Security Operations Lead Playbook

Role: Security Operations Lead (Karine)
Scope: Company-wide cybersecurity monitoring, protection, and incident response

---

1. Introduction

This playbook provides structured guidance on responsibilities, daily operational workflows, incident response procedures, communication protocols, and tools used within the SOC environment.

2. Key Responsibilities

1. **Threat Monitoring and Detection**
    - Continuously monitor SIEM dashboards and alerts.
    - Identify anomalies, suspicious behavior, and potential intrusions.
    - Tune alert thresholds to minimize false positives.
2. **Incident Analysis and Response**
    - Perform initial triage of alerts.
    - Investigate indicators of compromise (IoCs) using threat intelligence tools.
    - Classify and prioritize incidents based on severity.
    - Document incident details and escalate when necessary.
3. **Threat Intelligence Integration**
    - Collect and analyze threat data from internal and external sources.
    - Update detection signatures and correlation rules.
    - Contribute to threat reports and intelligence briefs.
4. **Vulnerability Management Support**
    - Collaborate with IT teams to identify and remediate vulnerabilities.
    - Validate patching effectiveness and track exposure metrics.
5. **Continuous Improvement**
    - Participate in post-incident reviews.
    - Recommend and implement SOC process improvements.
    - Support automation efforts to optimize response time.

3. SOC Workflow Overview

Phase	Objective	Key Actions	Tool Used
Monitoring	Detect anomalies and threats	SIEM log review, correlation rule validation	**Microsoft Sentinel**
Analysis	Determine impact and severity	Log correlation, endpoint analysis, threat intel lookup	**Microsoft Defender for Endpoint**
Response	Contain and eradicate threat	Quarantine systems, revoke credentials, block IPs	**Microsoft Intune / Microsoft 365 Defender**

Phase	Objective	Key Actions	Tool Used
Recovery	Restore systems and validate	Patch, verify normal operations	**Azure Backup**
Review	Learn and improve	Document lessons learned and corrective actions	**Microsoft SharePoint**

Explanation:

- **Microsoft Sentinel** — SIEM/SOAR platform for centralized monitoring.
- **Defender for Endpoint** — provides detailed incident analysis and correlation.
- **Intune / 365 Defender** — enables device isolation, credential revocation, and real-time response.
- **Azure Backup** — ensures quick and secure recovery.
- **SharePoint** — used for post-incident documentation and knowledge sharing.

4. Incident Response Playbook (See Annex 1)

Step 1: Alert Detection

- Triggered by SIEM, IDS/IPS, or user report.
- Confirm alert validity and classify type (malware, phishing, unauthorized access, etc.).

Step 2: Triage and Prioritization

- Identify affected systems and data sensitivity.
- Assign severity: Low, Medium, High, or Critical.

Step 3: Investigation

- Gather evidence: logs, network packets, system snapshots.
- Correlate IoCs with known threat patterns.
- Determine the root cause and attack vector.

Step 4: Containment

- Isolate compromised systems.
- Block malicious IPs or domains.
- Disable affected user accounts if necessary.

Step 5: Eradication and Recovery

- Remove malware or malicious scripts.
- Patch vulnerabilities exploited in the incident.
- Restore clean backups and verify system integrity.

Step 6: Post-Incident Review

- Conduct debrief with SOC and IT teams.
- Update detection and prevention mechanisms.
- Document incident timeline and lessons learned.

5. Daily, Weekly, and Monthly Tasks (See Annex 2)

Frequency	Tasks
Daily	Review SIEM alerts, analyze anomalies, update watchlists, report findings to SOC lead.
Weekly	Conduct trend analysis, review false positive rates, participate in team briefings.
Monthly	Perform rule tuning, generate monthly threat landscape report, review KPIs.

6. Key Performance Indicators (KPIs)

Metric	Target	Frequency
Mean Time to Detect (MTTD)	< 30 minutes	Monthly
Mean Time to Respond (MTTR)	< 2 hours	Monthly
False Positive Rate	< 10%	Monthly
Phishing Click Rate	< 5%	Quarterly
Patch Compliance	100%	Monthly

7. Collaboration and Communication

- Maintain open communication with IT, Incident Response, and Risk Management teams.
- Escalate critical incidents according to defined escalation paths.
- Use collaboration tools such as Microsoft Teams, Slack, and JIRA for documentation and coordination.
- Maintain confidentiality and integrity of all SOC data and reports.

8. Key Tools & Platforms

Category	Selected Tool	Purpose
EDR	**Microsoft Defender for Endpoint**	Endpoint protection & telemetry
SIEM/MDR	**Microsoft Sentinel**	Centralized log monitoring & threat detection
Email Security	**Microsoft Defender for 365**	Phishing & spam filtering
Backup & Recovery	**Azure Backup**	Data protection and restoration
Access Control	**Microsoft Entra ID (formerly Azure AD)**	MFA & identity management
Reporting	**Power BI**	Metrics visualization & dashboards

9. Continuous Learning and Development

- Stay current with emerging threats, exploits, and security technologies.
- Obtain certifications such as:
  - CompTIA Security+
  - Certified SOC Analyst (CSA)
  - Certified Ethical Hacker (CEH)
  - GIAC Certified Incident Handler (GCIH)
- Participate in threat-hunting exercises and red team/blue team simulations.

SOC Governance & RACI Section

The **RACI matrix** defines *who is Responsible, Accountable, Consulted, and Informed* for each key security process.

Function / Task	Project Manager (A)	Lead Architect (B)	Identity & SaaS Eng (C)	Network & Data Protection (D)	Security Operations Lead (E)	Incident Response Lead (F)
Security policy definition	C	A	C	C	C	C

Function / Task	Project Manager (A)	Lead Architect (B)	Identity & SaaS Eng (C)	Network & Data Protection (D)	Security Operations Lead (E)	Incident Response Lead (F)
Identity & access management	I	C	R/A	C	I	I
Endpoint protection (EDR, patching)	I	C	C	R	A	I
Network security & segmentation	I	C	I	R/A	C	I
Logging & monitoring (SIEM/MDR)	I	C	I	C	R/A	C
Phishing awareness & training	I	I	I	I	R	A
Incident detection & triage	I	I	I	I	R/A	C
Incident response coordination	I	I	I	I	C	R/A
Backup and recovery testing	I	C	I	R	C	A
Reporting & KPI tracking	A	I	I	I	R	C

NOTE:
R — Responsible | A — Accountable | C — Consulted | I — Informed

---

Runbooks:

1. **Phishing Alert Runbook**
    - Verify alert from SIEM (sender domain, reputation).
    - Isolate affected inbox (Exchange quarantine or Google Workspace).
    - Notify user not to click or reply.
    - Delete suspicious email from all mailboxes.
    - Block domain in email security gateway.

    - Report incident in SOC ticket system.
2. **Ransomware Detection Runbook**
    - Disconnect endpoint from the network.
    - Trigger EDR scan.
    - Check backup availability and integrity.
    - Restore clean image if needed.
    - Update incident report and notify management.
3. **Unauthorized Access Runbook**
    - Identify affected account (via SIEM logs).
    - Force MFA reset and password change.
    - Review recent login locations.
    - Revoke suspicious sessions.
    - Conduct post-incident analysis.
4. **Data Loss / Device Theft Runbook**
    - Mark device as lost in MDM.
    - Trigger remote wipe (if available).
    - Change passwords for connected accounts.
    - Review access logs for anomalies.
    - File report to management and legal if PII affected.

Lessons Learned

Section	Content
Incident Summary	Date, time, type of incident, detection source
Impact	Affected systems, users, data (PII, financial, etc.)
Root Cause	Technical and human factors
Response Actions Taken	Timeline of containment, eradication, and recovery
Lessons Learned	What worked, what failed
Preventive Measures	Future improvements, new controls
Approval	SOC Lead signature and date

Annex 1.

Incident Response Procedure

1. Objective

The objective of the Incident Response Procedure is to ensure that all cybersecurity incidents affecting EasyBusy's information systems are managed in a structured, timely, and effective manner.
This procedure defines the phases, responsibilities, and tools used to detect, analyze, contain, eradicate, and recover from security incidents, as well as to capture lessons learned to prevent recurrence.

2. Scope

This procedure applies to all EasyBusy employees, systems, and third-party partners with access to corporate information assets.
It covers incidents related to unauthorized access, malware infections, phishing, data breaches, denial-of-service attacks, and other cybersecurity events.

3. Roles and Responsibilities

Role	Responsibility
SOC Tier 1 Analyst	Initial alert review, triage, classification, and escalation.
SOC Tier 2 Analyst	In-depth investigation, correlation of events, and containment actions.
SOC Tier 3 / Incident Responder	Advanced analysis, malware reverse-engineering, and coordination of eradication and recovery.
SOC Lead (Security Operations Lead)	Oversight of the entire response process, communication with management, and post-incident review.
IT Operations Team	System isolation, patching, restoration, and technical recovery tasks.
Management / Legal / HR	Decision-making, external communication, and compliance actions when required.

4. Incident Response Lifecycle

4.1 Identification and Triage

- Monitor alerts from SIEM, EDR, and email security platforms.
- Validate whether the event constitutes a true incident.
- Assign severity based on impact and likelihood (Critical / High / Medium / Low).
- Create an incident record in the SOC ticketing system.

4.2 Containment

- Short-term: Isolate infected endpoints or suspend compromised accounts.
- Long-term: Implement firewall rules or network segmentation to prevent lateral movement.
- Notify the SOC Lead and affected business units.

4.3 Eradication

- Remove malicious files or artifacts.
- Patch vulnerable systems.
- Perform forensic analysis to confirm the threat is eliminated.

4.4 Recovery

- Restore services from backups if required.
- Closely monitor restored systems for any abnormal behavior.
- Verify that normal operations are fully resumed.

4.5 Post-Incident Activities

- Conduct a “Lessons Learned” session within 72 hours after incident closure.
- Document root cause, timeline, and actions taken.
- Update detection rules, runbooks, and awareness materials.
- Report incident summary to management and, if applicable, regulatory bodies.

5. Incident Severity Classification

Severity	Description	Response Target
Critical	Major breach affecting business continuity or sensitive data.	Immediate – SOC Lead notified instantly.
High	Serious compromise of key systems or privileged accounts.	Within 15 minutes.

Severity	Description	Response Target
Medium	Limited user or device infection, contained impact.	Within 2 hours.
Low	Suspicious activity or policy violation with minimal risk.	Within 24 hours.

6. Communication and Reporting

- All internal communications must follow the established SOC communication channels.
- External notifications (law enforcement, customers, regulators) must be approved by management.
- The SOC Lead is responsible for preparing a **Post-Incident Report** summarizing the event, response actions, and recommendations.

7. Continuous Improvement

- Incident metrics and response KPIs are reviewed monthly.
- Runbooks and response procedures are updated quarterly or after major incidents.
- Regular simulation exercises and tabletop tests ensure SOC readiness.

Annex 2.

SOC LEAD Tasks Table

Daily Tasks

#	Task	Purpose
1	Review EDR and SIEM dashboards for new alerts or anomalies.	Early detection of threats.
2	Check email security gateway logs (phishing/quarantine).	Identify phishing or spam attempts.
3	Verify endpoint compliance (MFA enabled, EDR running, encryption status).	Maintain endpoint security baseline.
4	Communicate with IT/Network leads on any critical alerts.	Rapid response and escalation.
5	Log any incidents or suspicious activity into the Incident Log.	Maintain full audit trail.

Weekly Tasks

#	Task	Purpose
1	Conduct threat hunting using SIEM queries (unusual logins, data transfers).	Proactive detection.
2	Review vulnerability scans and coordinate patch deployment with IT.	Reduce attack surface.
3	Verify new assets or SaaS accounts are added to the inventory.	Maintain asset visibility.
4	Check backup system logs for recent job completion and integrity.	Ensure recoverability.
5	Analyze phishing simulation results (if available) and report trends.	Improve employee awareness.

Monthly Tasks

#	Task	Purpose
1	Review access control lists — ensure least privilege is applied.	Prevent unauthorized access.
2	Perform endpoint compliance audit (patch level, encryption, EDR).	Validate security hygiene.
3	Run a backup restore test (verify RTO/RPO).	Confirm recovery readiness.
4	Produce a Security Metrics Report (MFA %, EDR coverage %, alert volume).	Track progress vs KPIs.
5	Hold a coordination meeting with all leads (A–F).	Cross-team alignment.
6	Update the Security Operations Runbook with lessons learned.	Institutionalize knowledge.

Quarterly Tasks

#	Task	Purpose
1	Lead an **Incident Response tabletop exercise**.	Improve readiness and communication.
2	Review SIEM/MDR configuration and alert thresholds.	Optimize signal-to-noise ratio.
3	Update security awareness training content with new examples.	Adapt to evolving threats.
4	Review and adjust KPIs and security roadmap with PM.	Continuous improvement.
5	Verify all security policies are still relevant and up to date.	Maintain compliance.