HIVE SENTINEL:

The Hackers Confine

Presented By:

Qaseem Ul Hassan

Mariyam

Presented To:

Dr. Nabeel Ahmed

Overview

- Introduction
- Project Objectives
- Architectural View
- Project Sequence
- Infrastructure
- Tools
- Gantt Chart

Problem Statement

High-interaction honeypots replicate live environments to lure threats, but lack of health monitoring poses risks: false security, inaccurate data, and vulnerabilities. Robust monitoring is crucial, ensuring accurate threat detection and informed decisions, safeguarding assets, and enhancing resilience against cyber threats.

Honeypots

A "honey pot" is a decoy system or network designed to attract hackers, diverting them from actual targets. It helps gather information about their methods and motives for improved cybersecurity.

Types of Honeypots

a) Low Interaction Honeypot

b) Medium Interaction Honeypot

c) High Interaction Honeypot

Low Interaction Honeypots

1. Emulates limited services, reducing exposure to attacks.
2. Provides basic insights into attacker methods with minimal risk.
3. Easy to deploy and maintain but lacks extensive interaction realism.

Examples:

Dionaea

Kippo

Honeyd

Medium Interaction Honeypots

1. Simulates multiple services for deeper attacker engagement.
2. Gathers more detailed insights into attacker tactics.
3. Balances interaction realism with moderate security risks.

Examples:

- Cowrie
- Honeypy
- Medusa

High Interaction Honeypots

1. Fully replicates real systems, offering the most authentic interaction.
2. Provides comprehensive insights into attacker behaviour and techniques.
3. Involves higher security risks due to exposure of genuine components.

Examples:

- Capture-HPC
- Sebek
- Cuckoo Sandbox

Hacker Deception

Hacker Deception is the strategic use of misleading information, fake systems, or traps to misdirect and confuse **hackers** attempting unauthorized access to computer networks. It aims to lure hackers into controlled environments (such as honeypots) to detect, monitor, and analyze their activities, ultimately enhancing cybersecurity defenses by learning from potential threats.

Deception 1.0

Deception 1.0: Key Challenges

1. Low vs. High Interaction
2. Emulation Complexity
3. Deployment Scaling
4. Honeypot Identifiability
5. Administration Challenges
6. Compromise Risks
7. Limited Deception Scope
8. Limited Threat Analysis

Deception 2.0

Deception 2.0: Functionality and Key Points

1. Diverse Interactivity
2. Realistic, Non-Emulated Deceptions
3. Scalability and Efficiency
4. Automated Setup and Maintenance
5. Advanced Risk Mitigation
6. Comprehensive Resource Deception
7. Integration with Security Ecosystem
8. Enhanced Threat Analysis
9. Holistic Deception Strategy

Feature Difference

Feature	Deception 1.0	Deception 2.0
Interactivity	Low and high interaction	Diverse interactivity
Emulations	Emulations for realistic service mimicry, fingerprinting risk	Realistic, non-emulated deceptions, dynamic deceptions
Scalability	Scaling challenges for large networks, Gartner's 10:1 ratio	Scalability through innovative techniques
Automation	Manual setup and maintenance, administration challenges	Automated setup and maintenance, DevOps model
Risk Mitigation	Risk of compromise with compromised honeypots	Advanced risk mitigation strategies
Deception Scope	Limited to honeypots, standalone products, limited interaction with other security components	Comprehensive deception across various enterprise resources
Integration	Honeypots as standalone products, limited interaction with security infrastructure	Integration with security ecosystem
Threat Analysis	Primarily malware capture, limited threat analysis	Enhanced threat analysis and engagement

Control Managemnt in Honeypots

Control management of honeypots involves overseeing their setup, monitoring their activities, and analyzing gathered data to enhance cybersecurity.

Project Objectives

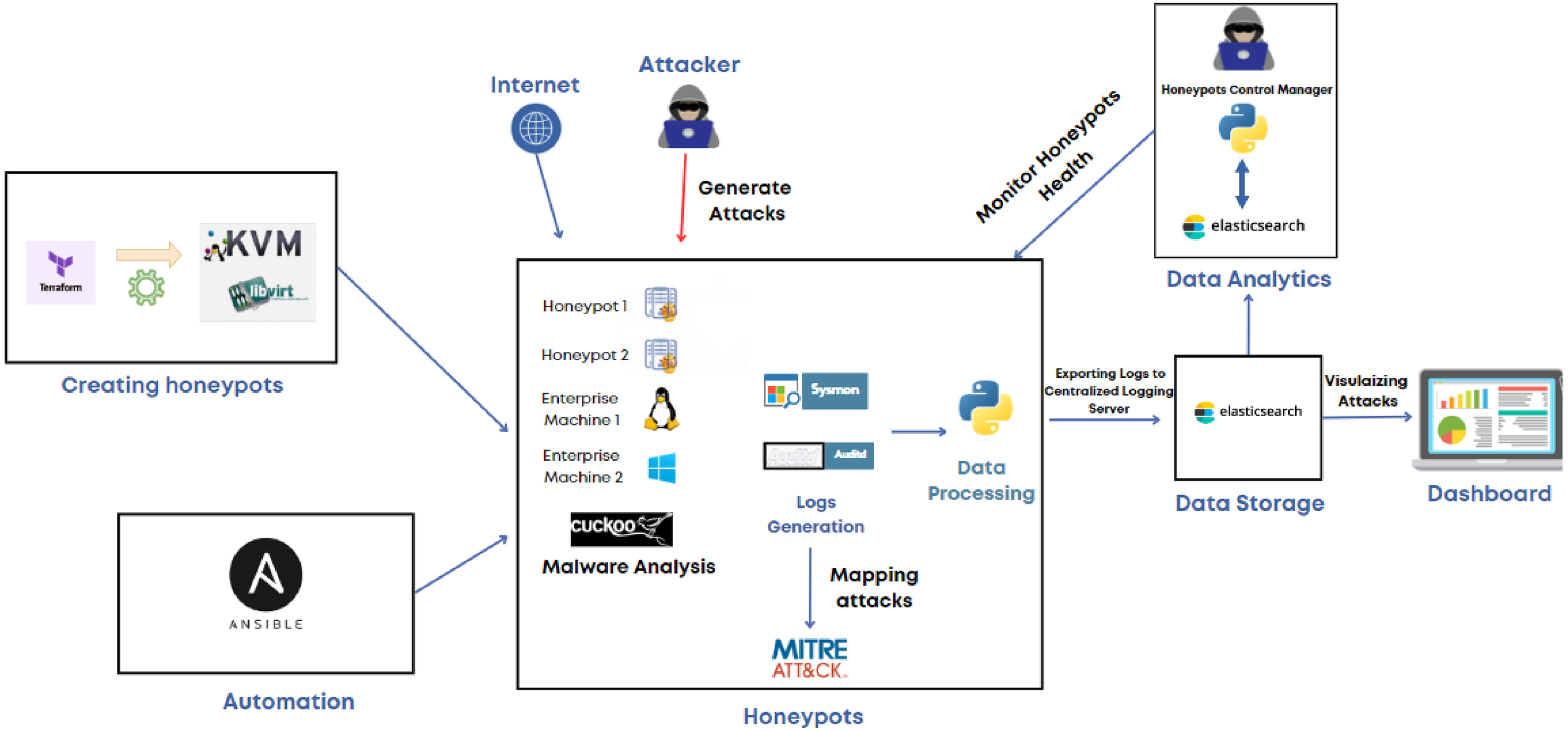
a) Streamlined Setup

b) Centralized Monitoring

c) Threat Intelligence Gathering

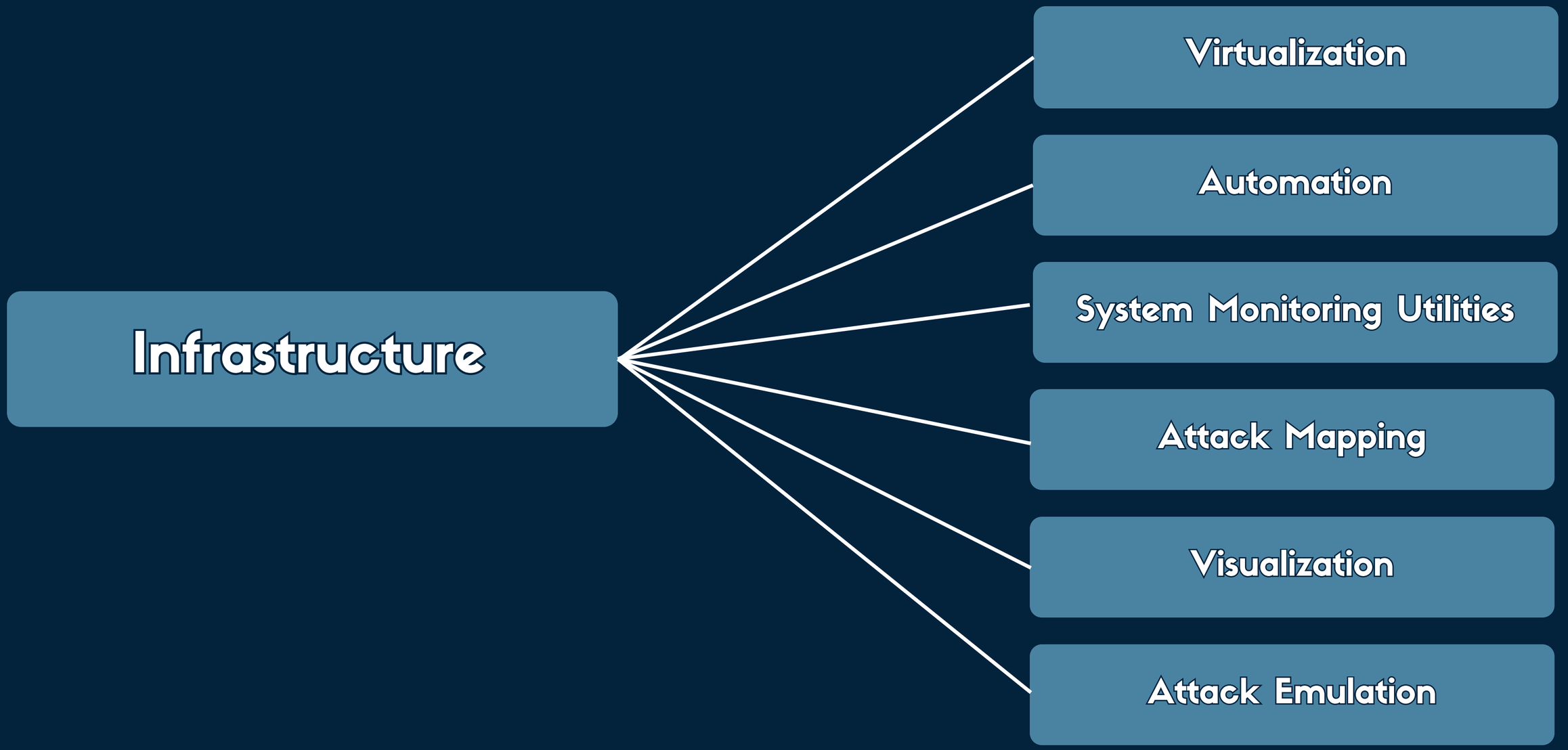
d) Incident Response Enhancement

Architectural View



Project Sequence

1. Deploy Honey Pots: Set up security traps with Terraform.
2. Manage Services: Deploy and oversee services using Ansible.
3. Sysmon Installation: Install Sysmon for advanced system monitoring.
4. Normalize Logs: Standardize log formats for consistency.
5. Centralized Log Export: Send logs to a central server for streamlined analysis.
6. Identify Threat Levels: Assess data to gauge security threats.
7. MITRE Mapping: Relate incidents to MITRE ATT&CK framework.
8. Honey Pot Health Dashboard: Monitor honey pot status through a dashboard.
9. Visualize Attacks: Create intuitive attack pattern visualizations.
10. Attack Emulation: Simulate attacks to validate response systems.


Infrastructure
Virtualization
Automation
System Monitoring Utilities
Attack Mapping
Visualization
Attack Emulation

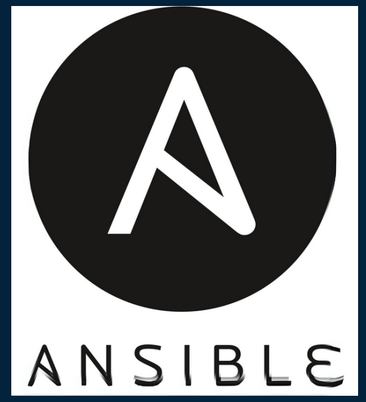
Virtualization

It is a virtualization technology that allows the creation and management of virtual machines (VMs) on a host system.

Deployment

Terraform is an open-source infrastructure as code tool that enables efficient creation, modification, and versioning of virtualized environments and cloud resources, facilitating seamless management and automation of IT infrastructure.

Automation



Ansible is an open-source automation tool that simplifies IT tasks by allowing users to automate software installation, configuration, and management across multiple servers using a simple, human-readable language (YAML).
It operates agentlessly and is widely used for efficient IT orchestration and configuration management.

Sandboxing

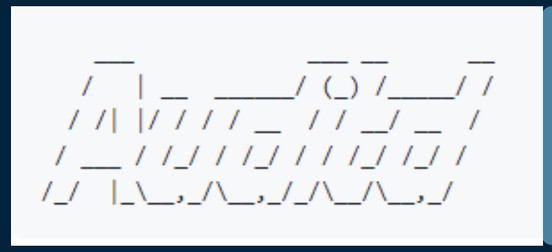
Cuckoo Sandbox is open-source tool for automated analysis of suspicious files and URLs in a secure, virtualized environment, aiding malware detection and research.

System Monitoring Utilities

Sysmon

System Monitor is a Windows system service and device driver that provides advanced monitoring and logging of system activity.

System Monitoring Utilities



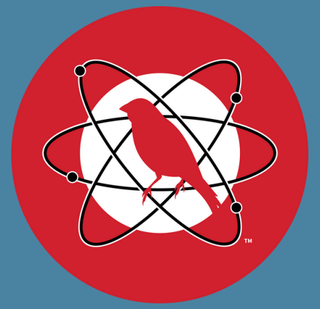
Auditd

auditd is a Linux system daemon that provides auditing and logging capabilities for monitoring system activities and security events.

Attack Mapping

MITRE ATT&CK is a framework that provides a comprehensive and structured way to understand the tactics, techniques, and procedures (TTPs) that adversaries use during cyberattacks.

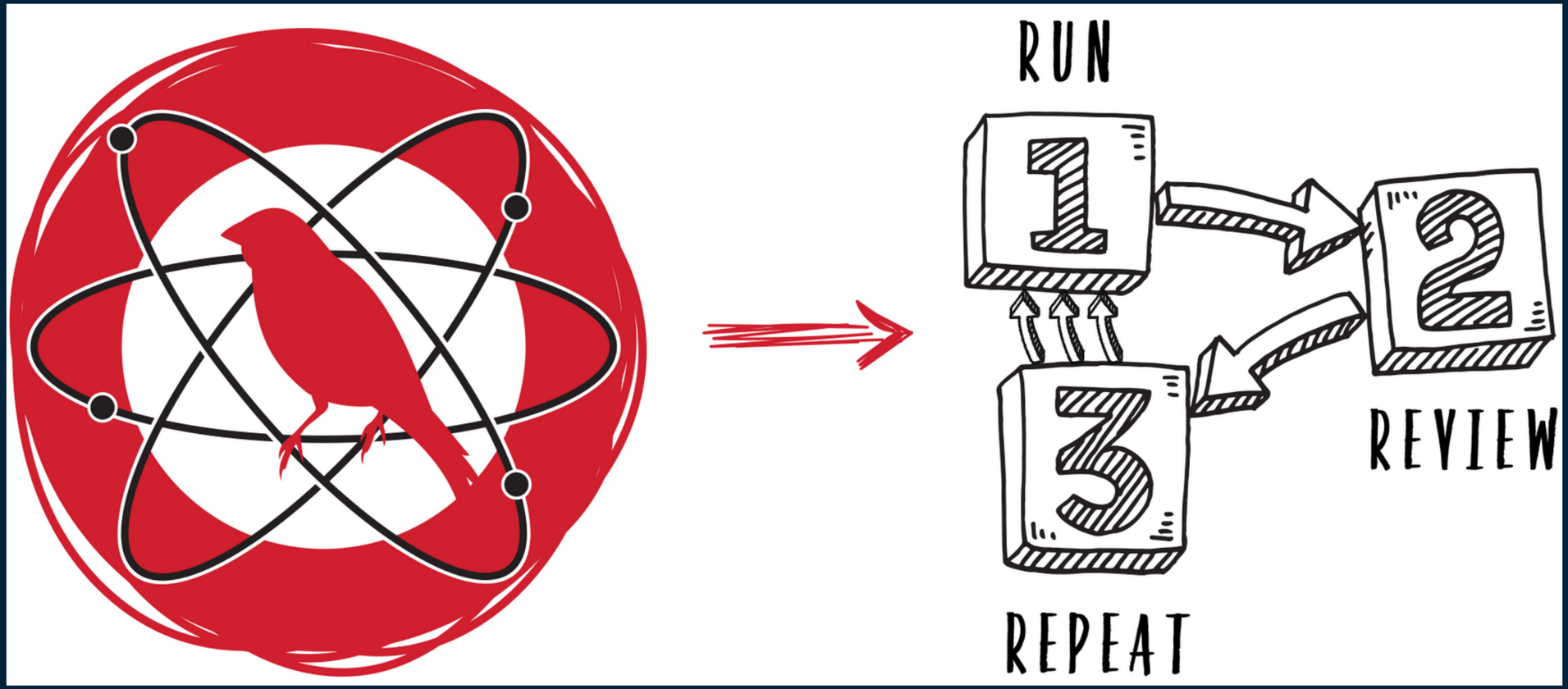
Attack Emulation



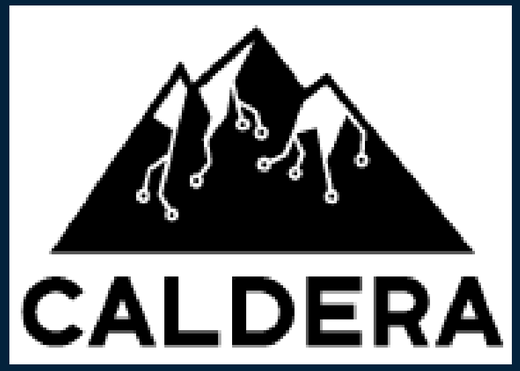
Atomic Red Team

Atomic Red Team provides a library of test cases that mimic real-world attack techniques and behaviors, allowing organizations to assess the strength of their defenses and detection capabilities.

Attack Emulation



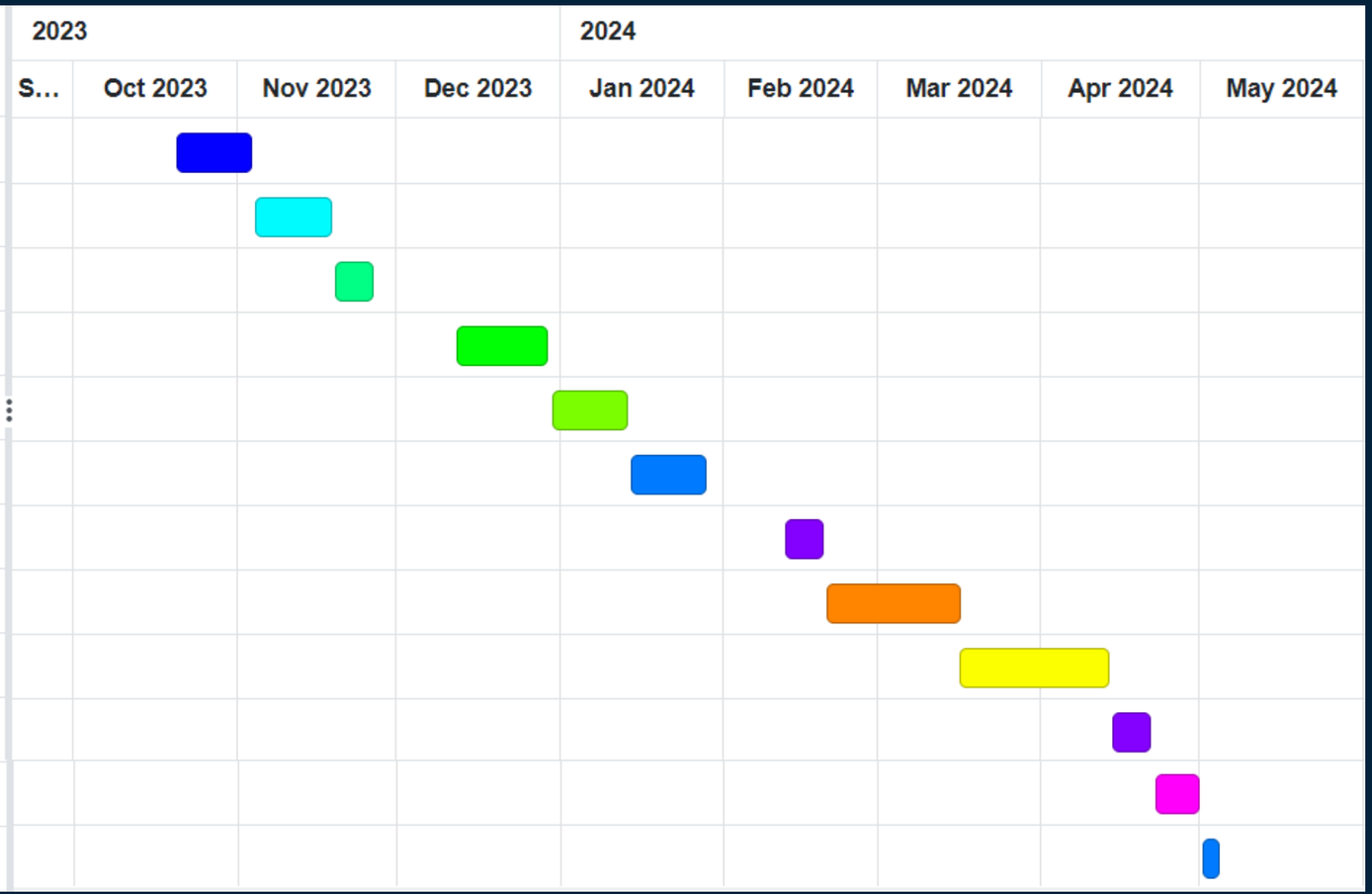
Attack Emulation



Caldera is an open-source platform designed for conducting automated adversary emulation and cyber threat simulation.

Gantt Chart

ID	Name	Start Date	End Date	Duration
1	Deploy Honeypots	Oct 20, 2023	Nov 03, 2023	15 days
2	Deploy Services	Nov 04, 2023	Nov 18, 2023	15 days
3	Install and configure Sysmon	Nov 19, 2023	Nov 26, 2023	8 days
4	Logs Normalization	Dec 12, 2023	Dec 29, 2023	18 days
5	Logs export	Dec 30, 2023	Jan 13, 2024	15 days
6	Identify threat level	Jan 14, 2024	Jan 28, 2024	15 days
7	Mapping on MITRE ATT&CK	Feb 12, 2024	Feb 19, 2024	8 days
8	Health monitoring dashboard	Feb 20, 2024	Mar 16, 2024	26 days
9	Attacks visualization dashboard	Mar 16, 2024	Apr 13, 2024	29 days
10	Attack Emulation	Apr 14, 2024	Apr 21, 2024	8 days
11	Testing of project	Apr 22, 2024	Apr 30, 2024	9 days
12	Deployment of project	May 01, 2024	May 04, 2024	4 days



Questions & Comments