SOC Investigation Workflow Cheat Sheet

🔹 1. Basic SOC Investigation Flow

When an alert appears:

1. Validate the alert
2. Check log sources and context
3. Identify affected systems or users
4. Determine if activity is benign or malicious
5. Collect supporting evidence
6. Escalate or close with documentation

Consistency matters more than speed.

🔹 2. SIEM Investigation Checklist

When reviewing SIEM alerts:

• Confirm timestamp accuracy
• Identify source and destination systems
• Check related events before and after alert
• Review user activity tied to the event
• Look for repeated patterns
• Correlate with known attack techniques

SIEM is a starting point — not the full investigation.

🔹 3. Network Analysis Quick Steps

When analyzing traffic:

• Identify unusual external connections
• Check destination reputation if unknown
• Look for abnormal protocols or ports
• Inspect packet patterns if needed
• Compare behavior with normal baseline traffic

Network analysis helps confirm suspicious activity.

🔹 4. IDS / Detection Rule Thinking

When reviewing detection rules:

• Understand what behavior the rule detects
• Check for possible false positives
• Identify attacker techniques tied to rule logic
• Confirm rule scope (network, endpoint, etc.)
• Ensure alerts generate useful context

Detection rules should support investigation, not just create noise.

🔹 5. Endpoint Investigation Checklist

When analyzing a host:

• Identify running processes
• Look for unusual parent-child process relationships
• Check recent file changes
• Review login activity
• Identify persistence indicators
• Look for suspicious command-line usage

Endpoints often show the attacker's real actions.

🔹 6. Malware Triage Quick Flow

When malware is suspected:

1. Identify suspicious file or process
2. Check hashes and known indicators
3. Review behavior and system impact
4. Look for network communication patterns
5. Map activity to known techniques
6. Preserve evidence for deeper analysis

Triage helps decide whether full forensic analysis is needed.

🔹 7. Digital Forensics Investigation Steps

Forensic work usually includes:

• Evidence identification
• Evidence preservation
• Timeline reconstruction
• Artifact analysis
• Root cause determination
• Documentation of findings

Forensics supports both incident response and long-term security improvement.