing certificate to launch a Golden SAML attack and impersonate any user within the target organization.	https://github.com/secureworks/whiskeysamlandfriends
Collabfiltrator	Advanced	Secureworks	This tool is designed to exfiltrate blind remote code execution output over DNS via Burp Collaborator.	https://github.com/0xC01DF00D/Collabfiltrator
O365Spray	Advanced	Secureworks	This tool is a username enumeration and password spraying tool aimed at Microsoft Office 365.	https://github.com/0xZDH/o365spray

Free Cyber Security Services and Tools
From the Cybersecurity & Infrastructure Security Agency

Service	Skill Level	Owner	Description	Link
Tachyon	Advanced	Securework s	Tachyon is a rapid web application security reconnaissance tool. It is designed to crawl a web application and look for leftover or non-indexed files with the addition of reporting pages or scripts leaking internal data (a.k.a "blind" crawling). It is used from the command line and targeted at a specific domain. Tachyon uses an internal database to construct these blind queries swiftly.	https://github.com/delvelabs/tachyon
Vane2	Advanced	Securework s	Vane2 is a WordPress site vulnerability scanner. It is meant to be targeted at WordPress websites and identifies the corresponding WordPress version as well as its installed plugins in order to report known vulnerabilities on each.	https://github.com/delvelabs/vane2
Batea	Advanced	Securework s	Batea is a practical application of machine learning for pentesting and network reconnaissance. It consumes map reports and uses a context-driven network device ranking framework based on the anomaly detection	https://github.com/delvelabs/batea

Service	Skill Level	Owner	Description	Link
			family of machine learning algorithms. The goal of Batea is to allow security teams to automatically filter interesting network assets in large networks using nmap scan reports.	
Checkov	Advanced	Palo Alto Networks	This tool scans Infrastructure as Code (IaC), container images, open-source packages, and pipeline configuration for security errors. With hundreds of built-in policies, Checkov surfaces misconfigurations and vulnerabilities in code across developer tools (CLI, IDE) and workflows (CI/CD pipelines).	https://github.com/bridgecrewio/checkov
Palo Alto Networks Unit 42- Actionable Threat Objects and Mitigations (ATOMs)	Advanced	Palo Alto Networks	ATOMs is a free repository of observed behaviors of several common threat adversaries, mapped to the MITRE ATT&CK framework. ATOMs can be filtered by targeted sector, region, or malware used for ease of information sharing and deployment of recommended security mitigations.	https://unit42.paloaltonetworks.com/atoms/ ;

Service	Skill Level	Owner	Description	Link
Google ClusterFuzz	Advanced	Google	ClusterFuzz is a scalable fuzzing infrastructure that finds security and stability issues in software. It is also the fuzzing backend for Google OSS-Fuzz. ClusterFuzz Lite is simple CI-integrated fuzzing based on ClusterFuzz.	https://google.github.io/clusterfuzz/

Take Steps to Quickly Detect a Potential Intrusion

Service	Skill Level	Owner	Description	Link
Microsoft Defender Antivirus	Basic	Microsoft	This tool protects and detects endpoint threats, including file-based and fileless malware. Built into Windows 10 and 11 and in versions of Windows Server.	https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows
Microsoft Safety Scanner	Basic	Microsoft	Microsoft Safety Scanner is a scan tool designed to find and remove malware from Windows computers. It can run scans to find malware and try to reverse changes	https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Service	Skill Level	Owner	Description	Link
			made by identified threats.	
Windows Malicious Software Removal tool	Basic	Microsoft	This tool is released by Microsoft on a monthly cadence as part of Windows Update or as a standalone tool. It can be used to find and remove specific prevalent threats and reverse the changes they have made.	https://support.microsoft.com/en-us/topic/remove-specific-prevalent-malware-with-windows-malicious-software-removal-tool-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0
MSTICpy	Basic	Microsoft	MSTICPy is a SIEM-agnostic package of Python tools for security analysts to assist in investigations and threat hunting. It is primarily designed for use in Jupyter notebooks.	https://msticpy.readthedocs.io/en/latest/
Google Safe Browsing	Basic	Google	This service identifies known phishing and malware across the web and helps notify users and website owners of potential harm. It is integrated into many major products and	https://safebrowsing.google.com

Service	Skill Level	Owner	Description	Link
			provides tools to webmasters.	
Mandiant Red Team and Investigative Tools	Advanced	Mandiant	These tools are designed to confirm and investigate suspected security compromises.	https://github.com/Mandiant
Splunk Connect for Syslog	Advanced	Splunk	This tool is used for getting syslog-based data into Splunk, including functions for data filtering and parsing.	https://splunkbase.splunk.com/app/4740/#/overview
Enterprise Log Search and Archive (ELSA)	Advanced	Open source	Enterprise Log Search and Archive (ELSA) is a three-tier log receiver, archiver, indexer, and web front end for incoming syslog.	https://github.com/mcholste/elsa
Mandiant Azure AD Investigator	Advanced	Mandiant	This repository contains a PowerShell module for detecting artifacts that may be indicators of UNC2452 and other threat actor activity. Some indicators are "high-fidelity"	https://github.com/mandiant/Mandiant-Azure-AD-Investigator

Service	Skill Level	Owner	Description	Link
			indicators of compromise; other artifacts are so-called "dual-use" artifacts. Dual-use artifacts may be related to threat actor activity, but also may be related to legitimate functionality.	
VirusTotal	Advanced	Google	VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a variety of tools, to extract signals from the studied content. Users can select a file from a computer via the browser and send it to VirusTotal. Submissions may be scripted in any programming language using the HTTP-based public API.	https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works
Netfilter	Advanced	Open Source	Netfilter is a packet filter implemented in the standard Linux kernel. The user space iptables tool is	https://www.netfilter.org/

Service	Skill Level	Owner	Description	Link
			used for configuration. It supports packet filtering (stateless or stateful), many kinds of network address and port translation (NAT/NAPT), and multiple API layers for third-party extensions. It includes many different modules for handling unruly protocols, such as FTP.	
Wireshark	Advanced	Open Source	Wireshark is an open-source multi-platform network protocol analyzer that allows users to examine data from a live network or from a capture file on disk. The tool can interactively browse capture data, delving down into just the level of packet detail needed. Wireshark has multiple features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds	https://www.wireshark.org/

Service	Skill Level	Owner	Description	Link
			of protocols and media types.	
Ettercap	Advanced	Open Source	Ettercap is a suite for adversary-in-the-middle attacks on LAN that includes sniffing of live connections, content filtering on the fly, and many other features. It supports active and passive dissection of many protocols (including ciphered protocols) and includes many features for network and host analysis.	http://ettercap.sourceforge.net/
Kismet	Advanced	Open Source	Kismet is a console (ncurses)-based 802.11 layer-2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively sniffing and can decloak hidden (non-beaconing) networks if they are in use. It can automatically detect network IP blocks by sniffing	https://www.kismetwireless.net/

Service	Skill Level	Owner	Description	Link
			TCP, UDP, ARP, and DHCP packets, log traffic in Wireshark/tcpdump compatible format, and even plot detected networks and estimated ranges on downloaded maps.	
Snort	Advanced	Cisco	This network intrusion detection and prevention system conducts traffic analysis and packet logging on IP networks. Through protocol analysis, content searching, and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior. Snort uses a flexible rule-based language to describe traffic that it should collect or pass, and a modular detection engine. The related free Basic Analysis and	https://www.snort.org/

Service	Skill Level	Owner	Description	Link
			Security Engine (BASE) is a web interface for analyzing Snort alerts.	
sqlmap	Advanced	Open Source	sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of back-end database servers. It comes with a broad range of features, from database fingerprinting to fetching data from the DB and accessing the underlying file system and executing OS commands via out-of-band connections.	http://sqlmap.org/
RITA	Advanced	Open Source	Real Intelligence Threat Analytics (R-I-T-A) is an open-source framework for detecting command and control communication through network	https://www.activecountermeasures.com/free-tools/rita/

Service	Skill Level	Owner	Description	Link
			traffic analysis. The RITA framework ingests Zeek logs or PCAPs converted to Zeek logs for analysis.	
Secureworks Dalton	Advanced	Secureworks	Dalton is a system that allows a user to run network packet captures against a network sensor of their choice using defined rulesets and/or bespoke rules. Dalton covers Snort/Suricata/Zeek analysis in one system.	https://github.com/secureworks/dalton

Ensure That The Organization is Prepared to Respond if an Intrusion Occurs

Service	Skill Level	Owner	Description	Link
GRR Rapid Response	Basic	Google	GRR Rapid Response is an incident response framework focused on remote live forensics. The goal of GRR is to support forensics and investigations in a fast, scalable manner to allow analysts to quickly triage attacks and perform analysis remotely.	https://grr-doc.readthedocs.io
Microsoft PsExec	Advanced	Microsoft	PsExec is a lightweight telnet replacement that	https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

Service	Skill Level	Owner	Description	Link
			lets users execute processes on other systems (complete with full interactivity for console applications) without having to manually install client software. PsExec's uses include launching interactive command-prompts on remote systems and remote-enabling tools such as IpConfig that otherwise do not have the ability to show information about remote systems.	
VMware Workstation Player	Advanced	VMware	This tool runs a single virtual machine on a Windows or Linux PC. It can be used when setting up an environment to analyze malware.	https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
VMware ESXi - Free	Advanced	VMware	This tool can be used when setting up an environment to analyze malware. It is a bare-metal hypervisor that installs directly onto a physical server, providing direct access to, and control of, underlying resources. It can be used to effectively partition hardware to consolidate applications.	https://www.vmware.com/products/esxi-and-esx.html
dTimeWolf	Advanced	Google	dTimeWolf is an open-source framework for orchestrating forensic collection, processing, and data export.	https://dftimewolf.readthedocs.io
Turbinia	Advanced	Google	Turbinia is an open-source framework for	https://turbinia.readthedocs.io

Service	Skill Level	Owner	Description	Link
			deploying, managing, and running distributed forensic workloads.	
Timesketch	Advanced	Open Source	Timesketch is an open-source tool for collaborative forensic timeline analysis. Using sketches, users and their collaborators can easily organize timelines and analyze them all at the same time.	https://timesketch.org/

Maximize the Organization's Resilience to a Destructive Cyber Incident

Service	Skill Level	Owner	Description	Link
Windows Auto-Backup	Basic	Microsoft	This tool sets up automatic backups of Windows 10 and 11 operating systems.	https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-352091d2-bb9d-3ea3-ed18-52ef2b88cbef
Google Backup & Sync	Basic	Google	This tool backs up files on Windows or Mac computers. **Note:** it does not allow users to restore their system; it only saves copies of files.	https://support.google.com/drive/answer/7638428
Microsoft Threat Modeling Tool	Advanced	Microsoft	This tool is designed to make threat modeling easier for developers through a standard notation for visualizing system components, data flows, and security boundaries.	https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
Microsoft SecCon Framework	Advanced	Microsoft	This framework is designed to help prioritize endpoint hardening recommendations.	https://github.com/microsoft/SecCon-Framework

Free Cyber Security Services and Tools From the Cybersecurity & Infrastructure Security Agency