MONTHLY SECURITY REPORT · REMOTE PLAN

# Syarikat Contoh Sdn Bhd

Reporting period 1 to 31 October 2026 · fictional company, mock data

| PLAN | SITES | MONITORED | PREPARED BY |
|---|---|---|---|
| Remote 24x7 | 2 (HQ, Branch) | 36 sources · 182 endpoints | Daniel T. |

| ALERTS TRIAGED | SLA KPIS MET | INCIDENTS | P1 INCIDENTS |
|---|---|---|---|
| 1,146 | 8 / 8 | 9 | 0 |

SAMPLE

## Summary

- **9 incidents**, none critical: **0 × P1, 2 × P2, 5 × P3, 2 × P4**. Both P2s were contained within 15 minutes of confirmation, and no data loss was found.
- A phishing campaign impersonating LHDN reached 23 mailboxes on 14 October. We quarantined it from all of them within 11 minutes of the first report; 2 staff had clicked, neither entered a password.
- **Action needed:** 14 active accounts, including 2 with admin rights, still sign in without MFA. These are the accounts attackers try first. See recommendation 1.

## SLA scorecard

| KPI | TARGET | RESULT | STATUS |
|---|---|---|---|
| P1/P2 alerts triaged within target | ≥ 95% | 100% (6 of 6) | Met |
| Confirmed P1/P2 notified within target | 100% | 2 of 2 | Met |
| SIEM platform availability | ≥ 99.5% | 99.96% | Met |
| Log sources reporting | ≥ 95% | 99.2% | Met |
| Silent log source flagged to client | ≤ 24 hrs | 1 of 1, 52 min | Met |
| Shift handover logs completed | 100% | 93 of 93 | Met |
| Monthly report delivered | Working day 5 | 06 Nov (day 5) | Met |
| Escalation matrix call-tested | Monthly | 20 Oct | Met |

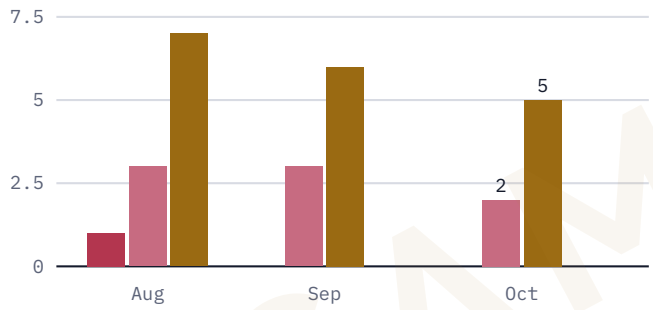
Service credits this month: none. Triage time runs from the alert to an analyst starting work on it. Notification time runs from confirmation to our call to your on-call contact.

## Alert funnel how 52 million events became 9 incidents

| STAGE | OCTOBER | SEPTEMBER | WHAT HAPPENS |
|---|---|---|---|
| Events collected | 52.4 M | 49.8 M | Every log line from the 36 sources and 182 endpoints |
| Alerts raised | 1,146 | 1,390 | Matched a detection rule or threat-intel indicator |
| Closed after AI enrichment and analyst check | 928 | 1,151 | Known-good activity, e.g. backup jobs, approved admin work |
| Investigated in depth | 218 | 239 | Analyst opened a case |
| **Confirmed incidents** | **9** | **11** | **Real security events needing action** |

Alerts fell 18% after we tuned 6 noisy rules in September (backup server, vulnerability scanner, IT admin jump host).

## Incidents by severity last 3 months




P1 P2 P3 P4 not shown (2 in October).

## Response times October

| SEVERITY | COUNT | MEDIAN TRIAGE | TARGET |
|---|---|---|---|
| P1 | 0 | – | 15 min |
| P2 | 2 | 6 min | 30 min |
| P3 | 5 | 38 min | 4 hrs |
| P4 | 2 | 5 hrs | 1 day |

## P2 incidents

| DATE | INCIDENT | TRIAGE | CONTAINED BY | TO CONTAIN |
|---|---|---|---|---|
| 09 Oct 23:17 | Sign-in to a sales mailbox from a VPS provider abroad with a valid session token; attacker read 12 emails | 4 min | DC: revoked sessions, disabled account | 7 min |
| 22 Oct 14:41 | Cracked software with a cryptominer installed on an engineering workstation | 8 min | DC: isolated via Defender | 12 min |

## Containment actions taken

| WHEN | ACTION | AUTHORISATION | LIFTED |
|---|---|---|---|
| 09 Oct 23:24 | Revoke sessions and disable sales.06 | C2 · no call needed | 10 Oct 09:05 by client IT |
| 14 Oct 09:52 | Quarantine "LHDN: Notis Cukai" email from 23 mailboxes | C5 · no call needed | Not reversed |
| 14 Oct 09:55 | Block domain lhdn-semakan[.]example on DNS filter | C4 · no call needed | Still in place |
| 22 Oct 14:53 | Isolate ENG-WS-11 | C1 · no call needed | 23 Oct 11:30 after rebuild |

SAMPLE

## Threats seen blocked or detected in October

| THREAT | OCTOBER | SEPTEMBER | NOTES |
|---|---|---|---|
| Phishing emails quarantined | 284 | 197 | LHDN and courier lures up sharply mid-month, matching a national CERT advisory |
| Password spray / brute-force attempts | 6,410 | 5,880 | Mostly against Entra ID; 0 successful |
| Connections to known-bad IPs blocked | 8,926 | 9,301 | Scanners and botnets; no outbound connections from your hosts |
| Malware blocked by EDR | 17 | 21 | USB drives (11), downloads (6) |

## Log source health

| EVENT | SOURCE | DURATION | CAUSE |
|---|---|---|---|
| Went silent 17 Oct 02:10 | FW-ALG-01 (Branch firewall) | 5 hrs 50 min | Syslog target reset by a firmware upgrade. Client IT restored it; we reviewed the gap from the firewall's local log. |

### Detection coverage

148 active rules covering **94 MITRE ATT&CK techniques** (up from 89). Added this month: OAuth consent phishing, inbox rule hiding, LOLBin download via certutil, Entra ID token replay.

Tuned: 6 rules. Retired: 1 (duplicated by Defender).

### Coverage changes

Added: SRV-HR-02 (new HR system), Mimecast gateway.
Removed: SRV-OLD-FTP-01 (decommissioned).

Total at month end: 36 log sources (6 over the 30 included, billed as one block of 10) and 182 endpoints (one block of 50).

## Risk observations seen in your logs; fixing them is outside our scope

| OBSERVATION | WHY IT MATTERS | COUNT |
|---|---|---|
| Active accounts signing in without MFA | First target of password sprays; 2 have admin rights | 14 |
| Servers still accepting SMBv1 | Used by ransomware to spread | 2 |
| Windows Server 2012 R2 (no longer patched) | Known vulnerabilities will not be fixed | 3 |
| Shared admin account "itadmin" used from 6 PCs | Actions can't be traced to a person | 1 |

SAMPLE

## Recommendations

| # | RECOMMENDATION | OWNER | BY |
|---|---|---|---|
| 1 | Enforce MFA on the 14 accounts listed in Appendix B, starting with the 2 admin accounts | Client IT | 15 Nov 2026 |
| 2 | Replace the shared "itadmin" account with named admin accounts | Client IT | 30 Nov 2026 |
| 3 | Disable SMBv1 on SRV-FILE-01 and SRV-PRN-01 | Client IT | 30 Nov 2026 |
| 4 | Plan migration off the 3 Windows Server 2012 R2 hosts | Client IT Manager | Q1 2027 |

## Requests outside the Remote plan

| DATE | REQUEST | WHAT WE DID |
|---|---|---|
| 22 Oct | Rebuild ENG-WS-11 after the cryptominer | Referred to client IT, with a list of what to check. Rebuilding is not part of the SOC service. |

## Appendix A · Log source coverage register extract, 6 of 36 entries

| SOURCE | TYPE | SITE | CRITICALITY | METHOD | REPORTED |
|---|---|---|---|---|---|
| FW-HQ-01 | Firewall (FortiGate) | HQ | Critical | Syslog TLS, API | 100% |
| DC-HQ-01 | Domain controller | HQ | Critical | Agent | 100% |
| contoh.onmicrosoft | Entra ID | Cloud | Critical | Graph API | 100% |
| contoh.onmicrosoft | Microsoft 365 audit | Cloud | Critical | Management API | 100% |
| MDE-CONTOH | Defender for Endpoint | Cloud | Critical | Defender API | 100% |
| SRV-ERP-01 | Windows server, ERP | HQ | Critical | Agent | 100% |

The full register, and Appendix B (accounts without MFA), are attached as separate locked PDFs each month, because they name users.

## Appendix C · Definitions

| | |
|---|---|
| P1 | Confirmed active compromise, or a threat to a critical system or to large amounts of personal data. Triage 15 min, notify 30 min, contain 60 min. |
| P2 | Likely compromise of one user or host, limited in scope. Triage 30 min, notify 2 hrs, contain 4 hrs. |
| P3 | Suspicious activity, no confirmed compromise. Triage 4 hrs. |
| P4 | Informational or hygiene. Next business day. |

**Prepared by**
Daniel T., SOC Lead
05 Nov 2026

**Reviewed by**
Hafiz R., Service Delivery Manager
06 Nov 2026

AI-assisted: enrichment counts, threat summary and the summary draft, all reviewed by the SOC Lead. Issued as a locked PDF. Editing is disabled; printing and copying text are allowed. Only the copy issued by Dunia Canggih SOC with the reference above is valid. This sample uses a fictional company, fictional people and mock data.

SAMPLE