10ALYTICS CAPSTONE PROJECT - SOC Environment Audit

Document Information

- **Prepared by:** Harriet Obinyan
- **Date:** March 15, 2025

Risk Assessment Report & Security Policy Document

Executive Summary

This audit evaluated Diamond Gems Inc.'s Security Operations Center (SOC) environment, focusing on its ability to detect, prevent, and respond to security threats. The assessment revealed that although the organization implemented an adequate security monitoring process using Wazuh SIEM, some critical vulnerabilities exist within the system's configuration and security controls. Recently, a security incident (CSA-SOC-MAR-2025–001) demonstrated how misconfigured SSH services and inadequate access controls led to an unauthorized system access by brute-force attack. While the incident was successfully contained without a data breach, this audit recommends immediate implementation of stronger access controls, improved system hardening, enhanced monitoring capabilities, and a formalized security policies to prevent future incidents.

1. Introduction

1.1 Audit Purpose

This audit was conducted to evaluate the effectiveness of Diamond Gems Inc.'s Security Operations Center (SOC) environment, including its security monitoring capabilities, incident response procedures, and overall security posture. The audit was initiated following the recent security incident where an unauthorized access was detected and responded to by the SOC team.

1.2 Scope

The audit examined the following systems and processes:

- SOC infrastructure and design
- Security monitoring capabilities and SIEM implementation (Wazuh)
- Network security controls and firewall configuration (PFsense)
- Endpoint security on Windows and Linux systems
- Log management and alert configuration
- Incident response procedures and their effectiveness
- Access control
- Security policy compliance and governance

1.3 Methodology

The audit was conducted using a combination of:

- Document review of the incident report CSA-SOC-MAR-2025–001
- System configuration review
- Log analysis from Wazuh and PFsense
- Evaluation against NIST Cybersecurity Framework and MITRE ATT&CK framework
- Interviews with SOC team members
- Testing of alert mechanisms and notification systems

2. Risk Assessment

2.1 Asset Inventory

Asset ID	Asset Name	Description	Owner	Classification	Location
A001	Wazuh Server	SIEM server for log collection and analysis	SOC Team	Critical	Primary Data Center
A002	PFsense Firewall	Network firewall for traffic filtering	Network Team	Critical	Primary Data Center
A003	Ubuntu Linux Desktop	Endpoint user workstation	End User Department	Medium	Corporate Office
A004	Windows 10 Pro	Endpoint user workstation	End User Department	Medium	Corporate Office
A005	Windows Server 2022	Server providing business services	IT Department	Critical	Primary Data Center
A006	Slack Integration	Alert notification platform	SOC Team	Medium	Cloud Service

2.2 Threat Identification

Threat ID	Threat Description	Potential Impact	Likelihood	Related Assets
T001	Brute Force Attack	High	High	A003, A004, A005
T002	Unauthorized System Access	High	Medium	A003, A004, A005
T003	Misconfigured Services	High	High	A003, A004, A005
T004	Inadequate Monitoring Coverage	Medium	Medium	A001, A006
T005	Delayed Incident Response	High	Medium	A001, A006
T006	Insufficient Log Collection	Medium	Medium	A001, A002

2.3 Vulnerability Assessment

Vuln ID	Vulnerability	Affected Assets	Severity	Ease of Exploitation
V001	Open SSH Service Ports	A003, A004, A005	High	High
V002	Weak Authentication (Password-only)	A003, A004, A005	Critical	High
V003	Inadequate SOC Staffing	A001, A006	Medium	Medium
V004	Firewall Logs Not Integrated with SIEM	A001, A002	Medium	Low
V005	Lack of MFA Implementation	A003, A004, A005	High	Medium
V006	Insufficient System Hardening	A003, A004, A005	High	Medium

2.4 Risk Analysis Matrix

Risk ID	Risk Description	Related Threats	Related Vulnerabilities	Impact	Likelihood	Risk Rating	Existing Controls
R001	Unauthorized access through brute force attack	T001, T002	V001, V002, V005	High	High	Critical	SIEM monitoring, alerts
R002	Delayed detection of security incidents	T004, T005	V003, V004	High	Medium	High	Wazuh SIEM alerts, Slack integration
R003	System compromise due to misconfiguration	T003	V001, V006	High	High	Critical	Network scanning
R004	Insufficient incident response	T005	V003	Medium	Medium	Medium	Incident response procedures
R005	Incomplete log collection and analysis	T006	V004	Medium	Medium	Medium	Wazuh agent deployment

3. Compliance Assessment

3.1 Framework Mapping

This audit uses the NIST Cybersecurity Framework (CSF) and MITRE ATT&CK framework as benchmarks. The NIST CSF provides a comprehensive approach to managing cybersecurity risk, while MITRE ATT&CK provides a knowledge base of adversary tactics and techniques that helps identify specific threat actions.

3.2 Control Assessment

Control ID	Control Description	Framework Reference	Compliance Status	Observations	Evidence Collected
C001	Identity and Access Management	NIST CSF PR.AC	Partially Compliant	Password-only authentication for SSH services. No MFA implemented.	Incident report, system configuration
C002	Protective Technology	NIST CSF PR.PT	Partially Compliant	Firewall implemented but misconfigured services still accessible.	Nmap scan results, PFsense configuration
C003	Security Continuous Monitoring	NIST CSF DE.CM	Partially Compliant	Wazuh SIEM implemented but firewall logs not integrated.	Wazuh dashboard, missing firewall logs
C004	Detection Processes	NIST CSF DE.DP	Compliant	Detection processes in place and successfully identified attack.	Wazuh alerts, Slack notifications
C005	Response Planning	NIST CSF RS.RP	Compliant	Incident response process effectively contained the incident.	Incident report
C006	Vulnerability Management	NIST CSF ID.RA	Non-Compliant	Inadequate vulnerability assessment processes.	Open SSH ports, misconfigurations

3.2.1 Access Control Assessment

The organization implements basic access controls but lacks advanced authentication mechanisms. SSH services are configured to use password authentication rather than more secure methods like public/private key pairs or multi-factor authentication. User access management processes appear to be informal, with insufficient regular access reviews.

3.2.2 Log Management & Retention Assessment

Log collection is implemented through Wazuh agents on endpoints, but the PFsense firewall logs are not properly integrated with the SIEM system. This creates visibility gaps in the security monitoring. Log retention periods and review processes are not formally documented.

3.2.3 Incident Response Protocols Assessment

The incident response process demonstrated effectiveness in containing the recent brute-force attack. The SOC team successfully identified, contained, and eradicated the threat. However, staffing limitations were noted as a factor in delayed response. Formal documentation of incident response procedures was not evident at the time of audit.

3.2.4 Other Control Areas

- **Network Segmentation**: Limited evidence of proper network segmentation which could have contained the unauthorized access.
- **System Hardening**: Inadequate system hardening procedures allowed misconfigured services to remain accessible.
- **Security Awareness**: No evidence of security awareness training for end-users was provided.

4. Findings and Recommendations

4.1 Summary of Findings

Finding ID	Finding Description	Risk Level	Related Controls	Related Risks
F001	SSH services configured with password authentication instead of key-based authentication	Critical	C001	R001
F002	Open SSH ports accessible from untrusted networks	Critical	C002	R001, R003
F003	Firewall logs not integrated with SIEM platform	Medium	C003	R002, R005
F004	Inadequate SOC staffing for 24/7 monitoring	Medium	C003, C004	R002, R004
F005	Lack of formal vulnerability assessment program	High	C006	R003
F006	No multi-factor authentication for critical systems	High	C001	R001
F007	Insufficient system hardening standards	High	C002, C006	R003

4.2 Detailed Recommendations

Rec ID	Recommendation	Related Finding	Priority	Estimated Effort	Responsibility	Timeline
REC 001	Implement SSH key-based authentication for all systems and disable password authentication	F001	High	Medium	IT Security	30 days
REC 002	Configure firewall rules to restrict SSH access to authorized networks only	F002	High	Low	Network Team	14 days
REC 003	Configure agentless monitoring for PFsense firewall logs into Wazuh	F003	Medium	Medium	SOC Team	45 days
REC 004	Increase SOC staffing or implement 24/7 managed detection and response service	F004	Medium	High	Security Management	60 days
REC 005	Establish regular vulnerability scanning program with remediation tracking	F005	High	Medium	IT Security	30 days
REC 006	Implement multi-factor authentication for all administrative access	F006	High	Medium	IT Security	45 days
REC 007	Develop and implement system hardening standards based on CIS benchmarks	F007	High	Medium	IT Security	45 days
REC 008	Implement network segmentation to isolate critical systems	F002	Medium	High	Network Team	60 days
REC 009	Establish formal security policy documentation covering all critical areas	All	High	Medium	Security Management	30 days

5. Security Policy Document

5.1 Purpose and Scope

This security policy establishes the guidelines and requirements for protecting Diamond Gems Inc.'s information assets, including but not limited to systems, networks, applications, and data. This policy applies to all employees, contractors, and third parties who access company systems and information.

5.2 Roles and Responsibilities

- **Chief Information Security Officer (CISO)**: Overall responsibility for security governance and policy enforcement
- **SOC Team**: Responsible for security monitoring, incident detection, and response
- **IT Department**: Responsible for implementing security controls and maintaining systems
- **System Owners**: Responsible for ensuring their systems comply with security policies
- **End Users**: Responsible for complying with security policies and reporting security incidents

5.3 Access Control Policy

5.3.1 User Access Management

- All access must be provided based on the principle of least privilege
- Access requests must be formally documented and approved by management
- Access rights must be reviewed quarterly
- Access must be promptly revoked when no longer required
- Temporary access must have an expiration date

5.3.2 Privilege Management

- Administrative privileges must be strictly controlled and limited
- Administrative accounts must not be used for regular activities
- All privileged access must be logged and monitored
- Privileged account usage must be reviewed weekly

5.3.3 Authentication Requirements

- Multi-factor authentication is required for all administrative access
- SSH access must use key-based authentication, not passwords
- Passwords must meet complexity requirements (12+ characters, mixed case, numbers, symbols)
- Passwords must be changed every 90 days
- Failed login attempts must be limited to 5 before temporary lockout

5.4 Data Protection Policy

- Data must be classified according to sensitivity (Public, Internal, Confidential, Restricted)
- Access to data must be granted based on classification and need-to-know
- Confidential and Restricted data must be encrypted at rest and in transit
- Data retention periods must be defined and enforced
- Data disposal must follow secure procedures

5.5 Log Management Policy

5.5.1 Log Collection Requirements

- All systems must forward logs to the central SIEM platform (Wazuh)
- Logs must include authentication events, privilege changes, system changes, and security events
- Firewall and network devices must be configured for agentless log collection
- Log integrity must be protected against tampering

5.5.2 Log Retention Requirements

- Security event logs must be retained for at least 1 year
- System logs must be retained for at least 90 days
- Authentication logs must be retained for at least 180 days
- Log storage must be sized appropriately to meet retention requirements

5.5.3 Log Review Procedures

- Critical security alerts must be reviewed within 1 hour
- Daily log review must be performed by SOC team
- Weekly log review reports must be provided to security management
- Automated correlation rules must be regularly tuned and updated

5.6 Incident Response Policy

5.6.1 Incident Classification

- Incidents are classified as Low, Medium, High, or Critical based on:
  - Impact to business operations
  - Sensitivity of affected data
  - Scope of the incident
  - Potential for reputational damage

5.6.2 Incident Reporting

- All security incidents must be reported to the SOC team immediately
- Incidents must be documented in the incident management system
- Critical incidents must be escalated to senior management
- Regulatory reporting requirements must be followed where applicable

5.6.3 Incident Response Procedures

1. **Detection and Analysis**: Identify and verify the incident
2. **Containment**: Isolate affected systems to prevent spread
3. **Eradication**: Remove the threat from the environment
4. **Recovery**: Restore systems to normal operations
5. **Post-Incident**: Conduct lessons learned and improve processes

5.6.4 Post-Incident Review

- All incidents must undergo a post-incident review
- Lessons learned must be documented and shared
- Security controls must be updated based on findings
- Incident metrics must be tracked and reported

5.7 Compliance Requirements

- Systems must comply with relevant regulatory requirements
- Security controls must be mapped to compliance frameworks
- Regular compliance assessments must be conducted
- Non-compliance issues must be tracked and remediated

5.8 Policy Review and Updates

- This policy must be reviewed annually or after significant changes

- Policy updates must be approved by the CISO and executive management
- Policy exceptions must be formally requested, documented, and approved
- Compliance with this policy must be regularly audited

6. Appendices

Appendix A: Risk Assessment Methodology

The risk assessment followed a structured approach:

1. Asset identification and valuation
2. Threat identification and assessment
3. Vulnerability identification and assessment
4. Risk calculation using impact and likelihood factors
5. Risk prioritization based on calculated risk scores

Appendix B: Control Testing Procedures

Controls were tested using the following methods:

1. Documentation review of existing policies and procedures
2. Configuration review of systems and security tools
3. Log analysis to verify control effectiveness
4. Interview with key personnel
5. Comparison against industry best practices and frameworks

Appendix C: Evidence Collection

Evidence collected during this audit included:

1. Incident report CSA-SOC-MAR-2025–001
2. Wazuh dashboard screenshots and alerts
3. PFsense firewall configuration
4. Network scan results showing open ports
5. Slack notification samples
6. System configuration settings
7. Authentication logs from affected systems
8. Interview notes with SOC team members

Appendix D: Glossary of Terms

- **Brute Force Attack**: A trial-and-error method used to obtain information such as a password or PIN by systematically trying all possible combinations.