Security Operations Lead Playbook

Role: Security Operations Lead (Karine)
Scope: Company-wide cybersecurity monitoring, protection, and incident response
Goal: Maintain 24/7 operational security, minimize cyber risks, and ensure compliance.

---

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 (See Annex 2)

Phase	Objective	Key Actions	Tools Used
Monitoring	Detect anomalies and threats	SIEM log review, correlation rule validation	Splunk, Azure Sentinel, QRadar

Phase	Objective	Key Actions	Tools Used
Analysis	Determine impact and severity	Log correlation, endpoint analysis, threat intel lookup	Wireshark, VirusTotal, MITRE ATT&CK
Response	Contain and eradicate threat	Quarantine systems, revoke credentials, block IPs	EDR, Firewalls, IAM systems
Recovery	Restore systems and validate	Patch, verify normal operations	Backup tools, Change management systems
Review	Learn and improve	Document lessons learned	Confluence, JIRA, SharePoint

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 3)

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. Tools and Technologies

Category	Examples
SIEM	Splunk, Azure Sentinel, IBM QRadar
EDR/XDR	CrowdStrike, Microsoft Defender, SentinelOne
Network Analysis	Wireshark, Zeek, NetFlow
Threat Intelligence	VirusTotal, AbuseIPDB, AlienVault OTX
Ticketing & Documentation	JIRA, ServiceNow, Confluence

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.

Phase 1 — Preparation & Deployment

1. Deploy Endpoint Detection & Response (EDR)

Objective: Ensure continuous monitoring and protection across all endpoints.

Actions:

- Select and deploy an EDR solution (Microsoft Defender for Endpoint / CrowdStrike Falcon).
- Install agents on all workstations and servers.
- Configure centralized management console for alerts and telemetry.
- Verify connectivity and health status of all agents.
- Run a controlled test (e.g., EICAR file) to confirm detection and isolation.

Tools: Microsoft Defender / CrowdStrike / SentinelOne
KPI: 100% endpoint coverage, 0 offline agents

---

2. Set Up Centralized Logging (SIEM Integration)

Objective: Collect and correlate all security events for unified visibility.

Actions:

- Integrate data sources:
  - EDR
  - Firewalls / VPN
  - SaaS platforms (Google Workspace, CRM)
  - Identity provider (Azure AD)
- Deploy or configure SIEM platform (Microsoft Sentinel / Splunk / Wazuh).
- Build dashboards for:
  - Login anomalies
  - Failed authentications
  - Malware detections
- Implement initial correlation rules (e.g., brute-force, privilege escalation).

Tools: Sentinel / Splunk / Wazuh
KPI: 100% log source coverage, alert-to-resolution <2 hours

---

3. Enforce MFA & Access Control

Objective: Protect all user accounts with strong authentication and least privilege.

Actions:

- Enforce MFA across all SaaS and corporate systems.
- Configure conditional access rules for administrators.
- Review user permissions and revoke unnecessary privileges.
- Deactivate unused or orphaned accounts.

Tools: Azure AD / Google Admin Console
KPI: 100% MFA coverage, 0 orphan accounts

Phase 2 — Monitoring & Incident Response

4. Establish Incident Response (IR) Procedures

Objective: Respond to threats quickly and effectively.

Actions:

- Develop an **Incident Response Playbook** for:
  - Phishing attacks
  - Malware infections
  - Insider threats
- Define responsibilities and escalation paths.
- Automate common tasks using SOAR (e.g., isolating a device).
- Conduct tabletop exercises to validate readiness.

Tools: Sentinel Automation Rules / Splunk Phantom / TheHive
KPI: Detection-to-containment time <15 minutes

---

5. Phishing Simulation & Awareness Program

Objective: Improve employee resistance to phishing attempts.

Actions:

- Run simulated phishing campaigns quarterly.
- Track click rate and report incidents.
- Deliver targeted awareness training for vulnerable employees.

Tools: Microsoft Attack Simulator / KnowBe4
KPI: Phishing click rate <5%

---

6. Vulnerability Scanning & Patch Management

Objective: Detect and remediate vulnerabilities before exploitation.

Actions:

- Deploy a vulnerability scanner (Qualys / Nessus / OpenVAS).
- Schedule weekly scans for endpoints and servers.
- Share reports with the IT Lead for remediation.
- Enforce closure of critical vulnerabilities within 7 days.

Tools: Nessus / Qualys / OpenVAS
KPI: Critical vulnerabilities remediated <7 days

Phase 3 — Continuous Improvement

7. Backup & Recovery Validation

Objective: Ensure data can be recovered after any incident.

Actions:

- Verify daily backups and encryption status.
- Perform monthly restore tests for sample datasets.
- Document and report recovery success metrics.

Tools: Veeam / Azure Backup
KPI: 100% backup success, 100% recovery test success

---

8. Monthly Security Review & Reporting

Objective: Maintain visibility and improve performance through metrics.

Actions:

- Prepare monthly security report with key metrics:
  - MFA coverage
  - EDR health
  - Incident count and response time
  - Phishing click rate
- Present findings to the IT Lead and CTO.
- Propose process improvements based on data trends.

Tools: Power BI / Excel / SIEM Reports
KPI: ≥10% improvement month-over-month

---

9. Threat Intelligence Integration

Objective: Strengthen proactive defense by leveraging threat data.

Actions:

- Integrate external Threat Intelligence (TI) feeds.
- Automate IOC (Indicator of Compromise) updates in SIEM and firewalls.
- Use TI data to enhance correlation rules and detection models.

Tools: MISP / AlienVault OTX / Abuse.ch
KPI: 0 missed IOC alerts

Tools Setup Details

1. EDR Setup

- **Platform:** Microsoft Defender for Endpoint (preferred)
- **Deployment:**
  - Use Intune for bulk agent installation.
  - Enable “Automatic sample submission” and “Real-time protection.”
  - Configure tamper protection to prevent agent disabling.
- **Verification:**
  - Run PowerShell command `Get-MpComputerStatus` to verify active protection.
  - Check “Device compliance” dashboard in the Microsoft 365 portal.

---

2. SIEM (Microsoft Sentinel)

- **Data Connectors:**
  - Azure AD sign-in logs
  - Microsoft 365 activity logs
  - EDR logs
  - Firewall syslogs
- **Dashboards:**
  - Security overview
  - Threat summary
  - Login anomalies
- **Rules & Alerts:**
  - 5 failed logins in 10 minutes
  - Multiple geo-locations in one session
  - Detection of malware hash from TI feed

---

3. SOAR Automation

- **Tool:** Sentinel Logic Apps or Splunk Phantom
- **Automated Actions:**
  - Isolate endpoint (via Defender API)
  - Disable compromised account (via Azure AD connector)
  - Notify SOC via Teams / Email
  - Create a Jira ticket automatically

---

4. Vulnerability Scanning

- **Tool:** Nessus
- **Setup:**
  - Install scanner on dedicated VM.
  - Configure authenticated scanning using domain credentials.
  - Schedule weekly automatic scans.
- **Output:**
  - Generate report (CSV, PDF) sorted by CVSS score.
  - Forward to IT Lead for patching.

---

5. Threat Intelligence Integration

- **Platform:** MISP + OTX feed integration.
- **Setup Steps:**
  - Connect MISP to SIEM through REST API.
  - Enable automatic IoC sync (hourly updates).
  - Map IoCs (IP, domain, hash) to alert rules.

---

6. Phishing Simulation

- **Tool:** Microsoft Attack Simulation Training
- **Configuration:**
  - Select realistic phishing templates.
  - Exclude admin accounts from tests.
  - Schedule quarterly campaigns.
- **Output:**
  - CSV report with open/click rates.
  - Targeted awareness sessions for repeated clickers.

---

7. Backup Verification

- **Tool:** Veeam
- **Setup:**
  - Verify daily backup jobs and encryption key status.
  - Schedule monthly restore validation test.
  - Store results in Backup Success Report.

Key Tools & Platforms

Category	Example Tools	Purpose
EDR	Microsoft Defender for Endpoint / CrowdStrike Falcon	Endpoint protection & telemetry
SIEM/MDR	Microsoft Sentinel / Splunk / Arctic Wolf	Centralized log monitoring
Email Security	Proofpoint / Microsoft Defender for 365	Phishing & spam filtering
Backup & Recovery	Veeam / Acronis / Azure Backup	Data protection and restoration
Access Control	Azure AD / Okta	MFA, identity management
Reporting	Power BI / Excel	Metrics visualization

Top KPIs to Track

Metric	Baseline	Target	Reporting
MFA Coverage	80%	100%	Monthly
EDR Coverage	90%	100%	Monthly
Phishing Click Rate	15%	<5%	Quarterly
Mean Time to Detect (MTTD)	6 hours	<1 hour	Monthly
Mean Time to Respond (MTTR)	12 hours	<4 hours	Monthly
Backup Restore Success Rate	85%	100%	Monthly

Deliverables SOC LEAD Maintain:

- Incident Log (updated daily)
- Security Metrics Report (monthly)
- Asset Inventory (Excel)

- Backup and Recovery Test Report
- Security Operations Runbook
- Awareness Campaign Reports

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
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 (they can be expanded later):

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.

Automate KPI Tracking in SIEM or Ticketing System

Track key security metrics automatically using SIEM dashboards or your ticket system (like Jira or ServiceNow).

KPI	Baseline	Target	Frequency	Source
MFA coverage	80%	100%	Monthly	IdP logs
Endpoint encryption	70%	100%	Quarterly	MDM / EDR
Phishing click rate	10%	<5%	Quarterly	Training reports
Mean time to detect (MTTD)	4 hrs	<1 hr	Monthly	SIEM
Mean time to respond (MTTR)	6 hrs	<2 hrs	Monthly	IR logs

Post-Incident Report Template (Lessons Learned Template)

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

Personal Deliverables & Reporting Duties (SOC Lead)

- SOC architecture and monitoring plan
- Weekly KPI dashboard
- Monthly threat and incident report
- Updated runbooks and playbooks repository
- Annual SOC performance review

SOC Lead reports to the **Project Manager (A)** and coordinate closely with:

- **Incident Response Lead (F)** for joint playbooks
- **Network Engineer (D)** for endpoint and backup integration
- **Identity Engineer (C)** for MFA and access logs

Quarterly Review Meetings

Purpose:
To assess SOC effectiveness and identify areas for maturity improvement (aligning with NIST CSF tiers).

Suggested agenda:

1. Review KPIs and incident trends
2. Evaluate runbook effectiveness
3. Discuss lessons learned and control gaps
4. Define next quarter’s security improvement goals
5. Update risk register and residual risk assessment

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.
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.

Excellent question — and you're right to ask that ✓

A **SOC Workflow Table** is a key deliverable in any cybersecurity project report — it visually shows how incidents flow through detection, triage, escalation, and resolution stages.

We haven't explicitly created one yet, but I can prepare it for you right now.
Here's a professional example that matches your EasyBusy SOC project and roles:

Annex 2.

SOC Workflow Table

Phase	Description	Responsible Role(s)	Tools / Systems Used	Outputs / Deliverables
1. Detection	Identify suspicious activities or anomalies from logs, alerts, or employee reports.	SOC Tier 1 Analyst	SIEM (Microsoft Sentinel), EDR (Defender for Endpoint), Email Security Gateway	Initial alert / detection event
2. Triage	Validate alerts, filter false positives, assess potential impact, assign priority level.	SOC Tier 1 Analyst	SIEM dashboard, Ticketing system	Classified incident ticket
3. Escalation	Escalate confirmed incidents based on severity or complexity.	SOC Tier 1 → SOC Tier 2 / SOC Lead	Incident Management Platform	Updated incident record, notification to SOC Lead
4. Investigation	Conduct deep analysis to determine attack vector, scope, and affected assets.	SOC Tier 2 Analyst	EDR console, Network Traffic Analyzer, Threat Intelligence feeds	Investigation report, list of affected hosts/users
5. Containment	Limit the spread of the attack and prevent further damage.	SOC Tier 2, IT Operations	EDR isolation, Firewall rules, Account suspension tools	Containment confirmation log
6. Eradication	Remove the cause of the incident (malware, exploits, compromised credentials).	SOC Tier 3, IT Operations	EDR cleanup tools, Patch Management System	Cleaned and patched systems
7. Recovery	Restore affected systems and validate integrity of operations.	IT Operations, SOC Lead	Backup systems, Monitoring tools	Restored services, recovery validation checklist
8. Post-Incident Review	Analyze lessons learned, update documentation, improve processes.	SOC Lead, All SOC members	Post-Incident Report Template, Metrics dashboard	Final report, updated runbooks / policies

Key Notes

- Each phase is tracked in the **Incident Management System** (e.g., Jira, ServiceNow, or internal ticketing tool).
- The **SOC Lead** supervises all escalations and final approvals.
- Metrics from the workflow (e.g., detection-to-response time, mean time to contain, mean time to recover) feed into SOC KPIs.

Annex 3.

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.
