Overview of Tools Used by Security Operation Center (SOC)

By Mohammed AlSubayt

SIEM Tools

1. Splunk

Splunk is a popular SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

2. LogRhythm

LogRhythm is a cloud-based SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

3. IBM QRadar

IBM QRadar is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

4. McAfee Enterprise Security Manager

McAfee Enterprise Security Manager is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

5. Carbon Black

Carbon Black is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

6. CrowdStrike Falcon

CrowdStrike Falcon is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

7. Darktrace

Darktrace is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

8. Tanium

Tanium is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

9. ThreatConnect

ThreatConnect is a SIEM tool that provides real-time monitoring and analysis of security events. It offers advanced search capabilities, customizable dashboards, and integrations with other security tools.

10. NetWitness

NetWitness is a comprehensive platform that accelerates threat detection and response. It collects and analyzes data across all capture points (logs, packets, netflow, endpoint and IoT) and computing platforms (physical, virtual and cloud), enriching data with threat intelligence and business context.

Websites for Checking IP Reputation

Here are five websites you can use to check the reputation of an IP address:

- **VirusTotal:** Offers a comprehensive analysis of suspicious files and URLs, including IP address reputation.

  Website: https://www.virustotal.com/gui/

- **AbuseIPDB:** Allows you to report and check the reputation of IP addresses based on user reports.

  Website: https://www.abuseipdb.com/

- **IPVoid:** Provides various tools, including an IP reputation checker, DNS lookup, and more.

  Website: https://www.ipvoid.com/

- **Talos Intelligence:** Offers IP and domain reputation lookup services, powered by Cisco.

  Website: https://www.talosintelligence.com/reputation_center

- **AlienVault Open Threat Exchange (OTX):** Allows users to share and receive threat intelligence data, including IP reputation.

  Website: https://otx.alienvault.com/

Phishing email & Malware Analysis Platforms & Tools

Malware analysis platforms and tools are essential for security operation centers to prevent cyber attacks. These tools help identify and analyze malware, allowing security professionals to take action before an attack can occur. Here are the top 10 malware analysis platforms and tools:

1. VirusTotal

VirusTotal is a well-known and widely-used malware analysis platform. It allows users to upload suspicious files or URLs and scans them with multiple **over 70 antivirus scanners**, and URL/domain blocklisting services.

2. DOCGuard

DOCGuard can precisely detect the malware in seconds and extract the false positive free IoCs and may also identify obfuscation and encryption in the form of string encoding and document encryption.

3. Hybrid Analysis

Hybrid Analysis combines **static and dynamic analysis** techniques to provide a holistic view of malware. It enables users to submit files and URLs for analysis and executes them in a controlled virtual environment to observe their behavior. The platform offers **detailed reports,** including network traffic, system changes, and process activity.

4. Cuckoo Sandbox

Cuckoo Sandbox is an **open-source platform** that focuses on behavioral analysis. It allows analysts to submit suspicious files or URLs and executes them in an isolated environment to monitor their behavior. Cuckoo Sandbox generates detailed reports, including network activities, file modifications, and system calls.

5. Any.Run

Any.Run is a powerful **interactive** malware analysis platform. It allows users to run suspicious files and observe their **real-time behavior** via web browser. The platform provides **a sandbox environment** where analysts can interact with malware samples and analyze their activities step-by-step.

6. Joe Sandbox

Joe Sandbox is a comprehensive malware analysis platform that caters to **static and dynamic analysis** techniques. It offers a range of analysis options, including file and URL submissions, and provides **detailed reports** on behavioral activities, network connections, and system changes.

7. Viper Framework

Viper Framework is a **binary analysis and management** platform. It incorporates various analysis techniques under its different modules. Viper Framework offers a user-friendly web interface to upload and analyze files and the ability to create and export analysis profiles.

8. Trend Micro

Trend Micro is a commercial malware analysis platform that provides real-time protection against malware and other cyber threats.

9. Tria.ge

Triage, also known as the Triage Sandbox, is an advanced **malware sandboxing solution** initially created by Hatching. It provides users with the ability to execute malware samples within a secure and isolated environment, enabling the analysis of their actions and evaluation of their potential risks.

10. FileScan

FileScan.IO is an advanced **sandboxing solution** and a free malware analysis service. What sets it apart is its unique adaptive **threat analysis technology,** enabling **zero-day malware detection** and extracting a greater number of **IoCs**. Importantly, FileScan.IO offers these capabilities to users without any cost.

Hash Reputation Check

Hash reputation checks are commonly used in cybersecurity to identify known malicious files based on their hash values. Here are ten platforms and services that provide hash reputation checks:

1. **VirusTotal:**
   - Website: https://www.virustotal.com/gui/
   - Description: Offers a comprehensive analysis of files and URLs by scanning them with multiple antivirus engines and other security tools, including reputation checks based on file hashes.
2. **MetaDefender Cloud:**
   - Website: https://metadefender.opswat.com/
   - Description: Provides a multi-scanning service that checks files against multiple antivirus engines and threat intelligence sources, including hash reputation checks.
3. **Hybrid Analysis by Payload Security:**
   - Website: https://www.hybrid-analysis.com/
   - Description: Offers dynamic malware analysis and threat intelligence services, including hash reputation checks for known malicious files.
4. **Any.Run:**
   - Website: https://any.run/
   - Description: Provides interactive malware analysis and sandboxing services, including hash reputation checks and behavioral analysis of suspicious files.
5. **Jotti's Malware Scan:**
   - Website: https://virusscan.jotti.org/
   - Description: Allows users to upload files for scanning with multiple antivirus engines and checks file hashes against known malicious samples.
6. **ThreatCrowd:**
   - Website: https://www.threatcrowd.org/
   - Description: Aggregates threat intelligence data from various sources and allows users to search for file hashes to determine their reputation.
7. **MalShare:**
   - Website: https://malshare.com/
   - Description: A repository of malware samples and threat intelligence data, including file hashes and metadata for reputation checks and analysis.
8. **HashCheck:**
   - Website: https://www.hashcheck.net/
   - Description: A community-driven platform for sharing and checking file hashes, including known malicious hashes identified by security researchers and organizations.
9. **Joe Sandbox:**
   - Website: https://www.joesecurity.org/
   - Description: Provides advanced malware analysis and threat intelligence services, including hash reputation checks and sandbox-based analysis of suspicious files.
10. **ThreatConnect:**
    - Website: https://www.threatconnect.com/
    - Description: Offers a threat intelligence platform that integrates with various security tools and provides hash reputation checks as part of its threat intelligence feeds and analysis capabilities.

Monitoring URL Reputation

URL reputation monitoring is the process of tracking and analyzing the reputation of a website or domain. It involves checking the website's history, including its past performance, user reviews, and security measures. By monitoring URL reputation, businesses can identify potential cyber threats and take proactive measures to prevent them.

1. **VirusTotal:**
   - Website: https://www.virustotal.com/gui/
   - Description: Provides a comprehensive analysis of URLs by scanning them with multiple antivirus engines, domain information, and other security tools.
2. **URL Scan :**
   - Website: https://urlscan.io/
   - Description: checks URLs against its constantly updated lists of unsafe web resources, including phishing sites and malware-infected pages.
3. **URLVoid:**
   - Website: https://www.urlvoid.com/
   - Description: Offers a URL reputation checker that scans URLs against multiple blacklisting services to detect potentially harmful websites.
4. **Norton Safe Web:**
   - Website: https://safeweb.norton.com/
   - Description: Norton's service that analyzes URLs for potential security risks, including malware, phishing, and scams, and provides safety ratings.
5. **Web of Trust (WOT):**
   - Website: https://www.mywot.com/
   - Description: Community-driven website reputation service where users rate and review websites based on their experiences with trustworthiness, vendor reliability, privacy, and child safety.

Endpoint Protection Tools

1. McAfee Endpoint Protection

McAfee Endpoint Protection is a comprehensive solution that provides real-time protection against malware, viruses, and other cyber threats. It also includes features such as data loss prevention, encryption, and device management.

2. Symantec Endpoint Protection

Symantec Endpoint Protection is a powerful endpoint security solution that provides protection against a wide range of threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

3. Trend Micro Endpoint Protection

Trend Micro Endpoint Protection is a comprehensive solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

4. Bitdefender Endpoint Protection

Bitdefender Endpoint Protection is a powerful solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

5. Kaspersky Endpoint Protection

Kaspersky Endpoint Protection is a comprehensive solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

6. ESET Endpoint Protection

ESET Endpoint Protection is a powerful solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

7. Sophos Endpoint Protection

Sophos Endpoint Protection is a comprehensive solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

8. Webroot Endpoint Protection

Webroot Endpoint Protection is a powerful solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

9. Carbon Black Endpoint Protection

Carbon Black Endpoint Protection is a comprehensive solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

10. Cisco Endpoint Security

Cisco Endpoint Security is a powerful solution that provides real-time protection against cyber threats, including malware, viruses, and ransomware. It also includes features such as device management, encryption, and data loss prevention.

Vulnerability Scanning Tools

Nessus

Nessus is a vulnerability scanner that provides comprehensive vulnerability assessment and penetration testing.

OpenVAS

OpenVAS is an open-source vulnerability scanner that provides a wide range of scanning options and reporting capabilities.

Metasploit

Metasploit is a penetration testing framework that includes a vulnerability scanner and exploitation tools.

Qualys

Qualys is a cloud-based vulnerability scanner that provides real-time vulnerability assessment and compliance reporting.

Tenable.io

Tenable.io is a cloud-based vulnerability management platform that includes a vulnerability scanner and risk management tools.

Rapid7

Rapid7 is a vulnerability management platform that includes a vulnerability scanner and threat intelligence tools.

VulnDB

VulnDB is a vulnerability database that provides detailed information on vulnerabilities and their associated exploits.

Nmap

Nmap is a network exploration and security auditing tool that includes a vulnerability scanner and port scanner.

Acunetix

Acunetix is a web application security scanner that includes a vulnerability scanner and penetration testing tools.

Threat Intelligence Tools

1. Splunk

Splunk is a popular threat intelligence tool that provides real-time visibility into security events and incidents. It offers advanced analytics and machine learning capabilities to help security teams detect and respond to threats more effectively.

2. ThreatConnect

ThreatConnect is a cloud-based threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

3. Cisco Talos

Cisco Talos is a threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

4. CrowdStrike

CrowdStrike is a cloud-based endpoint security platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

5. Mandiant

Mandiant is a threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

6. Carbon Black

Carbon Black is a cloud-based endpoint security platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

7. FireEye

FireEye is a threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

8. Darktrace

Darktrace is a threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

9. LogRhythm

LogRhythm is a threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

10. ThreatQuotient

ThreatQuotient is a threat intelligence platform that provides real-time threat intelligence and incident response capabilities. It offers a wide range of features, including threat intelligence feeds, threat hunting, and incident response automation.

Network Traffic Analysis Tools

1. Wireshark

Wireshark is a popular network protocol analyzer that allows users to capture and analyze network traffic. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

2. Tcpdump

Tcpdump is a command-line tool that allows users to capture and analyze network traffic. It is commonly used for network troubleshooting and security auditing.

3. Snort

Snort is an open-source intrusion detection system that can be used to monitor network traffic for security threats. It supports a wide range of protocols and can be customized to meet specific security needs.

4. Netscap

Netscap is a network traffic analysis tool that allows users to monitor and analyze network traffic in real-time. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

5. Cisco Network Assistant

Cisco Network Assistant is a network management tool that allows users to monitor and analyze network traffic. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

6. SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor is a network traffic analysis tool that allows users to monitor and analyze network traffic in real-time. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

7. ManageEngine Network Monitor

ManageEngine Network Monitor is a network traffic analysis tool that allows users to monitor and analyze network traffic in real-time. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

8. GlassWire

GlassWire is a network traffic analysis tool that allows users to monitor and analyze network traffic in real-time. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

9. Pcap Sharp

Pcap Sharp is a network traffic analysis tool that allows users to capture and analyze network traffic. It supports a wide range of protocols and can be used to troubleshoot network issues, monitor network performance, and detect security threats.

10. Tcpdump-ng

Tcpdump-ng is a command-line tool that allows users to capture and analyze network traffic. It is commonly used for network troubleshooting and security auditing.

Exploit Tools

Metasploit

Used for penetration testing and exploitation of vulnerabilities.

BeEF

Used for browser exploitation and post-exploitation activities.

Immunity

Used for testing and training security professionals on exploitation techniques.

Burp Suite

Used for web application security testing and exploitation.

Nmap

Used for network exploration and vulnerability scanning.

John the Ripper

Used for password cracking and brute-force attacks.