HOW TO BUILD A SECURITY STACK

The security stack often defines a means to visualize the complexity of cybersecurity problems and find effective solutions for them. The stacks are layers that deliver services and exchange information to achieve a better level of service. The notion of a security stack serves the idea that security is integrated as a service. These enable relevant technologies and professional security services that implement these factors into association.

Security Tools by Category:

PRIORITY	TOOL CATEGORY	SOFTWARE NAME
High	Endpoint	Atera
Medium		ESET Endpoint Security
Medium		Trend Micro Apex One
High		CrowdStrike Falcon Insight
Low		Malwarebytes Endpoint Protection
High	Network	Wireshark
High		Icinga
Medium		Prometheus
Low		Nagios
High	Cloud security	Bitglass: Total Cloud Security
High		Cisco Systems Cloudlock
Medium		SpectralOps
Medium		Security code scan
Medium		Allot

High	IOT Security	Tempered
High		Rapid7
Low		Rack911 Labs
High	IDS/ IPS	Cisco NGIPS
Medium		Corelight and Zeek
Medium		Fidelis Network
High		FireEye Intrusion Prevention System

RISK ASSESSMENT AND JUSTIFICATION ;

Each tool is associated with certain risks and the justifications are being addressed as follows -

- **Atera -**

  This is a high risk based end point analysis tool. This tool is One comprehensive RMM solution built for IT professionals and offers IT automation.

- **ESET Endpoint Security -**

  This is a high risk based end point analysis tool. This tool offers functionalities such as File Server Security, Full Disk Encryption, Advanced Threat Defense, Cloud App Protection Mail Security and Detection and Response.

- **Trend Micro Apex One -**

  This is a medium risk based end point analysis tool. This tool uses Pre-execution and They also implement effective protection against scripts, injections, ransomware, memory, and browser attacks through innovative behavior analysis.

- **CrowdStrike Falcon Insight -**

  This is a high risk based end point analysis tool. These offer case studies, community tools and other features at the resource center. It also helps to gain full spectrum visibility

in real time.

- **Malwarebytes Endpoint Protection -**

  This is a medium-risk based end point analysis tool. Although the risk associated with the tool is medium, It offers precision detection at the point of attack. It also provides real-time protection from malware, ransomware, zero-day exploits, phishing and other threats.

- **Wireshark -**

  Wireshark is a high-risk-based network security tool. It helps to analyze traffic in the organization’s network and helps to understand the protocols and ports of the connection.

- **Icinga -**

  This is a high-risk-based network security tool. The six key strengths of the Icinga stack encompass every facet of monitoring. Gain ground with insightful analysis, prompt notifications, eye-opening visualizations, and analytics.

- **Prometheus -**

  Prometheus is a medium-risk-based network security tool. It is 100% open source. It has Multiple functionalities in determining and visualizing the data for network security and It also uses precise alerting based on Prometheus' flexible PromQL.

- **Nagios -**

  This is a low risk based network security tool. Your log data search can be made much simpler with Nagios Log Server. Create alerts to inform you when potential threats appear, or use log data queries to quickly audit any system.

- **Bitglass: Total Cloud Security -**

  This is a high-risk-based cloud security tool. This offers SmartEdge Secure Web Gateway and Zero Trust Network Access. Malware may be automatically stopped across the cloud, the web, and the network thanks to the integration of Bitglass and CrowdStrike during upload, download, and while the device is at rest.

- **Cisco Systems Cloudlock -**

  This is a low risk based cloud security tool. Your cloud users, data, and apps are all protected. The straightforward, open, and automated method of Cloudlock employs APIs to control the risks in your ecosystem of cloud apps. Cloudlock makes it easier to combat data breaches and adhere to regulatory standards.

- **SpectralOps -**

  This is a medium risk based cloud security tool. The services offered by spectral include monitoring, categorizing, and safeguarding your infrastructure, assets, and code for exposed API keys, tokens, credentials, and high-risk security configuration errors.

- **Security code scan -**

  This is a low risk based cloud security tool. SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other vulnerability analysis patterns are among the types it detects.

- **Allot -**

  This is a low risk based IOT security tool. It offers features such as behavior profiling and anomaly detection, behavior assurance, and threat protection.

- **Tempered -**

  This is a medium risk based IOT security tool. This uses airwall, a technology consisting

of cloaking, secure remote access, and edge to cloud.

- **Rapid7 -**

  This is a high risk based IOT security tool. They perform IoT penetration testing, hardware testing, and also use threat modeling for securing devices and enterprises.

- **Rack911 Labs -**

  This is a medium risk based IoT security tool. They provide a comprehensive range of security services, including secure managed hosting and penetration testing.

- Cisco NGIPS **-**

  This is a high risk based anti malware tool. They use Snort 3.0. They are adaptable, have minimal operating costs, and can be enhanced for high-performance applications.

- Corelight and Zeek **-**

  This is a medium risk based anti malware tool. Threats can be discovered with this technique before they result in a breach or compromise. inquiry and correction of speed attacks, Stop ransomware, exfiltration, or C2 assaults before they have an impact. Utilize metadata for inventory and discovery

- Fidelis Network **-**

  This is a medium risk based anti malware tool.All of the assets in your on-premises and cloud networks may be identified and categorized using the tool. Using carefully curated threat knowledge from Fidelis Insight, determine risk in real time. high-level visual examination of your cyber risk and in-depth examination of asset classification and status

- FireEye Intrusion Prevention System**-**

  This is a high risk based anti malware tool. The tool Utilize ML/AI and Correlation Engines for Retroactive Detection, Identify Attacks that Evade Traditional Defenses,

Detect Suspicious Lateral Movements, Block Attacks Inline in Real Time.

FIREWALLS -

Firewalls defend against online attackers. The machine and network are protected from unwanted and malicious network traffic by them. Additionally, the firewalls would stop harmful software from connecting to the computer or network via the internet.

- **Tufin SecureTrack -**

  SecureTrack enables you to create automated audit reports that are compatible with HIPAA, SOX, PCI-DSS, GDPR, and other regulations.

- **ManageEngine Firewall Analyzer -**

  The following functions are available with ManageEngine Firewall Analyzer: complete authority over your firewall's ruleset. Check your firewall network for irregularities. Learn how to optimize the performance of your firewall network by rearranging the rules.

- **FireMon -**

  A whole range of security management tools are available from FireMon, including FireMon Automation, Security Officer, and Controller of Global Policy. Planner of policies, Strategy Optimizer, Risk assessor.

- **Cisco Firepower Management Center -**

  As a network management solution, Cisco Firepower Management Center gives you the capabilities for centralized network monitoring, enables you to have a thorough understanding of all network components, and makes it very simple to identify and stop threats.

The signals from the intrusion detection systems are frequently received by a blue team (IDS). All of the network-connected devices in this situation—which are referred to as endpoints—are monitored using various toolkits. Endpoint security systems frequently focus on detection and alerting important employees in the company to start incident response and mitigation procedures. It is possible to create specific alert centers with the necessary tools to start the processes in order to centralize the alerts and the responses. Calculations have been made for all important tests pertaining to the organization's growth. The dangers are quantified using these. The operations to be conducted are taken into account by making greater use of the available tools and technologies. The following tasks are issued in a test setting that is designed to capitalize on monotonous work. These are labeled, and the pertinent test efficiencies are found by looking through them.

There are different security automation tools, such as -

- Robotic Process Automation (RPA)
- Security Orchestration, Automation and Response (SOAR)
- XDR

REFERENCES :

https://geekflare.com/edr-tools/

https://spectralops.io/blog/top-12-cloud-security-tools/

https://startupstash.com/iot-security-tools/

https://www.softwaretestinghelp.com/best-malware-removal/

https://www.networkstraining.com/best-firewall-management-software-tools/