Top Free Cybersecurity Services and Tools

@2023

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

CyberSecurity Tools

Top 26 Open Source Cyber Security Tools that are Best for you

Free Cybersecurity Services and Tools

As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.

The list is not comprehensive and is subject to change pending future additions. CISA applies neutral principles and criteria to add items and maintains sole and unreviewable discretion over the determination of items included. CISA does not attest to the suitability or effectiveness of these services and tools for any particular use case. CISA does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

Foundational Measures

All organizations should take certain foundational measures to implement a strong cybersecurity program:

- **Fix the known security flaws in software.** Check the CISA Known Exploited Vulnerabilities (KEV) Catalog for software used by your organization and, if listed, update the software to the latest version according to the vendor's instructions. **Note:** CISA continually updates the KEV catalog with known exploited vulnerabilities.
- **Implement multifactor authentication (MFA).** Use multifactor authentication where possible. MFA is a layered approach to securing your online accounts and the data they contain. When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service grants you access. Using MFA protects your account more than just using a username and password. Why? Because even if one factor (like your password) becomes

compromised, unauthorized users will be unable to meet the second authentication requirement, ultimately stopping them from gaining access to your accounts.

- **Halt bad practices.** Take immediate steps to: (1) replace end-of-life software products that no longer receive software updates; (2) replace any system or products that rely on known/default/unchangeable passwords; and (3) adopt MFA (see above) for remote or administrative access to important systems, resources, or databases.
- **Sign up for CISA's Cyber Hygiene Vulnerability Scanning.** Register for this service by emailing vulnerability@cisa.dhs.gov. Once initiated, this service is mostly automated and requires little direct interaction. CISA performs the vulnerability scans and delivers a weekly report. After CISA receives the required paperwork, scanning will start within 3 business days, and organizations will begin receiving reports within two weeks. **Note:** vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices.
- **Get your Stuff Off Search (S.O.S.).** While zero-day attacks draw the most attention, frequently, less complex exposures to both cyber and physical security are missed. Get your Stuff Off Search–S.O.S.–and reduce internet attack surfaces that are visible to anyone on web-based search platforms.

Free Services and Tools

After making progress on the measures above, organizations can use the free services and tools listed below to mature their cybersecurity risk management. These resources are categorized according to the four goals outlined in CISA Insights: Implement Cybersecurity Measures Now to Protect Against Critical Threats:

1. Reducing the likelihood of a damaging cyber incident;
2. Detecting malicious activity quickly;
3. Responding effectively to confirmed incidents; and
4. Maximizing resilience.

Network Security Monitoring: Zeek

AntiVirus: ClamAV

Vulnerability Scanning: OpenVAS

Incident Response: TheHive

Security Appliance: PFSense

Analytics: Elastic

Endpoint Visibility: Osquery

Packet Capture and Search: Arkime

XDR and SIEM: Wazuh, Alien Vault Ossim

Forensic and Incident Response: Velociraptor

Threat Intelligence: MISP project

Security Operating System: Kali Linux, Parrot

Identity and Access Management: OpenIAM

Malware Analysis: Yara

VPN: Wireguard

HIDS: OSSEC

IDS/IPS: Suricata

Anti-phishing: Phish Report

Log Management: Graylog

DevOps: Trivy

EDR: OpenEDR

Penetration Testing: Metasploit

Network Mapper: NMAP

1. Zeek:

Zeek, formerly known as Bro, is an open-source network security monitoring tool that analyzes network traffic in real time, providing insights into network activity, security threats, and performance issues. Zeek operates as a passive network sniffer, meaning it does not generate any traffic or interfere with network operations. It can be used to monitor a wide range of network protocols, including HTTP, SMTP, DNS, and SSH, and can detect and alert on security threats such as malware, botnets, and denial of service attacks. Zeek also provides extensive logging and reporting capabilities, allowing users to analyze and visualize data from multiple sources.

2. ClamAV:

ClamAV is an open-source antivirus software that is designed to detect and remove malware from computers and servers. It uses a combination of signature-based detection, heuristics, and machine learning to identify and classify potential threats. ClamAV is widely used by individuals, businesses, and organizations to protect against viruses, worms, Trojans, and other types of malware. It is available for Windows, Linux, and macOS and can be easily integrated into existing security systems and workflows.

3. OpenVAS:

OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner that helps organizations identify and prioritize vulnerabilities in their network infrastructure, applications, and devices. It utilizes a database of known vulnerabilities and exploits, as well as a variety of tools and techniques, to scan systems and report on potential weaknesses. OpenVAS can be used to assess the security of systems running a variety of operating systems, including Windows, Linux, and macOS. It is a comprehensive tool that is used by a

wide range of organizations to improve the security of their systems and networks.

4. TheHive:

TheHive is an open-source incident response platform that is designed to help organizations quickly and effectively respond to security incidents and threats. It provides a central platform for managing and tracking incidents and tools for analyzing and triaging threats, collaborating with team members, and communicating with stakeholders. TheHive integrates with a variety of other security tools and technologies, including malware analysis platforms, threat intelligence feeds, and SIEM systems, to provide a holistic view of incidents and facilitate efficient response.

5. PFSense:

PFSense is an open-source security appliance that provides firewall, VPN, and router capabilities in a single package. It is designed for use in small to medium-sized businesses and organizations and can be easily configured to meet the specific

security needs of a given organization. PFSense includes a web-based management interface that allows administrators to easily set up and manage firewall rules, VPN connections, and others to enhance their network security.

6. Elastic:

Elastic is an open-source analytics platform that helps organizations search, analyze, and visualize data from a wide range of sources. It includes a suite of tools, including Elasticsearch, Logstash, and Kibana, that can be used to collect, process, and analyze data in real time. Elastic is particularly well-suited for analyzing large volumes of data, such as log files, in order to identify trends, patterns, and anomalies. It is used by a wide range of organizations, including businesses, governments, and non-profits, to gain insights into their data and improve decision-making.

7. Osquery:

Osquery is an open-source endpoint visibility tool that enables organizations to monitor and track the

activity and configuration of their systems and devices. It allows administrators to define and execute custom queries using a SQL-like language, providing insights into system state and performance. Osquery can be used to identify security issues, such as missing patches or misconfigured settings, as well as to track system changes over time. It is available for Windows, Linux, and macOS and can be easily integrated into existing security workflows and tools.

8. Arkime:

Arkime is an open-source packet capture and search tool that allows organizations to capture, store, and analyze network traffic in real time. It utilizes a distributed architecture and a powerful search engine, enabling users to quickly and easily search through large volumes of traffic data. Arkime is particularly useful for investigating security incidents and identifying patterns and trends in network activity. It is available for Linux and can be easily integrated into existing security systems and workflows.

9. Wazuh:

Wazuh is an open-source XDR (extended detection and response) and SIEM (security information and event management) platform that helps organizations detect and respond to security threats. It combines real-time monitoring with advanced analytics and machine learning to identify and prioritize threats and includes a range of tools and features for incident response, such as threat hunting, incident triage, and remediation. Wazuh is available for Windows, Linux, and macOS, and can be easily integrated into existing security workflows and tools.

10. Alien Vault Ossim:

Alien Vault Ossim is an open-source SIEM (security information and event management) platform that helps organizations collect, analyze, and respond to security threats. It combines real-time monitoring with advanced analytics and machine learning to identify and prioritize threats, and includes a range of tools and features for incident response, such as threat hunting, incident triage, and remediation. Alien Vault Ossim is available for Windows, Linux,

and macOS and can be easily integrated into existing security workflows and tools.

11. Velociraptor:

Velociraptor is an open-source forensic and incident response tool that helps organizations investigate and respond to security incidents. It provides a range of features for analyzing system activity and identifying anomalies, including memory analysis, network traffic analysis, and file system analysis. Velociraptor is available for Windows and Linux and can be easily integrated into existing security workflows and tools.

12. MISP project:

The MISP project (Malware Information Sharing Platform) is an open-source platform for sharing and collaborating on threat intelligence information. It provides a central repository for storing and sharing threat intelligence data and tools for analyzing and disseminating that data to relevant stakeholders. The MISP project is used by a wide range of organizations, including businesses, governments,

and non-profits, to improve their ability to detect and respond to security threats.

13. Kali:

Kali is an open-source security operating system that is designed specifically for penetration testing and digital forensics. It includes a wide range of tools and features for testing the security of systems and networks, including tools for network mapping, vulnerability scanning, and exploitation. Kali is based on the Debian Linux distribution and is available for a variety of platforms, including desktop and laptop computers, as well as virtual machines. It is widely used by security professionals, researchers, and enthusiasts for testing the security of systems and networks.

14. Parrot:

Parrot is an open-source security operating system designed for a variety of security-related tasks, including penetration testing, digital forensics, and incident response. It is based on the Debian Linux distribution and includes a wide range of tools and

features for testing the security of systems and networks, including tools for network mapping, vulnerability scanning, and exploitation. Parrot is available for a variety of platforms, including desktop and laptop computers, as well as virtual machines, and is widely used by security professionals, researchers, and enthusiasts for testing the security of systems and networks.

15. OpenIAM:

OpenIAM is an open-source identity and access management (IAM) platform that helps organizations manage and secure user identities and access to systems and resources. It includes a range of tools and features for managing user accounts, authentication, and authorization, as well as for implementing and enforcing security policies. OpenIAM is available for a variety of platforms and can be easily integrated into existing security systems and workflows.

16. Yara:

Yara is an open-source tool for detecting and identifying patterns in files, networks, and other data sources. It utilizes a simple yet powerful, rules-based system to identify patterns of interest, such as malicious code, and can be used to scan and analyze a wide range of data types, including executables, documents, and network traffic. Yara is widely used by security professionals, researchers, and enthusiasts for detecting and analyzing potential threats.

17. Wireguard:

Wireguard is an open-source virtual private network (VPN) tool that is designed to provide fast, secure and easy-to-use VPN connectivity. It utilizes state-of-the-art cryptographic techniques to encrypt and protect data in transit and is designed to be simple to set up and maintain. Wireguard is available for a variety of platforms, including desktop and mobile devices, and can be easily integrated into existing security systems and workflows.

18. OSSEC:

OSSEC (Open Source Security) is an open-source host-based intrusion detection system (HIDS) that helps organizations monitor and protect their systems and networks from potential threats. It utilizes a range of techniques, including file integrity checking, logs analysis, and network monitoring, to identify and alert to potential security issues.

19. Suricata:

Suricata is an open-source intrusion detection/prevention system (IDS/IPS) that helps organizations monitor and protects their systems and networks from potential threats. It utilizes a range of techniques, including packet capture and analysis, signature-based detection, and anomaly detection, to identify and alert potential security issues.

20. Shuffler:

Shuffler is an open-source security orchestration, automation, and response (SOAR) platform that helps organizations automate and streamline their security processes and workflows. It provides a

range of tools and features for automating tasks, such as incident triage, threat analysis, and remediation, as well as for integrating with other security tools and technologies.

21. Phish Report:

Phish Report is an open-source anti-phishing tool that helps organizations protect their users from phishing scams and other types of social engineering attacks. It provides a range of features for detecting and responding to phishing attacks, including email analysis, URL tracking, and user reporting. Phish Report is available for a variety of platforms, including Windows, Linux, and macOS, and can be easily integrated into existing security systems and workflows.

22. Graylog:

Graylog is an open-source log management platform that helps organizations collect, analyze, and visualize data from a wide range of sources. It includes a range of tools and features for collecting, storing, and processing log data, as well as for

analyzing and visualizing that data to identify trends, patterns, and anomalies.

23. Trivy:

Trivy is an open-source DevOps/Infrastructure as Code (IaC) scanning tool that helps organizations identify and fix vulnerabilities in their software and infrastructure. It utilizes a range of techniques, including static analysis, dynamic analysis, and manual testing, to identify potential vulnerabilities and provide recommendations for fixing them.

24. OpenEDR:

OpenEDR (Open Endpoint Detection and Response) is an open-source endpoint detection and response (EDR) platform that helps organizations monitor and protect their systems and networks from potential threats. It utilizes a range of techniques, including file integrity checking, log analysis, and network monitoring, to identify and alert to potential security issues.

25. Metasploit:

Metasploit is an open source penetration testing tool that helps organizations test the security of their systems and networks. It includes a wide range of tools and features for identifying and exploiting vulnerabilities, as well as for simulating attacks and evaluating the effectiveness of security measures.

26. NMAP:

NMAP (Network Mapper) is an open source network mapping and security scanning tool that helps organizations identify and assess the security of their systems and networks. It includes a wide range of features for mapping networks, identifying live hosts, and scanning for vulnerabilities, as well as for analyzing and visualizing data.

All in all, there are wide variety of open-source cybersecurity tools available to help organizations and individuals safeguard against cyber threats. These tools cover a range of categories, including network security monitoring, antivirus, vulnerability scanning, incident response, security appliances,

analytics, endpoint visibility, packet capture and search, XDR Conclusion. There are a wide variety of open-source cybersecurity tools available to help organizations and individuals safeguard against cyber threats.

Open-source cybersecurity tools can be an effective and cost-effective solution for organizations and individuals looking to enhance their cybersecurity defenses. These tools are typically developed and maintained by a community of volunteers and are often updated and improved on a regular basis to keep up with the evolving threat landscape.

Reducing the Likelihood of a Damaging Cyber Incident

Service	Skill Level	Owner	Description	Link
OpenVAS	Basic	Greenbone	This is a vulnerability scanner and capabilities include unauthenticated and authenticated	OpenVAS - Open Vulnerability Assessment Scanner

Service	Skill Level	Owner	Description	Link
			testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.	
Network Reporting	Basic	Shadow Server	A subscription service that sends custom remediation reports to inform organizations about the state of its networks and security exposures.	Network Reporting | The Shadowserver Foundation
Vulcan Cyber	Basic	Remedy Cloud	A searchable database of	https://vulcan.io/remedy-cloud/

Service	Skill Level	Owner	Description	Link
			remedies and fixes for thousands of known vulnerabilities. It also provides highlight trend analytics such as "most-searched CVEs" and "most-visited vulnerability remedies."	
Ransomware Risk Assessment	Basic	Zscaler	This service assesses an organization's ability to counteract a ransomware infection and its spread, but also to resume operations in case of an infection. This tool scans defenses against ransomware-specific	testmydefenses.com

Service	Skill Level	Owner	Description	Link
			intrusion, lateral movement, and exfiltration methods. It is safe to use and runs within the browser.	
Internet Threat Exposure Analysis	Basic	Zscaler	This tool analyzes an organization's environment to cyber risk posture. It scans security stack to find common intrusion and data exfiltration methods left exposed. It is safe to use and runs within the browser. It won't introduce malware, and doesn't access data or change settings.	Free, Instant Security Scan - It's 100% Safe | Zscaler
CISA Cybersecurity	Basic	CISA	CISA provides automatic updates to subscribers via	https://www.cisa.gov/subscribe-updates-cisa

Service	Skill Level	Owner	Description	Link
Publications			email, RSS feeds, and social media. Subscribe to be notified of CISA publications upon release.	
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
Immunet Antivirus	Basic	Cisco	Immunet is a malware and antivirus protection	https://www.immunet.com/

Service	Skill Level	Owner	Description	Link
			system for Microsoft Windows that utilizes 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	https://www.cloudflare.com/plans/free/

Service	Skill Level	Owner	Description	Link
			browser. Cloudflare allows any internet property to use SSL with the click of a button.	
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 protection in Windows	Basic	Microsoft	Controlled folder access in Windows helps protect against threats like ransomware by protecting folders, files, and memory areas on the device from	https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders

Service	Skill Level	Owner	Description	Link
			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	https://github.com/cisagov/cset

Service	Skill Level	Owner	Description	Link
			systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.	
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/
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

Service	Skill Level	Owner	Description	Link
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	https://safebrowsing.google.com

Service	Skill Level	Owner	Description	Link
			of potential harm. It is integrated into many major products and 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	https://cloud.google.com/web-risk

Service	Skill Level	Owner	Description	Link
			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.	
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 misconfigurations,	https://cloud.google.com/security-command-center

Service	Skill Level	Owner	Description	Link
			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 Vulnerabil	Basic	Open Source	OSV is a vulnerability database and	https://osv.dev/

Service	Skill Level	Owner	Description	Link
ities (OSV)			triage infrastructure for open source projects aimed at helping both open source maintainers and consumers of open source.	
Open Source Insights	Basic	Open Source	Open Source Insights is a searchable dependency graph with vulnerability information.	https://deps.dev/
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	https://github.com/ossf/scorecard

Service	Skill Level	Owner	Description	Link
			security practices of an open source package before use. Results available publicly as a Google Cloud Big Query Dataset.	
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,	https://cloud.google.com/security/gcat

Service	Skill Level	Owner	Description	Link
			threat reports, and information regarding recent vulnerabilities.	
Tsunami Security Scanner	Basic	Open Source	Tsunami is a general purpose network security scanner with an extensible plugin system for detecting high severity vulnerabilities with high confidence.	https://github.com/google/tsunami-security-scanner
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/
Continuous Monitorin	Basic	Security Scorecard	Security ratings provide an objective, data-	Free Security Rating | SecurityScorecard

Service	Skill Level	Owner	Description	Link
g & Security Ratings			driven view of your company's cybersecurity risk exposure and cybersecurity hygiene, which are quantified and scored in an easy-to-understand A-F (0-100) cyber security rating.	
Binary Edge	Basic	Binary Edge	This tool continuously collects and correlates data from internet accessible devices, allowing organizations to see what is their attack surface and what they are exposing to attackers. No-cost offering is limited to one user and limited monthly scans.	BinaryEdge Portal

Service	Skill Level	Owner	Description	Link
Atomic Red Team	Basic	Open Source	Atomic Red Team™ is a PowerShell-based execution framework and provides a library of simple tests that every security team can execute to test their defenses. Tests are focused, have few dependencies, and are defined in a structured format that can be used by automation frameworks. Note: Use of this tool could make it more difficult for some organizations to identify malicious PowerShell usage.	Meet the Atomic Family | Atomic Red Team

Service	Skill Level	Owner	Description	Link
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,	https://www.tenable.com/products/nessus/nessus-essentials

Service	Skill Level	Owner	Description	Link
			and an embedded scripting language for writing your own plugins or understanding existing ones. Limited by default to 16 hosts.	
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	Advanced	AT&T Cybersecurity	OTX provides open access to a global community of	https://cybersecurity.att.com/open-threat-exchange

Service	Skill Level	Owner	Description	Link
Exchange (OTX)			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.	

Service	Skill Level	Owner	Description	Link
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-threaded daemon, a command-line scanner, and an advanced tool for automatic database updates.	http://www.clamav.net/
Kali Linux Penetration Testing Platform	Advanced	Kali Linux Project	Kali Linux contains several hundred tools targeted toward various information	https://www.kali.org/

Service	Skill Level	Owner	Description	Link
			security tasks, such as penetration testing, security research, computer forensics, and reverse engineering.	
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	https://www.cloudflare.com/plans/free/

Service	Skill Level	Owner	Description	Link
			Service; DNS Resolution and Filters; and Cloud Access Security Broker.	
Microsoft Sysinternals Security Utilities	Advanced	Microsoft	Sysinternals Security Utilities are free, downloadable tools for diagnosing, troubleshooting, and deeply understanding the Windows platform.	https://docs.microsoft.com/en-us/sysinternals/downloads/security-utilities
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	https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/enable-virtualization-based-protection-of-code-integrity

Service	Skill Level	Owner	Description	Link
			drivers to hijack computers.	
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

Service	Skill Level	Owner	Description	Link
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, aggregate actionable intelligence, consult with experts, and collaborate with peers.	https://www.ibm.com/products/xforce-exchange
Mandiant Attack Surface Management	Advanced	Mandiant	This early warning system for information security allows you to: create comprehensive visibility through graph-	https://www.mandiant.com/advantage/attack-surface-management/get-started

Service	Skill Level	Owner	Description	Link
			based mapping; know when assets change to stay ahead of the threat; and empower security operations to mitigate real-world threats.	
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	https://github.com/splunk/salo

Service	Skill Level	Owner	Description	Link
			actions to initiate the event that causes a log event.	
Splunk Attack Detection Collector (ADC)	Advanced	Splunk	This tool simplifies the process of collecting MITRE ATT&CK® techniques from blogs or PDFs and mapping ATT&CK TTPs to Splunk detection content.	https://github.com/splunk/attack-detections-collector
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

Service	Skill Level	Owner	Description	Link
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	https://www.parosproxy.org/

Service	Skill Level	Owner	Description	Link
			vulnerabilities in web applications. It includes a web traffic recorder, web 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	https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmic

Service	Skill Level	Owner	Description	Link
			(WMI). WMIC is compatible with existing shells and utility commands.	
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/
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/

Service	Skill Level	Owner	Description	Link
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	http://w3af.org/

Service	Skill Level	Owner	Description	Link
			vulnerabilities, featuring dozens of web assessment and exploitation plugins.	
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
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	https://github.com/secureworks/PhishInSuits

Service	Skill Level	Owner	Description	Link
			SMS-based phishing to emulate BEC campaigns and includes automated data-exfiltration capabilities.	
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	https://github.com/0xC01DF00D/Collabfiltrator

Service	Skill Level	Owner	Description	Link
			output over DNS via Burp Collaborator.	
O365Spray	Advanced	Securework s	This tool is a username enumeration and password spraying tool aimed at Microsoft Office 365.	https://github.com/0xZDH/o365spray
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	https://github.com/delvelabs/tachyon

Service	Skill Level	Owner	Description	Link
			command line and targeted at a specific domain. Tachyon uses an internal database to construct these blind queries swiftly.	
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	https://github.com/delvelabs/batea

Service	Skill Level	Owner	Description	Link
			learning for pentesting and network reconnaissance. It consumes map reports and uses a context-driven network device ranking framework based on the anomaly detection 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	https://github.com/bridgecrewio/checkov

Service	Skill Level	Owner	Description	Link
			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).	
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	https://unit42.paloaltonetworks.com/atoms/ ;

Service	Skill Level	Owner	Description	Link
			filtered by targeted sector, region, or malware used for ease of information sharing and deployment of recommended security mitigations.	
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
CodeSec	Basic	Contrast Security	It can serve as a static analysis tool for Java and .Net. The offering can test and protect 3rd party open-source code moving through supply chain with continuous monitoring in production. The tool can also find code security, open-source security and permission issues.	Developer Central | Contrast Security
Cascade (MITRE ATT&CK)	Basic	MITRE	Built on MITRE-ATT&CK Framework: The prototype CASCADE server has the ability to	GitHub - mitre/cascade-server: CASCADE Server

Service	Skill Level	Owner	Description	Link
			handle user authentication, run analytics, and perform investigations. The server runs analytics against data stored in Splunk/Elastic Search to generate alerts. Alerts trigger a recursive investigative process where several ensuing queries gather related events.	
Atomic Red Team	Basic	Red Canary	A library of tests mapped to the MITRE ATT&CK framework. Security teams can use Atomic Red Team to quickly, portably, and	GitHub - redcanaryco/atomic-red-team: Small and highly portable detection tests based on MITRE's ATT&CK.

Service	Skill Level	Owner	Description	Link
			reproducibly test their environments.	
Red Team Automation (RTA)	Basic	Endgame	A framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, leveraged the MITRE ATT&CK framework.	GitHub - endgameinc/RTA
Suricata	Advanced	Open Information Security Foundation (OISF)	Suricata is an open-source network analysis and threat detection software utilized to protect users assets. Suricata uses deep packet inspection to perform	Home - Suricata

Service	Skill Level	Owner	Description	Link
			signature-based detection, full network protocol, and flow record logging, file identification and extraction, and full packet capture on network traffic.	
WiFi Network Security	Advanced	Aircrack-ing	This offering includes a suite of tools to assess WiFi network security including: monitoring, attacking, testing, and cracking. All tools are command line, which allows for heavy scripting. The	www.aircrack-ng.org

Service	Skill Level	Owner	Description	Link
			service must be downloaded from browser.	
Zed Attack Proxy (ZAP)	Advanced	OWASP	This integrated penetration testing tool is used for finding vulnerabilities in web applications. It is designed for users with a wide range of security experience.	OWASP ZAP (zaproxy.org)
Network Mapper	Basic	NMAP	This offering is a utility for network discovery and security auditing. Nmap uses raw IP packets to determine what hosts are available on the network, what services (application	Nmap: the Network Mapper - Free Security Scanner

Service	Skill Level	Owner	Description	Link
			name and version) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters/firewalls are in use.	
Cyber Readiness Check (CRCs)	Basic	Project Spectrum	A system that requires organizations to make an account to access the free service. This tool helps organizations determine current level of security.	Project Spectrum
Perception Point	Basic	Perception Point	Perception Point's Free Email Security Plan, protects organizations from any threat	Free Email Security Plan - Perception Point (perception-point.io)

Service	Skill Level	Owner	Description	Link
			entering organization via email and other collaboration channels. The plug-n-play deployment does not require a change to existing infrastructure. Once implemented, users can see, within minutes, how Perception Point's free advanced email security catches threats.	
Semperis Purple Knight	Basic	Semperis	Purple Knight queries an organization's Active Directory environment and performs a	Purple Knight | Evaluate the security of your Active Directory. (purple-knight.com)

Service	Skill Level	Owner	Description	Link
			comprehensive set of tests against the most common and effective attack vectors to uncover risky configurations and security vulnerabilities. Users receive prioritized, corrective guidance including mapping of indicators of exposure to the MITRE ATT&CK framework to close gaps before they get exploited by attackers.	
Microsoft Defender Antivirus	Basic	Microsoft	This tool protects and detects endpoint threats, including file-	https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows

Service	Skill Level	Owner	Description	Link
			based and fileless malware. Built into Windows 10 and 11 and in versions of Windows Server.	
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 made by identified threats.	https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
Windows Malicious Software Removal tool	Basic	Microsoft	This tool is released by Microsoft on a monthly cadence as part of Windows	https://support.microsoft.com/en-us/topic/remove-specific-prevalent-malware-with-windows-malicious-software-removal-tool-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0

Service	Skill Level	Owner	Description	Link
			Update or as a standalone tool. It can be used to find and remove specific prevalent threats and reverse the changes they have made.	
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	https://safebrowsing.google.com

Service	Skill Level	Owner	Description	Link
			notify users and website owners of potential harm. It is integrated into many major products and provides tools to webmasters.	
Coalition Control Scanning	Basic	Coalition Control	Coalition Control is your account home and includes free attack surface scanning and ongoing monitoring of your organization from the outside in. When vulnerabilities are identified, the tool will show where they are and how to fix	Coalition Control (coalitioninc.com)

Service	Skill Level	Owner	Description	Link
			them. Upgraded scanning requires users to be a Coalition insturance policyholder.	
Security Onion	Basic	Open Source	Security Onion is a free and open Linux distribution for threat hunting, enterprise security monitoring, and log management. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise. Security Onion includes	Security Onion Solutions

Service	Skill Level	Owner	Description	Link
			Elasticsearch, Logstash, Kibana, Suricata, Zeek (formerly known as Bro), Wazuh, Stenographer, CyberChef, NetworkMiner, and many other security tools.	
Syft	Advanced	Anchore	The first is Syft, a CLI tool and Go library for generating a Software Bill of Materials (SBOM) from container images and filesystems. It also supports CycloneDX/SPDX and JSON format. Syft can be installed and run directly on the developer machine to	https://github.com/anchore/syft

Service	Skill Level	Owner	Description	Link
			generate SBOM's against software being developed locally or can be pointed at a filesystem.	
Grype	Advanced	Anchore	Grype which is an open source vulnerability scanner for container images and filesystems that can be used to find zero day vulnerabilities such as log4j.	https://github.com/anchore/grype
Hedgehog	Advanced	Malcolm	Hedgehog Linux is a Debian-based operating system built to monitor network interfaces, capture packets to	https://github.com/idaholab/Malcolm

Service	Skill Level	Owner	Description	Link
			PCAP files, detect file transfers in network traffic and extract and scan those files for threat, and generate and forward to Zeek logs.	
Malcolm	Advanced	CISA	Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files) and Zeek logs.	https://github.com/cisagov/Malcolm
ICS Network Protocol Parsers	Advanced	CISA	The industrial control systems network protocol parsers (ICSNPP) project, only compatible	https://github.com/cisagov/ICSNPP

Service	Skill Level	Owner	Description	Link
			with Zeek, is an ongoing effort to provide open-source tools to enable asset owners, operators, and OT security teams to achieve greater operational network and process level visibility.	
Lumu Free	Advanced	Lumu Technologies	Lumu Free offers continuous monitoring across the network by leveraging multiple sources of metadata (DNS, proxy, firewall). Organizations can uncover contact with malicious	Lumu

Service	Skill Level	Owner	Description	Link
			infrastructure, enabling threat mitigation and attack prevention. Malicious incidents can be labeled to ensure prioritization according to an organization's risk tolerance.	
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	https://splunkbase.splunk.com/app/4740/#/overview

Service	Skill Level	Owner	Description	Link
			data filtering and parsing.	
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" indicators of compromise; other artifacts are so-called "dual-use"	https://github.com/mandiant/Mandiant-Azure-AD-Investigator

Service	Skill Level	Owner	Description	Link
			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	https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

Service	Skill Level	Owner	Description	Link
			may be scripted in any programming language using the HTTP-based public API.	
Netfilter	Advanced	Open Source	Netfilter is a packet filter implemented in the standard Linux kernel. The user space iptables tool is 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	https://www.netfilter.org/

Service	Skill Level	Owner	Description	Link
			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	https://www.wireshark.org/

Service	Skill Level	Owner	Description	Link
			features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds 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	http://ettercap.sourceforge.net/

Service	Skill Level	Owner	Description	Link
			protocols (including ciphered protocols) and includes many features for network and host analysis.	
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	https://www.kismetwireless.net/

Service	Skill Level	Owner	Description	Link
			network IP blocks by sniffing TCP, UDP, ARP, and DHCP packets, log traffic in Wireshark/tcp dump 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	https://www.snort.org/

Service	Skill Level	Owner	Description	Link
			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 Security Engine (BASE) is a web interface for analyzing Snort alerts.	

Service	Skill Level	Owner	Description	Link
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	https://www.activecountermeasures.com/free-tools/rita/

Service	Skill Level	Owner	Description	Link
			Analytics (R-I-T-A) is an open-source framework for detecting command and control communication through network 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	https://github.com/secureworks/dalton

Service	Skill Level	Owner	Description	Link
			bespoke rules. Dalton covers Snort/Suricata /Zeek analysis in one system.	
Elastic SIEM	Advanced	Elastic	Tool is an application that provides security teams with visibility, threat hunting, automated detection, and Security Operations Center (SOC) workflows. Elastic SIEM is included in the default distribution of the most successful logging platform, Elastic (ELK) Stack software. It ships with out-of-the-box detection	Elastic SIEM: free and open for security analysts everywhere | Elastic Blog

Service	Skill Level	Owner	Description	Link
			rules aligned with the MITRE ATT&CK framework to surface threats often missed by other tools. Created, maintained, and kept up-to-date by the security experts at Elastic, these rules automatically detect and address the latest threat activity. Severity and risk scores associated with signals generated by the detection rules enable analysts to rapidly triage issues and	

Service	Skill Level	Owner	Description	Link
			turn their attention to the highest-risk work.	

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

Service	Skill Level	Owner	Description	Link
Caldera (MITRE ATT&CK)	Basic	MITRE	Built on MITRE-ATT&CK Framework: A cyber security platform designed to easily automate adversary emulation, assist manual red-teams, and automate incident response.	GitHub - mitre/caldera: Automated Adversary Emulation Platform
OpenSSH Suite	Basic	Open BSD Project	This connectivity tool is used for remote login with the SSH protocol. It encrypts all traffic to eliminate eavesdropping,	OpenSSH

Service	Skill Level	Owner	Description	Link
			connection hijacking, and other attacks. OpenSSH also provides suite of secure tunneling capabilities, several authentication methods, and configuration options.	
Metasploit Framework	Basic	Rapid7	This computer security project provides information about security vulnerabilities and aids in penetration testing and IDS signature development.	Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit
GRR Rapid Response	Basic	Google	GRR Rapid Response is an incident response framework focused on remote live forensics. The goal of GRR is to	https://grr-doc.readthedocs.io

Service	Skill Level	Owner	Description	Link
			support forensics and investigations in a fast, scalable manner to allow analysts to quickly triage attacks and perform analysis remotely.	
PacketBasics	Basic	ExtraHop	Designed to integrate with AWS environments, this PCAP tool is a subset of the Reveal(x) NDR platform. PacketsBasics might help some organizations develop a more comprehensive approach to tackling M-21-31 and EO-14028 modernization requirements.	Introducing ExtraHop Packet Basics
Microsoft PsExec	Advanced	Microsoft	PsExec is a lightweight telnet replacement that lets users execute	https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

Service	Skill Level	Owner	Description	Link
			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	https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

Service	Skill Level	Owner	Description	Link
			setting up an environment to analyze malware.	
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
dfTimewolf	Advanced	Google	dfTimewolf is an open-source framework for orchestrating forensic collection, processing, and data export.	https://dftimewolf.readthedocs.io

Service	Skill Level	Owner	Description	Link
Turbinia	Advanced	Google	Turbinia is an open-source framework for deploying, managing, and running distributed forensic workloads.	https://turbinia.readthedocs.io
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/
Velociraptor	Advanced	Rapid7	Velociraptor allows incident response teams to rapidly collect and examine artifacts from across a network, and deliver forensic detail following a security incident.	GitHub - Velocidex/velociraptor: Digging Deeper....

Service	Skill Level	Owner	Description	Link
			In the event of an incident, an investigator controls the Velociraptor agents to hunt for malicious activity, run targeted collections, perform file analysis, or pull large data samples. The Velociraptor Query Language (VQL) allows investigators to develop custom hunts to meet specific investigation needs with the ability to adapti queries quickly in response to shifting threats and new information gained through the investigation.	

Maximize the Organization's Resilience to a Destructive Cyber Incident

Service	Skill Level	Owner	Description	Link
Metta	Basic	Uber-Common	Leverages the MITRE-ATT&CK Framework: An information security preparedness tool. This project uses Redis/Celery, Python, and vagrant with VirtualBox to do adversarial simulation.	GitHub - uber-common/metta: An information security preparedness tool to do adversarial simulation.
Sandbox Scryer	Basic	Hybrid-Analysis	Leverages the MITRE-ATT&CK Framework: An open-source tool for producing threat hunting and intelligence data from public	GitHub - PayloadSecurity/Sandbox_Scryer

Service	Skill Level	Owner	Description	Link
			sandbox detonation output. The tool can organize and prioritize findings, assisting in assembling IOCs, understanding attack movement and hunting threats.	
Forest Druid	Basic	Semperis	An attack path discovery tool that helps cybersecurity defensive teams prioritize high-risk misconfigurations that could represent opportunities for attackers to gain	Forest Druid - Focus on your Tier 0 perimeter (purple-knight.com)

Service	Skill Level	Owner	Description	Link
			privileged domain access.	
John the Ripper Password Cracker	Basic	OpenWall	This offering is a password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types, including for: user passwords of Unix flavors, macOS, Windows, groupware, and database servers; network traffic captures; encrypted private keys,	John the Ripper password cracker (openwall.com)

Service	Skill Level	Owner	Description	Link
			filesystems and disks, archives, and document files.	
Trusona 2-Step Verification with TOTP	Basic	Trusona	This free mobile app can be used with any 3rd party service that offers 2-step verification with a 6-digit TOTP code. App users will need to input its their username and password for the 3rd party service they would like to access.	Trusona 2-Step Verification with TOTP | Trusona Docs
Microsoft Security Compliance Toolkit 1.0	Basic	Microsoft	This toolset allows enterprise security administrators to download,	Download Microsoft Security Compliance Toolkit 1.0 from Official Microsoft Download Center

Service	Skill Level	Owner	Description	Link
			analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.	
Authentication Tool	Advanced	Trusona	A passwordless authentication for WordPress admins that enhances security & usability.	Trusona for WordPress – WordPress plugin | WordPress.org
HYPR Zero	Advanced	HYPR True Passwordless(™) MFA platform	HYPR Zero is designed for smaller organizations and delivers	True Passwordless MFA for Small Business Pricing | HYPR

Service	Skill Level	Owner	Description	Link
			passwordless multi-factor authentication.	
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	https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Service	Skill Level	Owner	Description	Link
			notation for visualizing system components, data flows, and security boundaries.	
Microsoft SecCon Framework	Advanced	Microsoft	This framework is designed to help prioritize endpoint hardening recommendations.	https://github.com/microsoft/SecCon-Framework

- Educational Institutions
- Federal Government
- Individuals and Families
- Industry

Alkhudari @ grcico