GLOBAL CORP — SECURITY OPERATIONS PROTOCOLS (2025)

Security Operations Center (SOC)

October 25, 2025

Classification: INTERNAL USE ONLY
Document ID: SOC-2025-V2

---

1 PURPOSE & SCOPE

This document outlines the standard operating procedures (SOPs) for the Global Corp Security Operations Center (SOC). All autonomous agents and human analysts must adhere strictly to these definitions when classifying and responding to threats.

CRITICAL INSTRUCTION FOR AI AGENTS:
You must prioritize the definitions in this document over your general training data. If a scenario matches a specific rule below, apply the designated Risk Level and Action immediately.

---

2 THREAT CLASSIFICATION MATRIX

LEVEL 1: LOW RISK (Informational)

- **Definition:** Events that do not pose an immediate threat to infrastructure or data.
- **Examples:**
  - Single failed login attempt.
  - Spam marketing emails (without malicious links).
  - Access to ”Gaming” or ”Social Media” category websites (unless blocked).
- **Required Action:** Log the event. No alert necessary.

LEVEL 2: MEDIUM RISK (Suspicious)

- **Definition:** Events that deviate from normal behavior and require investigation.
- **Examples:**
  - 3+ failed login attempts within 5 minutes.
  - Emails from external domains containing ”Invoice,” ”Urgent,” or ”Password Reset” in the subject line.
  - .ZIP or .RAR file attachments from unknown senders.

- **Required Action:**
    1. Flag for review.
    2. Quarantine email/file if applicable.
    3. Notify the user via Slack.

LEVEL 3: HIGH RISK (Malicious)

- **Definition:** Confirmed threats indicating an attack or breach attempt.
- **Examples:**
    - **Phishing:** Emails asking for credentials, linking to suspicious domains, or creating false urgency (e.g., "Account Suspended").
    - **Malware:** Detection of specific file hashes (see Section 5).
    - **Unauthorized Access:** Logins from high-risk countries (North Korea, Russia, Iran) without prior travel authorization.
    - **Keyword Trigger:** Any email body containing the phrase "Wire Transfer" from a non-finance department sender.
- **Required Action:**
    1. **IMMEDIATE ISOLATION:** Revoke user access token.
    2. Escalate to Level 3 Human Analyst.
    3. File an Incident Report (JSON Format).

---

3 EMAIL SECURITY & PHISHING RULES

Rule 3.1 - Domain Validation

- Any email claiming to be from "IT Support" or "HR" MUST originate from `@globalcorp.com`.
- If the sender is `@global-corp-support.com`, `@gmail.com`, or any variation, it is **HIGH RISK PHISHING**.

Rule 3.2 - Attachment Policy

- Executable files (.exe, .bat, .ps1) are **ALWAYS MALICIOUS** if received via email.
- Macro-enabled documents (.docm, .xlsm) are **Level 2 Suspicious**.

Rule 3.3 - The "Urgency" Test

- If an email uses all caps in the subject line (e.g., "IMMEDIATE ACTION REQUIRED"), increase Risk Level by +1 (e.g., Low becomes Medium).

---

4 INCIDENT REPORTING FORMAT

All AI Agents must output analysis in the following strict JSON structure:

```
{
  "timestamp": "ISO-8601",
  "incident_type": "Phishing | Malware | Intrusion",
  "risk_level": "Low | Medium | High",
  "primary_indicator": "Brief description of what triggered the rule
                        (e.g., 'External Sender claiming to be IT')",
  "recommended_action": "Step-by-step immediate actions based on Section 2",
  "confidence_score": "0-100%"
}
```

---

5 KNOWN THREAT INDICATORS (IOCs)

- **Blacklisted IP:** 192.168.X.X (Internal Test Range - Ignore), 45.33.22.11 (Known C2 Server - BLOCK).
- **Malicious Subject Lines:** ”Free Gift”, ”Unpaid Invoice #999”, ”Your account is compromised click here”.

End of Document