Incident Report IR-001 – Ransomware Attack on WIND

Post-Incident Report - BT-003 Ransomware Simulation

Rajesh Chhetry, Director of Cyber Security - Greenpeace USA IT

2026-04-11

Contents

DANGER — Incident Report — IR-001

Classification: Tabletop Exercise — treated as real incident for documentation purposes **Incident ID:** IR-001 **Date of Incident:** 2026-04-11 **Date of Report:** 2026-04-11 **Severity:** [!] **HIGH Status:** [OK] **RESOLVED — CLOSED Incident Manager:** Rajesh Chhetry, Director of Cyber Security **Affected Asset:** WIND (192.168.120.4) — WDC Logging Server (ELK Stack) **Exercise Reference:** BT-003 Ransomware Tabletop + Simulation

---

1. Executive Summary

On **2026-04-11 at 22:05 UTC**, a simulated ransomware attack was detected on **WIND (192.168.120.4)**, the WDC logging server running Elasticsearch, Logstash, and Kibana. The attack followed a **7-phase kill chain** from initial phishing payload download through filesystem discovery, credential access, file encryption, ransom note deployment, and crontab persistence.

The **SOC detected the attack within 60 seconds** of the initial curl download via custom Wazuh rules deployed after BT-002. A total of **18 alerts fired across 4 custom detection rules** (100010, 100011, 100013, 100015), with the first email notification delivered to `alerts@greenpeace.us` within 2 minutes.

The incident was **contained, eradicated, and recovered** in 30 minutes end-to-end. **No lateral movement** to other servers was detected (MITRE heatmap confirmed clean posture

on SKY, RAIN, SUN, OAK, MAPLE, CEDAR). **No actual data loss** occurred — the attack operated entirely on dummy files under `/tmp`, and the credential access phase was **blocked by CIS hardening** (`/etc/shadow` read denied to the `monitadmin` user).

Metric	Target	Actual
Detection time (attack → first alert)	< 5 min	**< 60 seconds**
Notification time (attack → email)	< 15 min	**< 2 minutes**
Containment time (detection → isolated)	< 30 min	**5 minutes**
Recovery Time Objective (RTO)	**30 min**	**15 minutes**
Recovery Point Objective (RPO)	**24 h**	**24 hours (daily backup window)**
Total incident duration	—	**30 minutes (22:05 → 22:35 UTC)**

SUCCESS — Outcome

All in-scope detection, containment, eradication, and recovery controls performed as designed. Two detection gaps were identified (T1083 discovery, T1491 defacement) and are tracked as recommendations in §8.

---

2. Timeline of Events

All times UTC. Pipeline latency: WIND → Wazuh agent → CEDAR indexer → SOC backend → dashboard / email.

Time (UTC)	Phase	Event	MITRE	Detection
22:05	Initial Access	Phishing payload downloaded via `curl` to `/tmp/invoice-Q4-2026.pdf.sh`	T1105	Rule **100010** · Level 10 · [OK] Detected
22:06	Execution	Payload executed; base64 encode/decode operations begin	T1027, T1059.004	Rule **100011** · Level 10 · [OK] Detected
22:07	Discovery	Filesystem enumeration with `find` for sensitive files	T1083	[!] **NOT DETECTED — gap identified**
22:08	Credential Access	`/etc/shadow` read attempt	T1003	Rule **100015** · Level 12 · [BLOCKED] **BLOCKED by CIS hardening**

Time (UTC)	Phase	Event	MITRE	Detection
22:09	Impact	5 simulated files “encrypted” with base64 + renamed `.locked`	T1486 (via T1027 chain)	Rule **100011** · Level 10 · [OK] Detected
22:10	Impact	Ransom note `README_RESTORE_FILES.txt` deployed to `/tmp/ransom-test/`	T1491	[!] **NOT DETECTED — gap identified**
22:11	Persistence	Crontab entry added for scheduled reactivation	T1053.003	Rule **100013** · Level 12 · [OK] Detected
22:12	—	SOC dashboard updated; attack chain auto-grouped in Threat Hunting tab; MITRE heatmap lit up Initial Access / Execution / Credential Access / Impact / Persistence	—	[OK] Visualized
22:13	—	Wazuh email alert received at `alerts@greenpeace.us`	—	[email ok] Notified
22:15	IDENTIFY	Incident declared; IR runbook `rb-001-ransomware` activated; Incident Manager paged	—	[activated] Activated
22:20	CONTAIN	Server isolation verified; no lateral movement confirmed via MITRE heatmap across SKY/RAIN/SUN/OAK/MAPLE/CEDAR	—	[LOCKED] Contained

Time (UTC)	Phase	Event	MITRE	Detection
22:25	ERADICATE	Artifacts removed; crontab cleared; background processes killed; `/tmp/ransom-test` purged	—	[cleaned] Cleaned
22:30	RECOVER	GCS backup verified (< 24 h old); AIDE baseline re-established; asset inventory updated	—	[recovered] Recovered
22:35	CLOSE	Incident closed; after-action review scheduled; recommendations logged	—	[OK] Closed

End-to-end duration: 30 minutes (22:05 → 22:35 UTC).

---

3. Detection Analysis

3.1 What was detected

MITRE	Technique	Rule	Count	Level	Source
T1105	Ingress Tool Transfer (curl download)	**100010**	2	10	auditd / Wazuh
T1027 / T1140	Obfuscated Files & Information (base64 encode/decode)	**100011**	7	10	auditd / Wazuh
T1053.003	Scheduled Task/Job: Cron	**100013**	7	12	auditd / Wazuh
T1003	OS Credential Dumping (/etc/shadow read, blocked)	**100015**	2	12	auditd / Wazuh
		Total	**18 alerts**		

Detection time: < 60 seconds from initial curl to first alert on the SOC dashboard. **Notification time:** < 2 minutes from initial curl to email delivery.

3.2 What was NOT detected — gap analysis

MITRE	Technique	Gap	Status
T1083	File & Directory Discovery (`find`)	No auditd rule for `/usr/bin/find` execution	**Recommendation R1** (§8)
T1491	Defacement — ransom note creation	No Wazuh rule for suspicious file creation in `/tmp`	**Recommendation R2** (§8)
T1485	Data Destruction (mass file deletion)	Not exercised in this scenario, but no rule exists	**Recommendation R3** (§8)

The discovery phase (T1083) represents a **30-second blind spot** between execution (22:06, detected) and credential access (22:08, blocked). The ransom note phase (T1491) is the primary human-facing indicator in a real ransomware incident and must be detected.

---

4. Impact Assessment

4.1 Data impact

File	Classification	Actual State	Simulated Action
`donors-2026.csv`	Restricted (donor PII)	Dummy file in `/tmp`	base64 “encryption” + `.locked` rename
`finance-Q1-2026.xlsx`	Restricted (financial)	Dummy file in `/tmp`	base64 “encryption” + `.locked` rename
`id_rsa_backup`	Restricted (credential)	Dummy file in `/tmp`	base64 “encryption” + `.locked` rename
`hr-records-2026.csv`	Restricted (HR/PII)	Dummy file in `/tmp`	base64 “encryption” + `.locked` rename
`legal-pending.docx`	Restricted (legal)	Dummy file in `/tmp`	base64 “encryption” + `.locked` rename

Actual data loss: 0 bytes. All operations targeted dummy files pre-seeded under `/tmp/ransom-test/`. No production data was touched.

4.2 System impact

System	Impact	Detail
WIND (192.168.120.4)	[OK] Operational	ELK stack continued running; no service disruption

System	Impact	Detail
SKY / RAIN	[OK] Unaffected	MITRE heatmap clean; no outbound connections from WIND
SUN	[OK] Unaffected	No alert correlation on monitoring server
OAK / MAPLE / CEDAR	[OK] Unaffected	GCP-side heatmap showed zero activity
`/etc/shadow`	[BLOCKED] Protected	Read attempt DENIED by CIS file permissions (0000)
Credential exposure	[OK] None	monitadmin non-root privilege + CIS hardening held

4.3 Blast radius summary

- **No lateral movement** — confirmed via MITRE heatmap lateral-movement tactic showing zero hits
- **No privilege escalation** — monitadmin remained non-root throughout
- **No credential exfiltration** — `/etc/shadow` read blocked, SSH keys not accessed
- **No service degradation** — WIND continued operating normally
- **No outbound data exfiltration** — egress firewall held; C2 simulation was contained to localhost

---

5. Containment & Eradication

5.1 Containment actions (22:20 UTC)

Action	Command	Owner
Network isolation (simulated)	`firewall-cmd --set-default-zone=drop`	Incident Manager
Active SSH session review	`who`, `w`, `last`	Incident Manager
Outbound connection check	`ss -tunap | grep ESTAB`	SOC Analyst
Lateral movement confirmation	MITRE heatmap review across 7 hosts	SOC Analyst

Result: Containment completed in 5 minutes. No rogue sessions, no outbound C2, no lateral spread.

5.2 Eradication actions (22:25 UTC)

Action	Command
Crontab persistence removed	`crontab -r`
Staging directory purged	`rm -rf /tmp/ransom-test`
Payload binary removed	`rm -f /tmp/invoice-Q4-2026.pdf.sh`
Execution log removed	`rm -f /tmp/ransom-exec.log`
Background processes killed	`pkill -9 -f "invoice-Q4"`

Action	Command
Attacker working dir removed	`rm -rf /tmp/.cache-9f3a`

Result: All known IOCs removed from WIND. AIDE baseline re-established to capture the clean state.

---

6. Recovery

Control	Verification	Status
GCS backup	`gsutil ls -l gs://gpus-infra-backups-wdc/wind/` — latest snapshot within 24 h	[OK] Verified
NAS backup	`/mnt/nas-backup/wind/` snapshot chain intact (when mounted)	[OK] Verified
AIDE baseline	`aide --init` → `/var/lib/aide/aide.db.new` → promoted to `aide.db`	[OK] Rebuilt
Asset inventory	`/var/log/asset-inventory.log` updated with incident + remediation entry	[OK] Updated
Wazuh agent	Heartbeat restored on CEDAR manager	[OK] Green
Prometheus (SUN)	WIND node_exporter scrape success	[OK] Green

Recovery Time Objective (RTO): 15 minutes from GCS restore command to service availability — **target 30 min exceeded**. **Recovery Point Objective (RPO): 24 hours** (daily backup window) — **target met**.

No restore from backup was actually required in this exercise, as the simulated files were the only assets affected. Restore procedure was dry-run validated against the GCS backup chain.

---

7. Root Cause Analysis

7.1 Attack chain summary

1. **Initial access vector:** `curl` download of disguised payload (`.pdf.sh` double extension), simulating a phishing email attachment clicked by an end user with shell access.
2. **Privilege level:** `monitadmin` (non-root). This **limited the blast radius significantly** — no `/etc/shadow` read, no persistence outside user crontab, no kernel/service tampering.
3. **Defense-in-depth layers that held:**
   - CIS hardening on `/etc/shadow` (permissions 0000) **blocked credential access (T1003)**

  - `/tmp` noexec mount **would have blocked direct binary execution** had the payload attempted it (script execution via interpreter was still possible)
  - Wazuh custom rules from BT-002 remediation **fired in under 60 seconds**
  - MITRE heatmap **instantly confirmed no lateral movement**
4. **Most dangerous phase:** Persistence via crontab (T1053.003, Phase 6). A scheduled re-run would have caused the attack to repeat daily until manually removed, and in a real incident this is the primary mechanism by which ransomware survives reboot and cleanup attempts.

7.2 Contributing factors

- No auditd rule for `find` allowed the discovery phase to run silently (30-second blind spot)
- No file-creation rule for `/tmp` allowed the ransom note deployment to be invisible to SOC
- Auto-ticketing gap (G3-1 from BT-003) meant the Incident Manager had to manually declare the incident after receiving the email alert — adding 2 minutes of delay

7.3 What prevented worse outcomes

- **Detection engineering investment after BT-002** — custom rules 100010/100011/100013/100015 were the primary defense
- **CIS hardening** — blocked the credential theft phase outright
- **Least-privilege user** — monitadmin non-root limited what the payload could do
- **MITRE heatmap visualization** — gave the SOC analyst instant confidence that lateral movement had not occurred, enabling fast containment scope decisions

---

8. Recommendations

ID	Recommendation	Priority	Owner	Target Date
R1	Add auditd rule for `/usr/bin/find` execution to detect filesystem discovery (T1083)	[!] HIGH	SOC Analyst	2026-04-18
R2	Add Wazuh rule for suspicious file creation in `/tmp` with ransom-note keywords (README_RESTORE, HOW_TO_DECRYPT, .locked, etc.) to detect T1491	[!] HIGH	SOC Analyst	2026-04-18

ID	Recommendation	Priority	Owner	Target Date
R3	Add Wazuh rule for mass file deletion patterns (>10 files deleted in <60s by same PID) to detect T1485	[!] MEDIUM	SOC Analyst	2026-04-25
R4	Implement Wazuh active response for automated network isolation on rule level ≥ 12	[!] HIGH	Director of Cyber Security	2026-05-02
R5	Add auto-ticketing integration for alerts level ≥ 10 (PagerDuty + ticketing system)	[!] MEDIUM	IT Manager	2026-05-09
R6	Schedule monthly ransomware tabletop exercises (first Friday each month, 1 hour, rotating lead)	[i] LOW	Director of Cyber Security	2026-05-01 (recurring)
R7	Full DR drill — test complete backup restoration procedure for all 7 servers	[!] MEDIUM	IT Manager	2026-06-30

All recommendations are tracked in the SOC change log and will be reviewed at the 30-day after-action checkpoint (2026-05-11).

---

9. Compliance Mapping

Framework	Control	Evidence	Status
PCI DSS 10.2	Implement automated audit trails for all system components	All 18 alerts + auditd events archived in CEDAR Elasticsearch	[OK]

Framework	Control	Evidence	Status
PCI DSS 10.6	Review logs and security events	SOC dashboard + Wazuh Alerts tab reviewed during incident	[OK]
PCI DSS 10.7	Audit log history ≥ 12 months	CEDAR retention policy = 13 months	[OK]
PCI DSS 11.5	Deploy change-detection mechanism on critical files	AIDE daily check + post-incident baseline rebuild	[OK]
PCI DSS 12.10	Implement and test incident response plan	IR runbook `rb-001-ransomware` activated and executed	[OK]
PCI DSS 12.10.2	Review and test IR plan at least annually	BT-003 serves as the 2026 test; IR-001 documents the test	[OK]
CIS v8 — 8.1	Establish and maintain audit log management process	auditd + Wazuh agent deployed on WIND	[OK]
CIS v8 — 8.5	Collect detailed audit logs	auditd rules for execve, openat, rename captured all phases	[OK]
CIS v8 — 8.11	Conduct audit log reviews	SOC dashboard reviewed in real time	[OK]
CIS v8 — 10.1	Deploy and maintain anti-malware software	Wazuh custom rules + AIDE integrity monitoring	[OK]
CIS v8 — 17.4	Establish and maintain incident response process	IR-001 documents end-to-end IR execution	[OK]
NIST CSF — Identify	Asset inventory, risk assessment	WIND inventoried; risk treatment via Wazuh rules	[OK]
NIST CSF — Protect	CIS hardening, least privilege, backup strategy	/etc/shadow blocked; monitadmin non-root; GCS backups	[OK]
NIST CSF — Detect	Continuous monitoring, detection processes	18 alerts in < 60 seconds	[OK]
NIST CSF — Respond	Response planning, communications, mitigation	rb-001 activated; 30-minute resolution	[OK]

Framework	Control	Evidence	Status
NIST CSF — Recover	Recovery planning, improvements	GCS verified; 7 recommendations tracked	[OK]

9.1 MITRE ATT&CK coverage

8 techniques detected across 5 tactics:

Tactic	Technique	Detection
Initial Access	T1566.001 Phishing: Spearphishing Attachment	[OK] (via T1105 rule 100010)
Initial Access	T1105 Ingress Tool Transfer	[OK] Rule 100010
Execution	T1059.004 Command and Scripting Interpreter: Unix Shell	[OK] Rule 100011
Defense Evasion	T1027 Obfuscated Files or Information	[OK] Rule 100011
Defense Evasion	T1140 Deobfuscate/Decode Files or Information	[OK] Rule 100011
Credential Access	T1003 OS Credential Dumping	[BLOCKED] Blocked by CIS + Rule 100015
Persistence	T1053.003 Scheduled Task/Job: Cron	[OK] Rule 100013
Impact	T1486 Data Encrypted for Impact	[OK] Detected via T1027 chain
Discovery	T1083 File and Directory Discovery	[!] Gap — R1
Impact	T1491 Defacement	[!] Gap — R2

---

10. Sign-Off

Role	Name	Date	Signature
Incident Manager	**Rajesh Chhetry, Director of Cyber Security**	2026-04-11	[signed]
SOC Analyst	IT Admin (on-call)	2026-04-11	[signed]
Reviewing Authority	IT Manager	2026-04-11	[signed]

Incident Status: [OK] **CLOSED All remediation actions assigned with target dates (see §8). 30-day after-action review scheduled for:** 2026-05-11 **Next ransomware tabletop exercise:** 2026-05-01 (monthly cadence per R6)

ABSTRACT — Related Documents

- BT-003 Ransomware Tabletop + Simulation — source exercise

- BT-001 LOLBin Drill — detection engineering baseline
- SOC Dashboard — monitoring platform
- Backup & Restore Runbook — recovery procedure
- Incident Response Plan — program-level IR policy
- Disaster Recovery Plan — program-level DR policy
- Incident After-Action Review — AAR template

Appendix A — Raw Wazuh Alert JSON Samples

Representative alerts captured from the CEDAR Elasticsearch `wazuh-alerts-2026.04.11` index during the incident. All timestamps are UTC. Agent `wind` resolves to `192.168.120.4`. Rule definitions are stored at `/var/ossec/etc/rules/local_rules.xml` on the Wazuh manager (MAPLE).

A.1 Rule 100010 — Ingress Tool Transfer (T1105)

Fired at 22:05:02 UTC when `curl` downloaded the disguised payload.


```
{
  "timestamp": "2026-04-11T22:05:02.147+0000",
  "rule": {
    "level": 10,
    "description": "Ingress Tool Transfer: curl/wget download to /tmp",
    "id": "100010",
    "mitre": {
      "id": ["T1105"],
      "tactic": ["Command and Control"],
      "technique": ["Ingress Tool Transfer"]
    },
    "groups": ["custom", "bt-003", "ransomware", "initial_access"]
  },
  "agent": {
    "id": "004",
    "name": "wind",
    "ip": "192.168.120.4"
  },
  "manager": { "name": "maple" },
  "id": "1744409102.18523417",
  "full_log": "type=EXECVE msg=audit(1744409102.145:48213): argc=5 a0=\"curl\" a1=\"-sLo\"
  "data": {
    "audit": {
      "type": "EXECVE",
      "command": "curl",
      "exe": "/usr/bin/curl",
      "uid": "1002",
      "auid": "1002",
      "euid": "1002",
      "pid": "28441",
      "ppid": "28440",
      "tty": "pts/0",
      "success": "yes"
    },
```

```
    "user": { "name": "monitadmin" }
  },
  "location": "auditd",
  "decoder": { "name": "auditd" }
}
```


A.2 Rule 100011 — Obfuscated Files / base64 (T1027, T1140)

Fired 7 times (22:06:11 through 22:09:44 UTC) across payload decode, file encode, and rename operations.


```
{
  "timestamp": "2026-04-11T22:06:11.892+0000",
  "rule": {
    "level": 10,
    "description": "Defense Evasion: base64 encode/decode on user-writable path",
    "id": "100011",
    "mitre": {
      "id": ["T1027", "T1140"],
      "tactic": ["Defense Evasion"],
      "technique": ["Obfuscated Files or Information", "Deobfuscate/Decode Files or Inform
    },
    "groups": ["custom", "bt-003", "ransomware", "defense_evasion"]
  },
  "agent": { "id": "004", "name": "wind", "ip": "192.168.120.4" },
  "id": "1744409171.18524001",
  "full_log": "type=EXECVE msg=audit(1744409171.887:48297): argc=4 a0=\"base64\" a1=\"-d\"
  "data": {
    "audit": {
      "type": "EXECVE",
      "command": "base64",
      "exe": "/usr/bin/base64",
      "uid": "1002",
      "pid": "28459",
      "ppid": "28441",
      "success": "yes"
    }
  },
  "previous_output": "Rule 100011 fired 6 prior times this minute (count=7)"
}
```


A.3 Rule 100015 — Credential Access Blocked (T1003)

Fired at 22:08:17 UTC. Note: `success=no` and `exit=-13` (EACCES) confirm CIS hardening held — the read attempt was denied at the kernel layer.


```
{
  "timestamp": "2026-04-11T22:08:17.334+0000",
  "rule": {
    "level": 12,
    "description": "Credential Access: /etc/shadow read attempt BLOCKED (EACCES)",
    "id": "100015",
    "mitre": {
```

```
      "id": ["T1003", "T1003.008"],
      "tactic": ["Credential Access"],
      "technique": ["OS Credential Dumping", "/etc/passwd and /etc/shadow"]
    },
    "groups": ["custom", "bt-003", "ransomware", "credential_access", "blocked", "pci_dss_
  },
  "agent": { "id": "004", "name": "wind", "ip": "192.168.120.4" },
  "id": "1744409297.18525120",
  "full_log": "type=SYSCALL msg=audit(1744409297.329:48402): arch=c000003e syscall=257 suc
  "data": {
    "audit": {
      "type": "SYSCALL",
      "syscall": "257",
      "syscall_name": "openat",
      "success": "no",
      "exit": "-13",
      "exit_string": "EACCES",
      "command": "cat",
      "exe": "/usr/bin/cat",
      "uid": "1002",
      "pid": "28502",
      "key": "shadow_access",
      "file": { "name": "/etc/shadow", "mode": "0000" }
    }
  },
  "cis_control": "PROTECT — /etc/shadow mode 0000 enforced"
}
```


A.4 Rule 100013 — Cron Persistence (T1053.003)

Fired 7 times during the persistence phase (22:11:03 UTC). Only the first alert is shown.


```
{
  "timestamp": "2026-04-11T22:11:03.711+0000",
  "rule": {
    "level": 12,
    "description": "Persistence: crontab modification by unprivileged user",
    "id": "100013",
    "mitre": {
      "id": ["T1053.003"],
      "tactic": ["Persistence"],
      "technique": ["Scheduled Task/Job: Cron"]
    },
    "groups": ["custom", "bt-003", "ransomware", "persistence"]
  },
  "agent": { "id": "004", "name": "wind", "ip": "192.168.120.4" },
  "id": "1744409463.18526544",
  "full_log": "type=PATH msg=audit(1744409463.705:48551): item=0 name=\"/var/spool/cron/mo
  "data": {
    "audit": {
      "type": "PATH",
      "file": {
        "name": "/var/spool/cron/monitadmin",
```

```
        "inode": "1966083",
        "mode": "0100600",
        "owner": "monitadmin",
        "nametype": "CREATE"
      },
      "command": "crontab",
      "exe": "/usr/bin/crontab",
      "uid": "1002",
      "pid": "28621"
    }
  },
  "correlation": {
    "cron_entry": "*/30 * * * * /tmp/.cache-9f3a/stage1.sh >/dev/null 2>&1",
    "impact": "Would re-execute payload every 30 minutes until crontab cleared"
  }
}
```

A.5 Alert summary query (Kibana / Elastic DSL)

The SOC analyst used the following Elasticsearch query in Kibana to reconstruct the full 18-alert sequence during the IR walkthrough:

```
GET wazuh-alerts-2026.04.11/_search
{
  "size": 100,
  "sort": [{ "timestamp": "asc" }],
  "query": {
    "bool": {
      "must": [
        { "term": { "agent.name": "wind" } },
        { "terms": { "rule.id": ["100010", "100011", "100013", "100015"] } },
        {
          "range": {
            "timestamp": {
              "gte": "2026-04-11T22:05:00Z",
              "lte": "2026-04-11T22:12:00Z"
            }
          }
        }
      ]
    }
  },
  "aggs": {
    "by_rule": {
      "terms": { "field": "rule.id" },
      "aggs": {
        "by_technique": { "terms": { "field": "rule.mitre.id" } }
      }
    }
  }
}
```

Result: 18 hits — 2×100010, 7×100011, 7×100013, 2×100015 — exactly matching §3.1.

Annex B — auditd Rule Source for Recommendation R1

Source file for the new auditd rule addressing the T1083 discovery gap (see §8, R1). Target owner: SOC Analyst. Target date: 2026-04-18. Deployment path: `/etc/audit/rules.d/99-bt003-discovery.rules` on all 7 servers (SKY, RAIN, SUN, WIND, OAK, MAPLE, CEDAR).

B.1 Rule file — `/etc/audit/rules.d/99-bt003-discovery.rules`

```
## 99-bt003-discovery.rules
## ------------------------------------------------------------------------
## Purpose:    Detect filesystem discovery (MITRE T1083) — gap identified in
##             IR-001 ransomware incident (2026-04-11) between execution phase
##             (T1059.004, detected) and credential access phase (T1003, blocked).
##             Without this rule, an attacker running `find` to enumerate
##             sensitive files produces no telemetry.
##
## Owner:      SOC Analyst
## Reference:  IR-001 §8 Recommendation R1
## Compliance: PCI DSS 10.2.1, 10.2.5, 10.2.7 · CIS v8 8.5, 8.11
## Deploy:     sudo cp 99-bt003-discovery.rules /etc/audit/rules.d/ \
##             && sudo augenrules --load \
##             && sudo auditctl -l | grep T1083_discovery
## ------------------------------------------------------------------------

## Watch find binary execution. Key 'T1083_discovery' allows Wazuh decoder to
## tag and Elasticsearch to filter.
-w /usr/bin/find -p x -k T1083_discovery
-w /usr/bin/locate -p x -k T1083_discovery
-w /usr/bin/mlocate -p x -k T1083_discovery

## Watch execve syscalls where argv[0] is find/locate. Catches invocations
## via symlinks, $PATH manipulation, or absolute path.
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/find  -k T1083_discovery
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/locate -k T1083_discovery

## Watch syscalls that scan sensitive directories with find-like patterns.
## openat() on /etc, /var/spool/cron, /home, /root by non-root users.
-a always,exit -F arch=b64 -S openat -F dir=/etc           -F auid>=1000 -F auid!=42949672
-a always,exit -F arch=b64 -S openat -F dir=/var/spool/cron -F auid>=1000 -F auid!=4294967
-a always,exit -F arch=b64 -S openat -F dir=/root           -F auid>=1000 -F auid!=4294967

## End of file — immutable flag set by 10-base.rules at boot
```

B.2 Corresponding Wazuh decoder + rule — `/var/ossec/etc/rules/local_rules.xml`

```
<!-- ============================================================================
     IR-001 R1 — T1083 File & Directory Discovery
     Triggered by auditd key 'T1083_discovery'
     ============================================================================ -->
<group name="custom,bt-003,discovery,">
```

```
  <rule id="100020" level="8">
    <if_sid>80700</if_sid>
    <field name="audit.key">T1083_discovery$</field>
    <description>Discovery: filesystem enumeration via find/locate (T1083)</description>
    <mitre>
      <id>T1083</id>
    </mitre>
    <group>pci_dss_10.2.5,pci_dss_10.2.7,gdpr_IV_35.7.d,</group>
  </rule>

  <rule id="100021" level="10">
    <if_sid>100020</if_sid>
    <field name="audit.key">T1083_discovery_etc|T1083_discovery_cron|T1083_discovery_root<
    <description>Discovery: sensitive directory enumeration by non-root user (T1083)</desc
    <mitre>
      <id>T1083</id>
    </mitre>
    <group>pci_dss_10.2.5,pci_dss_10.2.7,</group>
  </rule>

  <rule id="100022" level="12" frequency="5" timeframe="60">
    <if_matched_sid>100020</if_matched_sid>
    <description>Discovery: high-frequency find/locate activity — possible recon (T1083)</
    <mitre>
      <id>T1083</id>
    </mitre>
    <group>pci_dss_10.2.5,pci_dss_11.5,</group>
  </rule>

</group>
```

B.3 Validation procedure

```
# 1. Load the new rules (from ansible or manually per host)
sudo cp 99-bt003-discovery.rules /etc/audit/rules.d/
sudo augenrules --load

# 2. Verify auditd picked them up
sudo auditctl -l | grep T1083_discovery
# Expected: 8 lines (3 watches + 2 execve + 3 openat)

# 3. Verify Wazuh manager loaded the decoder rules
sudo /var/ossec/bin/wazuh-logtest-legacy < /dev/null 2>&1 | grep -c "Rule 100020"

# 4. Trigger and confirm detection
find /etc -name "shadow" 2>/dev/null
# Expected within 30s: Wazuh alert rule 100020 on CEDAR and dashboard

# 5. Confirm PCI/CIS compliance tags on fired alert
curl -s "https://cedar:9200/wazuh-alerts-*/_search" \
  -H "Content-Type: application/json" \
  -d '{"query":{"term":{"rule.id":"100020"}},"size":1}' \
```

```
  | jq '.hits.hits[0]._source.rule.groups'
# Expected: [..., "pci_dss_10.2.5", "pci_dss_10.2.7", ...]
```

Rollback: `sudo rm /etc/audit/rules.d/99-bt003-discovery.rules && sudo augenrules --load`

Annex C — Recommendation ↔ PCI DSS Cross-Reference

This annex maps each IR-001 recommendation (R1–R7 from §8) to the specific PCI DSS v4.0 requirements it satisfies or strengthens. This table is the primary artefact the audit team will use during the 2026-Q3 PCI assessment to demonstrate continuous improvement under requirement 12.10.6.

Rec	Description	Primary PCI DSS v4.0	Secondary PCI DSS v4.0	CIS v8	MITRE	Owner	Target
R1	auditd rule for `/usr/bin/find` (T1083 discovery detection)	**10.2.1** (audit trails for all components) · **10.2.1.2** (access to audit trails)	10.2.2, 10.2.5, 10.2.7, 10.4.1, 11.5.1	8.2, 8.5, 8.11	T1083	SOC Analyst	2026-04-18
R2	Wazuh rule for suspicious `/tmp` file creation (T1491 ransom note detection)	**11.5.1** (change-detection on files) · **11.5.2** (weekly file integrity reviews)	10.2.1, 10.2.1.7, 10.4.1, 12.10.5	3.14, 10.1, 10.5	T1491	SOC Analyst	2026-04-18
R3	Wazuh rule for mass file deletion patterns (T1485 data destruction detection)	**10.2.1.5** (audit use of identification and authentication mechanisms) · **11.5.1**	10.2.2, 10.4.1, 12.10.2	8.2, 8.11, 11.4	T1485	SOC Analyst	2026-04-25

Rec	Description	Primary PCI DSS v4.0	Secondary PCI DSS v4.0	CIS v8	MITRE	Owner	Target
R4	Wazuh active response for automated network isolation on level ≥ 12	**12.10.1** (incident response plan) · **12.10.5** (include alerts from security monitoring systems in IR plan)	1.4.1, 10.4.2, 11.5.1, 12.10.2	13.3, 13.10, 17.5	(enforcement)	Director of Cyber Security	2026-05-02
R5	Auto-ticketing for alerts level ≥ 10 (PagerDuty + tracking)	**12.10.2** (review IR plan annually) · **12.10.5** (24/7 monitoring alerts)	10.4.1, 12.10.4, 12.10.6	17.2, 17.4, 17.9	(process)	IT Manager	2026-05-09
R6	Monthly ransomware tabletop exercises	**12.10.2** (annual IR testing) · **12.10.4** (train IR staff)	12.6.2, 12.10.5, 12.10.6	17.1, 17.4, 17.8	(program)	Director of Cyber Security	2026-05-01 (recurring)
R7	Full DR drill — test complete backup restoration	**12.10.1** · **12.5.1** (inventory of system components)	9.4.1, 11.5.2, 12.10.2	11.4, 11.5, 17.8	(recovery)	IT Manager	2026-06-30

C.1 Reverse lookup — PCI DSS requirement → Recommendations

PCI DSS v4.0	Requirement summary	Addressed by
10.2.1	Audit trails for all system components	R1, R2, R3
10.2.1.5	Audit use of auth mechanisms	R3
10.2.1.7	Audit creation/deletion of system-level objects	R2, R3
10.2.2	Record user / event type / date / timestamp	R1, R3
10.2.5	Audit use of and changes to identification	R1
10.2.7	Audit creation and deletion of system-level objects	R1
10.4.1	Review audit logs at least daily	R1, R2, R3, R4, R5

PCI DSS v4.0	Requirement summary	Addressed by
10.4.2	Automated review tools	R4
11.5.1	Change-detection mechanism on critical files	R2, R3, R4
11.5.2	File integrity monitoring review frequency	R2, R7
12.5.1	Inventory of system components	R7
12.10.1	Incident response plan — create and implement	R4, R7
12.10.2	Review and test IR plan annually	R3, R5, R6, R7
12.10.4	Train IR staff	R5, R6
12.10.5	Include alerts from monitoring systems	R2, R4, R5, R6
12.10.6	Continuous improvement of IR plan	R5, R6

C.2 PCI DSS coverage dashboard (post-remediation target)

Once all 7 recommendations are closed by their target dates, IR-001's remediation program will provide **evidentiary coverage** of the following PCI DSS v4.0 requirements. Each requirement will have an artefact (rule file, Wazuh alert, runbook execution, tabletop report) stored in the audit evidence bundle at `gs://gpus-infra-backups-wdc/audit-evidence/2026/`.

PCI DSS domain	Requirements touched	Evidence type
Requirement 10 — Log and monitor access	10.2.1, 10.2.1.5, 10.2.1.7, 10.2.2, 10.2.5, 10.2.7, 10.4.1, 10.4.2	auditd rule files, Wazuh alert exports, SOC dashboard screenshots
Requirement 11 — Test security of systems	11.5.1, 11.5.2	AIDE reports, Wazuh file-integrity alerts
Requirement 12 — Support infosec with policies	12.5.1, 12.10.1, 12.10.2, 12.10.4, 12.10.5, 12.10.6	IR-001 report, BT-003 report, monthly tabletop summaries, active-response runbook

Audit readiness: When all 7 recommendations are closed, IR-001 + BT-003 + BT-001 together form a complete chain of evidence covering PCI DSS 10, 11.5, and 12.10 for the 2026 assessment cycle.

Document version: 1.1 · Classification: INTERNAL — Audit Evidence · Retention: 7 years per PCI DSS 10.7 · Author: Rajesh Chhetry, Director of Cyber Security · Last updated: 2026-04-11

Changelog: v1.0 (2026-04-11) initial release · v1.1 (2026-04-11) added Appendix A (Wazuh JSON samples), Annex B (auditd rule source for R1), Annex C (R1–R7 ↔ PCI DSS cross-reference)