FINAL SECURITY POSTURE REPORT

1. Introduction

This report presents the **final security posture** of the cloud-based enterprise environment after completing **Red Team attack simulations**, **Blue Team investigations**, and **comprehensive system hardening**.

The objective was to evaluate the system’s resilience **before and after security controls**, using real attack data and SIEM-based analysis.

2. Initial Security Posture (Before Hardening)

Before applying security controls, the environment exhibited multiple **high-risk weaknesses**, making it vulnerable to common cyberattacks.

Key Observations:

- SSH password authentication enabled
- No rate limiting on authentication services
- Open inbound access from the internet
- Verbose web server error responses
- Limited audit and monitoring rules
- Weak network segmentation between DMZ and Internal subnet

Impact:

- Successful brute force attempts were possible
- Web enumeration generated high-severity alerts
- Privilege escalation activities were logged
- Attack surface was broad and easily exploitable

3. Threat Detection Capability (Before Hardening)

Using **Wazuh SIEM**, the following attack patterns were detected:

Attack Type	**Detection Evidence**
SSH brute force	PAM authentication failures
Web enumeration	HTTP 400/404 bursts
Privilege escalation	Successful sudo events
Automated scanning	Repeated malformed requests

These detections confirmed **real-world attacker behavior**, validating the effectiveness of SIEM visibility even before hardening.

---

4. Security Controls Implemented

After investigation, **layered security hardening** was applied across all systems.

4.1 System Hardening

- Disabled root SSH login
- Enforced key-based authentication
- Limited authentication retries
- Enforced least privilege access

4.2 Network Hardening

- UFW firewall enabled
- Default deny inbound policy
- SSH restricted to SIEM VM only
- Rate limiting enabled for SSH

4.3 Application Hardening

- Apache server banner obfuscation
- Reduced verbose error responses

- Hardened web server configuration

4.4 Logging & Monitoring Enhancements

- Auditd enabled with custom rules
- Enhanced authentication logging
- Centralized log forwarding to SIEM
- Improved alert correlation

---

5. Post-Hardening Security Posture (After Hardening)

After implementing hardening measures, the environment showed a **significant reduction in attack success and alert severity**.

Improvements Observed:

- SSH brute force attempts blocked
- Web enumeration generated fewer alerts
- Reduced attack surface
- Faster detection and response
- Clear audit trails for privileged actions

---

6. Before vs After Comparison

Security Aspect	**Before Hardening**	**After Hardening**
SSH Access	Password-based	Key-based only
Firewall	Open	Restricted
Attack Surface	Wide	Minimized
Alert Volume	High	Reduced
Attack Success	Possible	Prevented
Logging Quality	Moderate	High

---

7. SIEM Validation Results

Re-executing the same attacks after hardening resulted in:

- **Lower severity alerts**
- **Blocked connections**
- **Improved correlation**
- **Clear distinction between benign and malicious activity**

This validated the **effectiveness of defensive controls** and SIEM tuning.

---

8. Final Security Assessment

The system transitioned from a **vulnerable, attack-prone state** to a **hardened, monitored, and resilient environment**.

Final Security Status:

- ✔ Secure authentication
- ✔ Controlled network access
- ✔ Strong visibility through SIEM
- ✔ Reduced risk of compromise
- ✔ Improved incident response readiness

---

9. Learning Outcomes

Through this project, the following competencies were achieved:

- Real-world attack simulation
- SOC-level log analysis
- Incident investigation & root cause analysis
- System and network hardening
- Security posture evaluation

10. Conclusion

This project successfully demonstrated how **cyberattacks can be detected, analyzed, and mitigated** using a structured Blue Team approach.

The final hardened environment reflects **industry-standard security practices**, significantly improving resilience against common threats.

Security is not a one-time setup, but a continuous process of detection, response, and improvement.

11. Future Enhancements

- IDS/IPS integration
- Automated response using SOAR
- Threat intelligence feeds
- Advanced correlation rules
- Compliance benchmarking (CIS/NIST)