

Initial SOC triage: first 15 minutes | v7

Start: select C5, Ctrl+; then Space, then Ctrl+Shift+; then Enter. Workstation must use Eastern Time. Gold = selections.

Act on urgent harm now. Document throughout; preserve evidence and use authorized containment at any time. Bands start at analyst triage.

Process tree → Parent process → Activity timeline → File creation events → Network activity

CASE	Case / alert ID	EXAMPLE-260911-01	Local priority	P2 - High
	Analyst name	Morgan Vale (fictional)	Eastern zone	EDT
	Alert generated UTC	2026-09-11 13:58:00	Queue age (min)	2.0
START	START HERE Eastern date & time	2026-09-11 10:00:00	Start time UTC	2026-09-11 14:00:00
	Decision recorded UTC	2026-09-11 14:12:00	Target (min)	15
	Primary host / account / tenant	FIN-WS042 / a.chen / Northstar Demo	Triage time (min)	12.0
	Original alert severity	EDR High - rule PS-104	Repeated hour	First (EDT)
Minutes	Analyst action	Findings / decision / gaps	Step status	Evidence IDs v7 Case: EXAMPLE-260911-01
0-1 DETECT	READ THE ALERT			
	Read the full alert: rule, event, source, entities and event time. Record case, analyst and triage start above. [NIST SP 800-53 Rev. 5: AU-3 / AU-8 / IR-5]	EDR PS-104: Office launched script interpreter on FIN-WS042 at 13:57:42Z. Alert queued 2 min. Full event reviewed.	Done	E01
	Finding recorded UTC	2026-09-11 14:01:00		
1-3 DETECT	CHECK WHAT IS NORMAL			
	Is this normal? Check role, baseline and approved changes; corroborate the alert or explain the false positive. [NIST SP 800-53 Rev. 5: AU-6 / SI-4]	Finance user; scripting is not baseline. No approved change. EDR and proxy corroborate unusual child process and outbound connection.	Done	E02, E03
	Finding recorded UTC	2026-09-11 14:03:00		

Minutes	Analyst action	Findings / decision / gaps	Step status	Evidence IDs v7 Case: EXAMPLE-260911-01
3-7 DETECT	BUILD THE PICTURE			
	Identify host/user/IP/app/owner. Start with 24-hour activity and alerts; compare peers and before/after events. Record window, peers, matches and gaps. [NIST SP 800-53 Rev. 5: IR-4 / AU-6 / SI-4]	Finance owner: R. Holt. 10.20.4.42; Office. Window: Sep 10 14:00 to Sep 11 14:06Z. 20 peers: 1 related host (FIN-WS017), 2 alerts total. Pre/post checked; DNS gap.	Done	E04, E05
	Finding recorded UTC	2026-09-11 14:07:00		
7-10 DETECT	TRACE THE ACTIVITY			
	Examine the process tree, parent, command line, children, files and connections, or the equivalent identity/cloud event chain. [NIST SP 800-53 Rev. 5: AU-6 / SI-4]	WINWORD > powershell > rundll32. File: invoice.dat. Connection to 203.0.113.77:443 at 13:57:48Z. EDR events corroborate chain; payload not yet analyzed.	Done	E06, E07
	Finding recorded UTC	2026-09-11 14:10:00		
10-13 RESPOND	MAKE THE INITIAL CALL			
	Assess scope, impact, severity and uncertainty. Apply incident criteria; notify lead and use authorized containment. Preserve evidence; log approval, action and result. [NIST SP 800-53 Rev. 5: IR-4 / IR-6 / AU-9]	High severity; suspicious, moderate uncertainty. Lead declared incident at 14:11Z. Both hosts isolated at 14:12Z under IR-07; exports preserved. No spread observed after isolation.	Done	E08, E09
	Finding recorded UTC	2026-09-11 14:13:00		
13-15 RESPOND	SUMMARIZE AND HAND OFF			
	Summarize trigger, checks, findings and assessment. Record next action/owner, due and handoff UTC, acknowledgment and open gaps. [NIST SP 800-53 Rev. 5: IR-5 / IR-8]	Escalated to Avery Stone at 14:14Z; acknowledged 14:14:30Z. Two hosts isolated. Payload and scope analysis due 14:30Z; DNS gap carried forward.	Done	E10
	Finding recorded UTC	2026-09-11 14:15:00		

N/A needs a reason. No matches applies only to checked coverage. Detect = orange; Respond = red. Detailed mappings: References.

Minutes	Analyst action	Findings / decision / gaps	Step status	Evidence IDs v7 Case: EXAMPLE-260911-01
ASSESS	Immediate harm / spread indicators?	Yes	Assessed severity	High
	Preliminary assessment	Suspicious	Assessment uncertainty	Moderate
	Decision	Escalate now	Decision guidance	Definitions: Team Setup
	Rationale, evidence, gaps and alternative	Unapproved process chain on 2 hosts (E04/E06). Benign automation not confirmed. No proven data loss; payload and DNS visibility remain gaps.	Incident declaration	Declared
ACTION	Action taken and result	Isolated FIN-WS042 and FIN-WS017; EDR confirmed success. Exports preserved (E08/E09).	Declared by	Avery Stone, IR lead
	Action UTC	2026-09-11 14:12:00	Declared UTC	2026-09-11 14:11:00
	Runbook / authority / approver	IR-07 §3; Avery Stone approved isolation in case at 14:11Z (E08).	Authority unclear?	Escalate to the lead. Record request and approval status.

Minutes	Analyst action	Findings / decision / gaps	Step status	Evidence IDs v7 Case: EXAMPLE-260911-01
HANDOFF	Handoff owner and channel	Avery Stone / #demo-ir / case	Business impact	Service degradation
	Handoff sent UTC	2026-09-11 14:14:00		
	Next action and owner	Avery Stone: analyze payload, extend scope, assess data access.	Observed scope	Recurring / related
	Next action due UTC	2026-09-11 14:30:00		
	Open gaps	DNS logs missing 13:50-14:00Z; payload unverified; data-access review pending.	Recovery referral	R. Holt; hold restore pending IR clearance.
	Next update UTC	2026-09-11 14:30:00		
	Ticket notes and evidence saved?	Yes		
	Recipient acknowledged?	Yes		
	Handoff review	Recorded - review quality and follow-up		