A day in the life of a SOC analyst with DFIR

From first alert to final report—precision at every step

8:00 am
Morning briefing and threat hunting

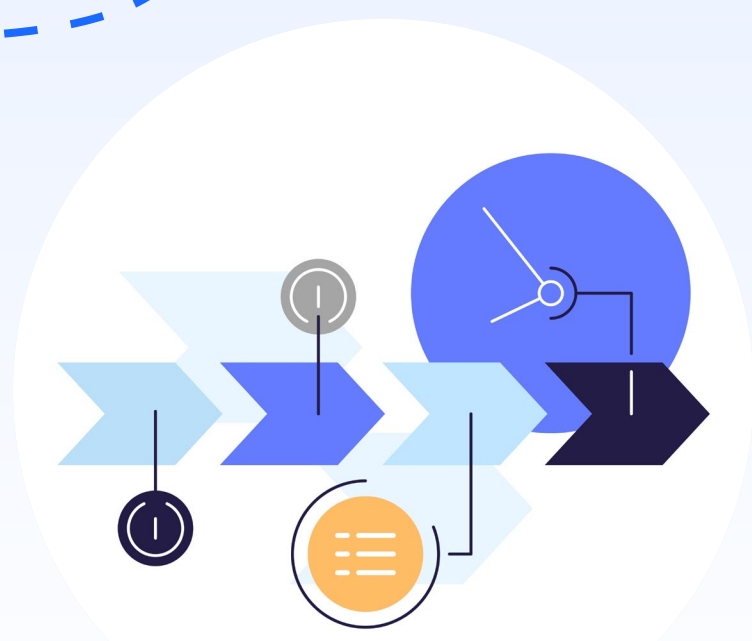
Review overnight alerts in SIEM; pivot to OpenText™ Endpoint Forensics & Response for deep dive on high-risk indicators

10:00 am
Live incident detection

Automated SOAR playbook triggers memory capture on compromised endpoint—no manual handoffs.

11:30 am
Evidence analysis and triage

Use forensic imaging to reconstruct timeline; tag critical artifacts in the OpenText Endpoint Forensics & Response console.



1:00 pm
Threat intelligence correlation

Leverage OpenText Endpoint Forensics & Response to enable rapid determination of compromise status

3:00 pm
Containment and remediation

Remotely isolate endpoints, delete malicious files, and terminate malicious processes via OpenText Endpoint Forensics & Response console.

4:00 pm
Executive reporting and continuous improvement

Export audit data of what action was taken, who took action and when the activity occurred for report summaries.

Precision-driven DFIR with OpenText Endpoint Forensics & Response

Empowering SOC teams to detect faster, investigate deeper, and report confidently

© 2025 Open Text • 10.25 | 236-000161-002