CYBERSECURITY MAJOR PROJECT

Attack, Detect & Secure the Environment: A Red Team vs Blue Team Simulation

Documenter
Tirath Chandravanshi

Documenter
Shivam Kishor

Attacker
Suraj Madharia

Attacker
Parmeshwar Sao

Defender
Yesh Nirmalkar

Defender
Amit Kumar

Guided by: **Anshul Kaundal**

PROJECT ABSTRACT

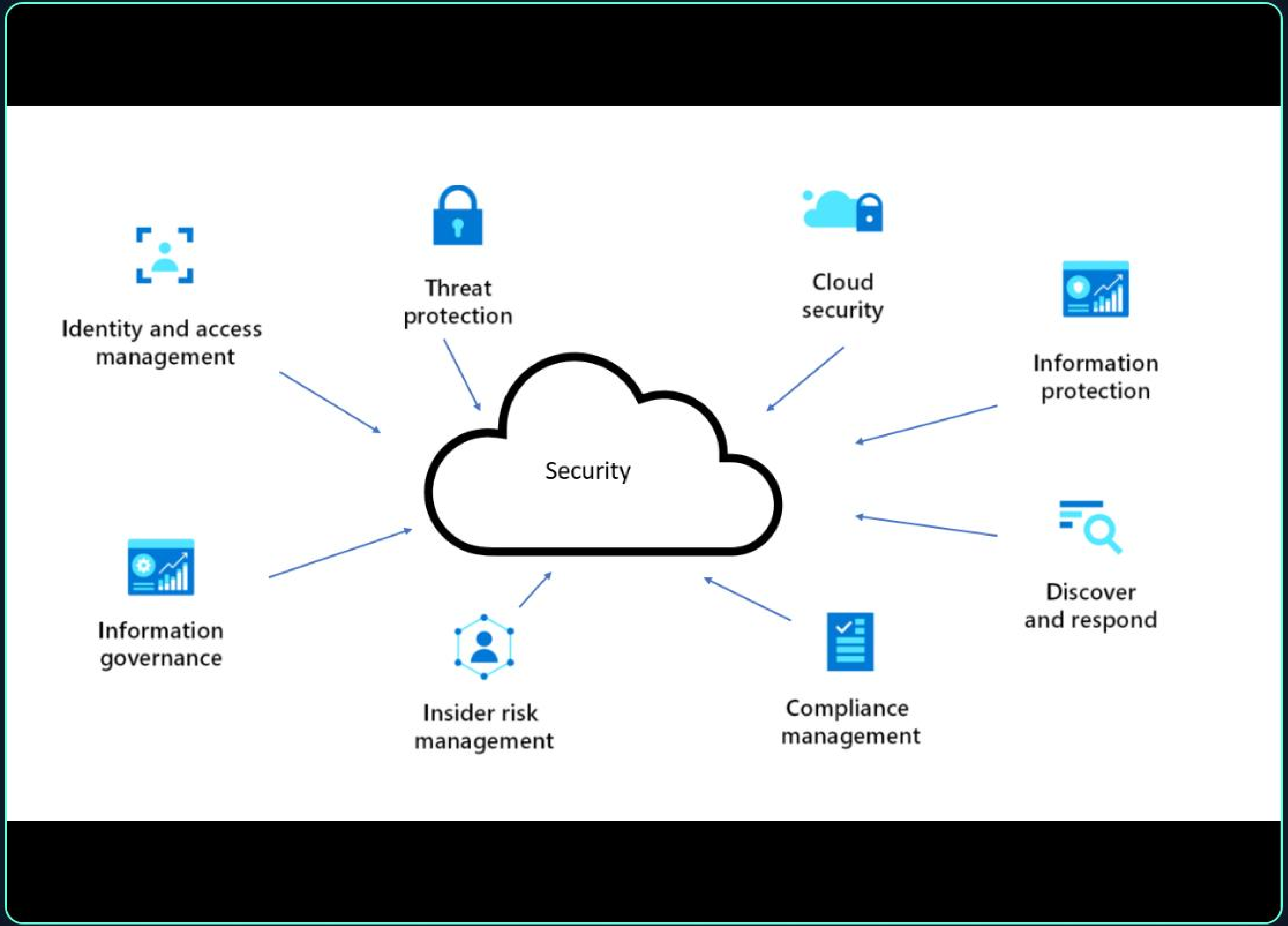
THE SIMULATION

This project involves a comprehensive simulation of cyber-attacks on cloud-based enterprise infrastructure. We simulate the entire kill-chain, from reconnaissance to exploitation.

THE DEFENSE

By acting as both the Red Team and Blue Team, we demonstrate the lifecycle of vulnerability exploitation, SIEM detection via Wazuh, and the application of industry-standard security hardening to validate a robust defensive architecture.

INFRASTRUCTURE INTRODUCTION



AZURE CLOUD ENVIRONMENT

- > **Target Nodes:** VMs hosting Apache/Nginx web servers and FreeIPA for identity management.
- > **Monitoring Core:** Centralized SIEM logs using Wazuh Agent/Server architecture.
- > **Network:** Deployed on Azure with NSGs configured to simulate a vulnerable enterprise network.
- > **Objective:** Provides a realistic sandbox for Red Team attacks and Blue Team monitoring.

THE PROBLEM STATEMENT

VULNERABLE SURFACE

Initial infrastructure lacks essential hardening, leaving SSH ports open to brute force and web services exposed to common injection attacks.

DETECTION GAPS

Without proper logging (Sysmon/Auditd) and SIEM configuration, malicious activities go unnoticed, lacking root cause identification.

THE GOAL

Generate Attacks > Identify Gaps > Fix Vulnerabilities > Validate Security. A complete feedback loop.

PRIMARY OBJECTIVES

1. SIMULATE

Execute real-world attacks (Hydra, SQLi) to generate authentic security events and Indicators of Compromise (IoCs) in the logs.

2. DETECT

Analyze logs using the Wazuh SIEM to identify malicious IPs, patterns, and anomalies associated with the attacks.

3. HARDEN

Apply security controls following industry standards (CIS Benchmarks) and re-validate to ensure the attacks are blocked.

PHASE ONE:
RED TEAM ATTACK

Simulation & IoC Generation

The first phase focuses on offensive operations. We assume the role of an external threat actor to stress-test the environment.

Key Goal: Populate the logs with real attack data (Failed Auth, SQL Errors, File Integrity Changes) to facilitate Blue Team analysis.

ATTACK SCENARIOS & METHODOLOGY

- **Reconnaissance (Nmap & Gobuster)**
  Scanning for open ports and hidden directories to map the attack surface.

- **SSH Brute Force (Hydra)**
  Targeting VM1 & VM2 with dictionary attacks to simulate unauthorized access attempts.

- **Web Exploitation**
  Executing SQL Injection (SQLi) and Directory Traversal attacks on the hosted Apache web servers.

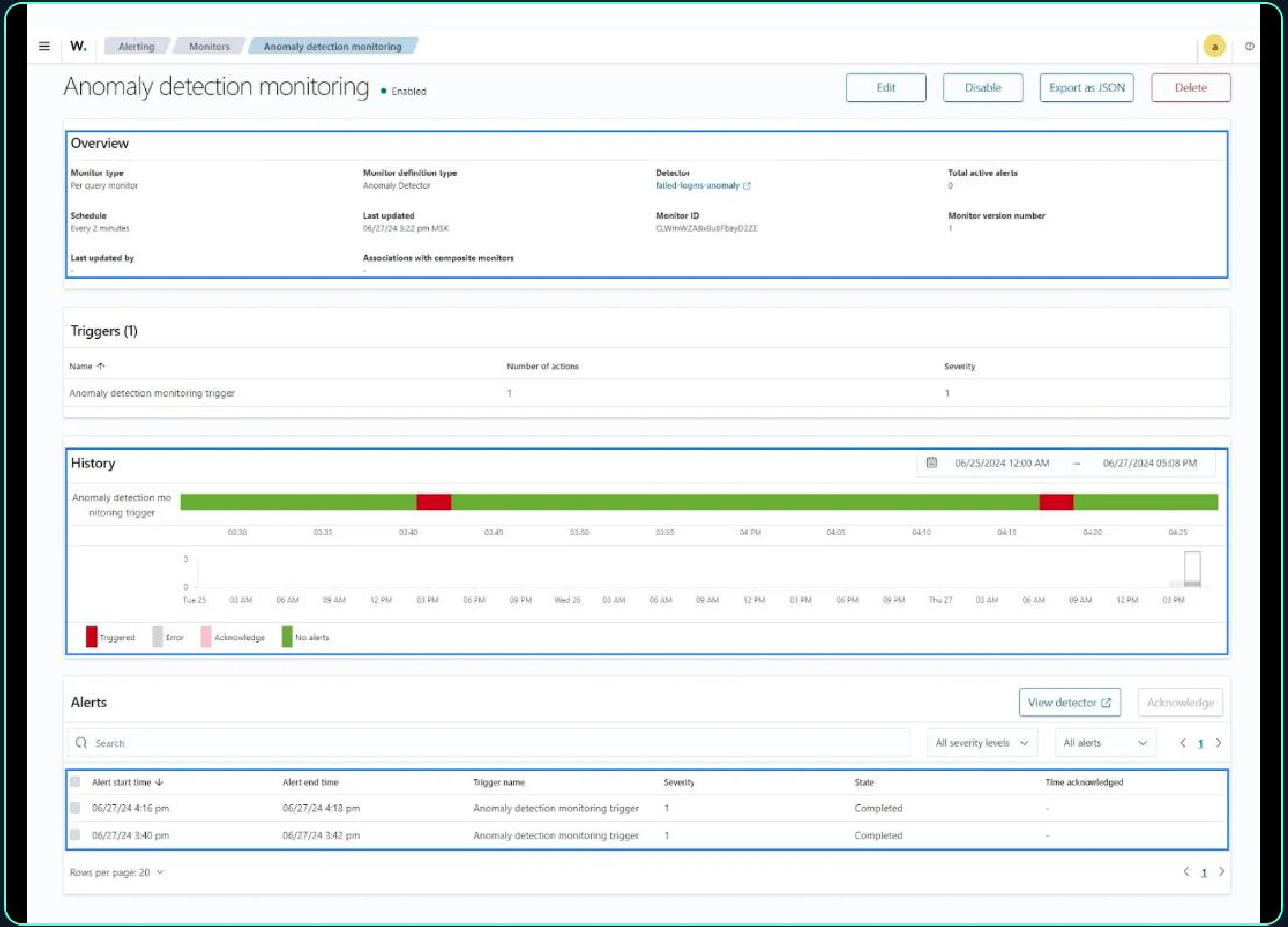
- **Privilege Escalation**
  Attempting to gain root access to demonstrate the impact of weak local security configurations.

BLUE TEAM: INVESTIGATION

POST-ATTACK ANALYSIS

Analysis focuses on identifying the attacker's footprint within the SIEM environment.

- > **Syslog Analysis:** Reviewing `auth.log` for rapid authentication failures (Brute force signatures).
- > **Wazuh Alerts:** Documenting triggered security rules (e.g., "Multiple failed logins", "Web attack detected").
- > **IoC Documentation:** Tracking and blacklisting malicious IPs and detecting unauthorized file changes via FIM.



Anomaly detection monitoring • Enabled

Overview

Monitor type: Per query monitor
Monitor definition type: Anomaly Detector
Detector: failed-logins-anomaly
Total active alerts: 0
Schedule: Every 2 minutes
Last updated: 06/27/24 3:22 pm MSK
Monitor ID: CLWmWZA8x8u8FbayD2ZE
Monitor version number: 1
Last updated by: -
Associations with composite monitors: -

Triggers (1)

Name ↑	Number of actions	Severity
Anomaly detection monitoring trigger	1	1

History

06/25/2024 12:00 AM → 06/27/2024 05:08 PM

Anomaly detection monitoring trigger

🟥 Triggered ▨ Error 🟪 Acknowledge 🟩 No alerts

Alerts

□	Alert start time ↓	Alert end time	Trigger name	Severity	State	Time acknowledged
□	06/27/24 4:16 pm	06/27/24 4:18 pm	Anomaly detection monitoring trigger	1	Completed	-
□	06/27/24 3:40 pm	06/27/24 3:42 pm	Anomaly detection monitoring trigger	1	Completed	-

Rows per page: 20

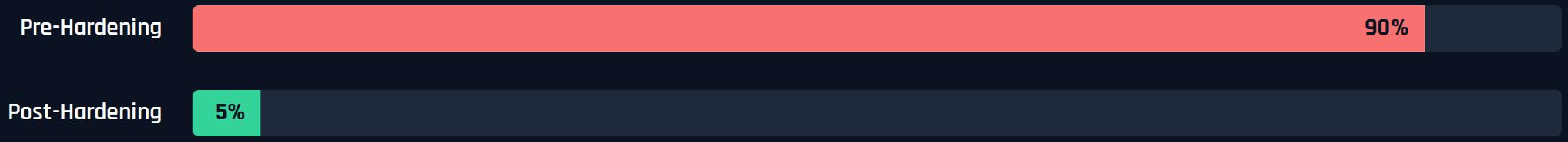
SECURITY HARDENING IMPLEMENTATION

Category	Hardening Measure	Tool / Detail
Logging	System & Audit Monitoring	Sysmon for Linux, Custom Auditd rules for granular tracking.
Network	Firewall & Port Control	UFW/Iptables configuration, Azure NSG Hardening (Whitelisting).
Access	SSH Hardening	Disable Root Login, Key-based auth only, Change Default Port, Fail2Ban.
Services	Web & Directory Security	Harden Apache/Nginx configs (Hide version, disable directory listing), FreeIPA policies.

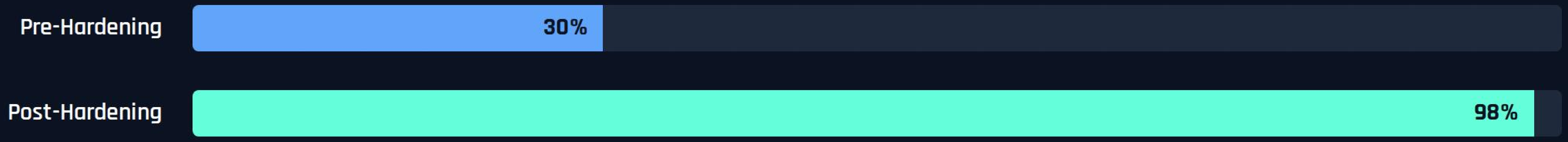
VALIDATION: BEFORE VS AFTER

Validation confirms a significantly reduced attack surface and improved alert fidelity.

ATTACK SUCCESS RATE (LOWER IS BETTER)



THREAT DETECTION RATE (HIGHER IS BETTER)



EXPECTED LEARNING OUTCOMES

RED TEAM SKILLS

Hands-on experience with offensive tools like Hydra, Nikto, and Nmap to understand the attacker's mindset.

SOC OPERATIONS

Developed critical log analysis skills for incident response, alert triage, and proactive threat hunting.

SYSTEM HARDENING

In-depth knowledge of Linux security, defensive architecture, and configuration management.

THANK YOU

Final Security Posture Validated and Documented.

References: Wazuh Documentation | CIS Benchmarks | Azure NSG Best Practices

QUESTIONS?

IMAGE SOURCES

https://learn.microsoft.com/en-us/azure/architecture/guide/security/images/security-overview.png

Source: learn.microsoft.com

https://res.cloudinary.com/teepublic/image/private/s--OpiQveG6--/t_Resized%20Artwork/c_fit,g_north_west,h_954,w_954/co_000000,e_outline:48/co_000000,e_outline:inner_fill:48/co_ffffff,e_outline:48/co_ffffff,e_outline:inner_fill:48/co_bbbbbb,e_outline:3:1000/c_mpad,g_center,h_1260,w_1260/b_rgb:eeeeee/t_watermark_lock/c_limit,f_auto,h_630,q_auto:good:420,w_630/v1621430371/production/designs/21939479_0.jpg

Source: www.teepublic.com

https://wazuh.com/uploads/2024/07/anomaly-detection-monitoring-dashboard.webp

Source: wazuh.com