

Cybersecurity Open Source Tools

U.S. Embassy Suva

Political/Economic Section



Overview

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

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

Pillars of Cybersecurity: What We're Trying to Accomplish



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



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



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



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



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

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

Least Privilege

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

Defense in Depth

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

Management and Monitoring

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

Cybersecurity Fundamentals: Good Cyber Hygiene

1. Risk Identification

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

2. Vulnerability Reduction

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

3. Threat Reduction

4. Consequence Mitigation

5. Enable Cybersecurity Outcomes



Where to Start (Cyber Hygiene)