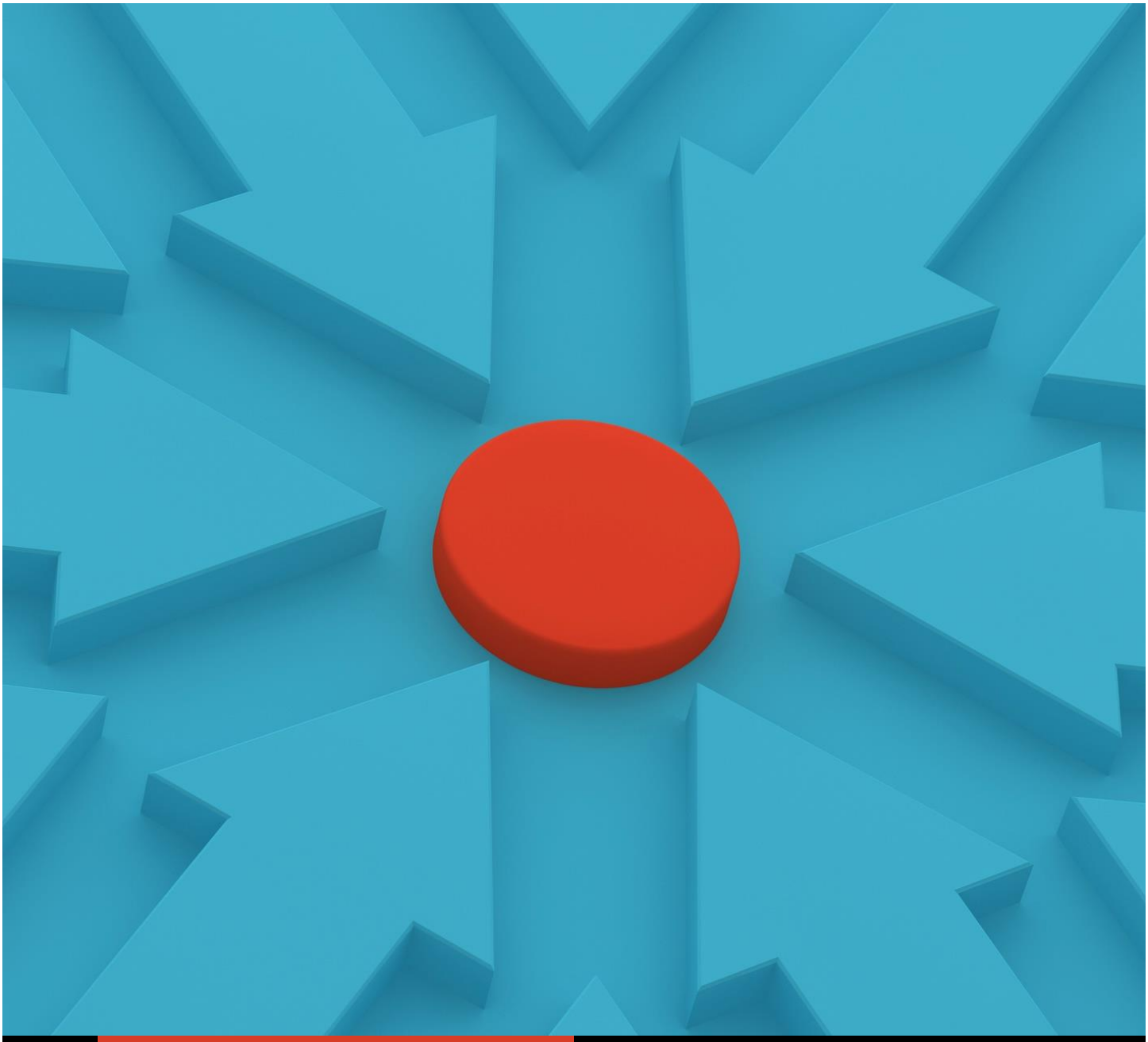

INTERNAL HONEYPOT RECCOMENDATION

ACME COMPANY

ROAD RUNENR CORPERATION soc@roadrunner.com

OVERVIEW

Executive Summary

In today's cybersecurity landscape, proactive measures are essential for early detection of malicious activities. Honeypots are decoy systems designed to lure attackers, allowing organizations to monitor and analyze attack patterns without risking actual assets. The Modern Honey Network (MHN) simplifies the deployment and management of honeypots, making it easier for security teams to gather intelligence on threats. This report recommends deploying a honeypot solution using the Modern Honey Network (MHN) to manage Cowrie, Dionaea and Glastopf honeypots. This approach will enhance our ability to detect and deflect a wide range of potential attacks, providing valuable insights into attacker behavior and tactics.

Solution Overview

The recommended solution involves deploying honeypot systems managed through the Modern Honey Network. This platform will be used to manage and monitor the following honeypots:

Cowrie Honeypot: A medium to high-interaction SSH and Telnet honeypot.

- It is used to simulate a fully functional shell to catch and log unauthorized login attempts.

Dionaea Honeypot: A low-interaction honeypot that emulates a variety of services and protocols such as SMB, FTP, HTTP, MSSQL, and more.

- Dionaea is designed to catch malware in the wild by mimicking vulnerable services.

Glastopf Honeypot: A low-interaction web application honeypot designed to emulate vulnerabilities and capture web-based attacks.

- It is focused on mimicking web vulnerabilities to attract and log attackers.

With Cowrie, Dionaea, and Glastopf in place, we will be able to detect and deflect a wide range of attack vectors in both our network and web applications. These honeypots provide early detection of malicious actors by simulating weak points in the network infrastructure that attackers might target. When an attack is detected, the MHN platform logs and analyzes the behavior, allowing our analysts to act quickly to mitigate any potential threat. The data collected from these honeypots will help us:

Identify Attack Patterns: Understand the tactics, techniques, and procedures (TTPs) used by attackers.

Enhance Incident Response: Improve our incident response capabilities by providing actionable intelligence.

Strengthen Security Posture: Use insights from honeypot data to bolster defenses and patch vulnerabilities in existing systems.

IMPLEMENTATION PLAN

Preparation and Requirements

Before deploying the Modern Honey Network and the associated honeypots, ensure that the following prerequisites are met:

Hardware Requirements

MHN Server: A dedicated server with at least 8 GB of RAM and 256 GB of disk space running Ubuntu 18.04, Ubuntu 16.04, or CentOS 6.9.

Honeypot Deployment Systems: Virtual machines or physical servers for running Cowrie, Dionaea, and Glastopf.

Software Requirements

Operating System: Ubuntu 20.04 LTS or later for the MHN server and honeypots.

Database: MongoDB is used by MHN to store logs and attack data. It is essential for the functionality of MHN, as it allows for efficient data management and retrieval.

- While the installation script for MHN may handle the setup of MongoDB, you should verify that it is installed and running properly after the MHN installation.

Web Server: Nginx or Apache serves as the web server for the MHN web interface, allowing users to access the dashboard and manage honeypots through a browser

- Similar to MongoDB, the installation script for MHN typically includes the setup of Nginx or Apache.
- After installation, you should check that the web server is running to ensure access to the MHN interface.

Analyst Tools:

Web Browser: For accessing the MHN web interface.

SIEM Integration: Tools like Splunk, ArcSight, or any existing log management tools.

Network Monitoring Tools: Existing tools for monitoring baseline network traffic.

COST ESTIMATE

Hardware Cost:

MHN Server: Approximately $20 to $50 per month for a cloud-based VPS (e.g., AWS, Digital Ocean).

Honeypot Deployment Systems: If utilizing existing infrastructure, this cost may be negligible. If additional servers are needed, costs will vary based on specifications.

Software Costs:

MHN: Free (Open Source).

Cowrie, Dionaea, and Glastopf: Free (Open Source)

Analyst Training: Estimated at $500 to $1,000 for training sessions on using MHN, Cowrie, Dionaea, and Glastopf, as well as analyzing logs if applicable.

Maintenance and Support: Consider budgeting for ongoing maintenance, updates, and potential support costs.

Utilizing Existing Tools: To maximize the effectiveness of the MHN deployment, we can leverage existing tools already in place in our environment:

Monitoring Solutions: Free (Snort)

- Utilize existing network monitoring tools to establish a baseline of normal traffic patterns and identify anomalies detected by the honeypots.

SIEM Integration: Free (Splunk & ArcSight)

- If a SIEM tool is already implemented, it can easily integrate with MHN logs into this system for enhanced analysis and correlation with other security events.

Total Estimated Cost: Approximately $1,000 to $1,500 for initial setup and training, with ongoing server costs of $20 to $50 monthly, depending on existing infrastructure.