VIRTUAL CAIM

MANAGED SECURITY AND SOC

Monthly Security Operations Report: October 2026

Prepared for Example Finserv Ltd. (fictional client). Round-the-clock monitoring, detection and response summary for 1 to 31 October 2026.

SAMPLE REPORT - fictional engagement, sanitized

SAMPLE

Report ID	VC-SAMPLE-SOC-2026-10
Client	Example Finserv Ltd. (fictional NBFC)
Reporting period	1 October 2026 to 31 October 2026
Issued	5 November 2026
Service	24x7 SOC monitoring, detection engineering, incident response support
Classification	Confidential (sample). Fictional data throughout.

Document control and scope of service

Prepared by	Virtual Caim SOC (sample)
Reviewed by	SOC Manager and Service Delivery Lead (sample)
Distribution	CISO, Head of IT, Head of Risk, Compliance Officer (named list held in the service agreement)
Monitored estate	58 log sources, 1,240 endpoints with EDR, 2 data centres and 1 cloud region (all India), 3 business-critical applications
Use cases in production	142 detection rules mapped to MITRE ATT&CK, 9 SOAR playbooks
Operating hours	24x7x365, three shifts, Tier 1 and Tier 2 analysts with an on-call incident lead

Contents

1. Executive dashboard 3
2. Alert volume and triage funnel 4
3. Incident summaries 5
4. Detection coverage against MITRE ATT&CK 7
5. Log source health and retention 9
6. SLA performance 10
7. Threat intelligence and exposure 11
8. Tuning actions 12
9. Recommendations and next month 12
Annex. Definitions and conventions 13

HOW TO READ THIS REPORT

Section 1 is written for management and takes five minutes. Sections 2 to 8 are for the security and IT teams. Section 9 lists what we ask you to decide or do. Every metric is defined in the annex so that month-on-month comparison is fair.

SAMPLE

1. Executive dashboard

412.6 M
EVENTS INGESTED
up 6.1% on September

27
INCIDENTS
1 P1, 4 P2, 13 P3, 9 P4

9 min
MEDIAN TIME TO DETECT
September: 12 min

22 min
P1 TIME TO CONTAIN
target 60 min

97.8%
ALERT ACKNOWLEDGEMENT SLA
target 95%

96.3%
RESOLUTION SLA
target 95%

1
REPORTED TO CERT-IN
within 6 hours

0
CONFIRMED DATA LOSS
month total

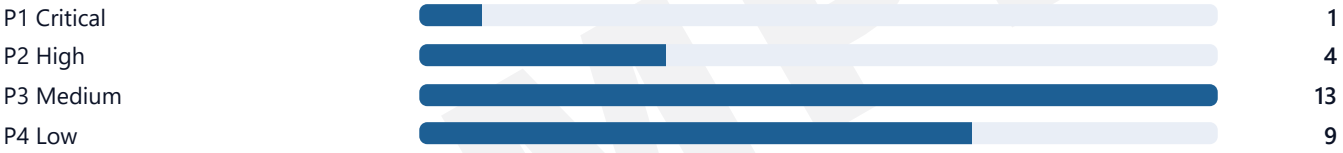
OVERALL POSTURE: STABLE, WITH ONE WATCH ITEM

No incident this month led to confirmed loss of customer data or service. One P1 (phishing leading to a mailbox compromise, INC-2610-004) was contained in 22 minutes from acknowledgement and reported to CERT-In within the 6 hour window. The watch item is credential-based attacks: phishing and password spraying both increased, which supports the multi-factor and conditional access actions in section 9.

Alerts per week



Incidents by severity



Median time to detect, last six months (minutes)



Top detection categories

Category	Alerts reviewed	Share	True positive rate
Authentication anomalies (spray, impossible travel)	1,104	34.4%	23%
Endpoint malware and suspicious execution	688	21.4%	41%
Web application attacks (WAF, application logs)	602	18.7%	19%
Network scanning and reconnaissance	410	12.8%	12%
Data movement and DLP	238	7.4%	37%
Other	170	5.3%	30%

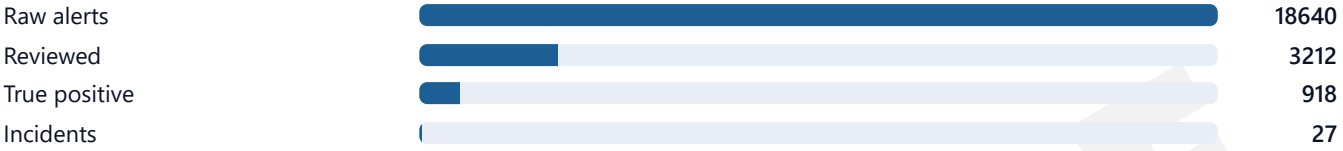
SAMPLE

2. Alert volume and triage funnel

Raw correlation matches are enriched and de-duplicated by SOAR playbooks before an analyst sees them. The funnel below shows how volume reduces to the incidents that needed human response.

Stage	Count	Notes
Events ingested	412,600,000	58 log sources, EDR telemetry, cloud audit logs
Correlation matches (raw alerts)	18,640	142 rules
Auto-closed by SOAR (enrichment, allow-list, known benign)	15,428	82.8% of raw alerts; each closure auditable
Analyst-reviewed alerts	3,212	Tier 1 and Tier 2
True positive alerts	918	28.6% of reviewed
False positive alerts	2,294	71.4% of reviewed (September: 76.0%)
Incidents opened	27	Grouped from related true positives

Funnel view



Alerts by log source family

Source family	Raw alerts	Reviewed	Incidents
Identity and email	5,230	1,104	9
Endpoint (EDR)	4,110	688	8
Network and perimeter	3,870	410	3
Web application and WAF	3,420	602	5
Cloud and data	2,010	408	2

Observations

- False positive share fell by 4.6 points after the tuning actions in section 8, freeing about 35 analyst hours.
- Identity and email telemetry now produces the largest share of incidents. This matches the industry pattern and the priorities in section 9.
- No alert backlog was carried into November.

SAMPLE

3. Incident summaries

Six of the 27 incidents are summarised here: the P1, the P2 incidents and one P3 that carried a lesson. Technical detail for all 27 is in the case management system, available to named client users.

INC-2610-004 Credential-harvesting phishing and mailbox compromise (finance user) Critical

Category	Phishing, unauthorised access (identity theft and phishing; unauthorised access of IT systems and data)
ATT&CK techniques	T1566.002 Spearphishing Link; T1078 Valid Accounts; T1114.003 Email Forwarding Rule
Timeline (IST)	8 Oct 14:12 detection (new inbox rule plus sign-in from an unusual location). 14:19 acknowledged. 14:41 account disabled, sessions revoked, rule removed. 15:30 scope check: 3 other recipients identified, no other sign-ins. 17:25 reported to CERT-In by the client Point of Contact (3 h 13 min after noticing).
Response	Account disabled and password reset. Phishing message removed from 3 mailboxes. Sender domain and link blocked. Affected user retrained. Mail logs reviewed for 30 days: no data transfer beyond the forwarding rule, which had forwarded 6 messages.
Root cause	User entered credentials on a lookalike sign-in page. Legacy authentication was still permitted for one protocol.
Reportability	Reported. Directions of 28 April 2022 require reporting within 6 hours of noticing. Client PoC filed the report with SOC support. The 6 forwarded messages held no customer personal data, and the client's internal personal-data breach assessment recorded that no notification duty arose.

INC-2610-009 Password spraying against the VPN gateway High

Category	Unauthorised access attempt
ATT&CK techniques	T1110.003 Password Spraying
Timeline (IST)	12 Oct 02:40 detection (low-and-slow attempts across 212 accounts from rotating addresses). 02:47 acknowledged. 03:05 source ranges blocked. 03:20 two accounts with weak passwords reset.
Response	No successful sign-in (MFA enforced on all accounts). Attempt volume dropped to zero within the hour. Conditional access rule added for the gateway.
Root cause	Predictable passwords on two service-desk accounts.
Reportability	Assessed as an attempt with no compromise. Logged, not individually reportable.

INC-2610-012 Suspicious script execution on a branch workstation High

Category	Malicious code
ATT&CK techniques	T1204.002 Malicious File; T1059.001 PowerShell; T1105 Ingress Tool Transfer
Timeline (IST)	14 Oct 11:03 detection by EDR behaviour rule. 11:08 acknowledged. 11:15 host isolated. 12:30 forensic triage complete. 15:10 host rebuilt.
Response	Host isolated and rebuilt. Hash and domain blocked tenant-wide. Mail gateway rule updated for the macro-enabled attachment type.
Root cause	User opened an attachment from a spoofed supplier email.
Reportability	Contained at the endpoint with no spread. Logged. No CERT-In report required.

SAMPLE

INC-2610-017 Large upload to personal cloud storage by a contractor account High

Category	Data leak (policy violation, internal)
ATT&CK techniques	T1567.002 Exfiltration to Cloud Storage
Timeline (IST)	19 Oct 16:44 DLP alert (1.2 GB in 9 minutes). 16:51 acknowledged. 17:10 session terminated and account suspended. 18:00 manager contacted.
Response	Contractor access suspended. Uploaded content reviewed with the client: internal project documents, no personal data. Contract reminder issued. DLP rule extended to cover two more storage services.
Root cause	Contractor used personal storage to work from home.
Reportability	Assessed as an internal policy violation with no personal data. Decision rationale recorded by the client Compliance Officer. Not reported.

INC-2610-021 Scanning followed by exploit attempts on a public web server High

Category	Attack on application, targeted scanning
ATT&CK techniques	T1595.002 Vulnerability Scanning; T1190 Exploit Public-Facing Application
Timeline (IST)	22 Oct 20:15 detection (WAF plus web log correlation). 20:22 acknowledged. 20:35 offending ranges blocked. 21:10 patch status of the targeted component verified.
Response	All attempts blocked by WAF. The targeted component was already patched. Rule coverage for the vulnerability family confirmed.
Root cause	Opportunistic internet scanning of a known component.
Reportability	Mass internet scanning is not reported individually. Directions list targeted scanning of critical systems as reportable; this activity was assessed as untargeted. Logged with rationale.

INC-2610-023 Privileged account used outside the change window Medium

Category	Policy deviation
ATT&CK techniques	T1078.002 Domain Accounts
Timeline (IST)	26 Oct 23:20 detection. 23:50 acknowledged. 27 Oct 11:00 confirmed as an emergency change with late approval.
Response	No malicious activity. Change record updated. Resolution SLA missed by 3 hours, waiting on the application owner.
Root cause	Emergency change raised after the work started.
Reportability	No report required. Process improvement noted.

SAMPLE

4. Detection coverage against MITRE ATT&CK

Coverage is measured against techniques that the joint threat model has marked as relevant for Example Finserv (a lending business with retail and agent channels). A technique is Covered when at least one tested rule produces a usable alert, Partial when coverage depends on a single data source or is untested, and a Gap when nothing detects it.

Reconnaissance TA0043 4 covered, 1 partial, 3 gap **56%**	**Resource Development** TA0042 2 covered, 1 partial, 3 gap **42%**	**Initial Access** TA0001 9 covered, 1 partial, 1 gap **86%**	**Execution** TA0002 10 covered, 1 partial, 1 gap **88%**	**Persistence** TA0003 11 covered, 3 partial, 2 gap **78%**
Privilege Escalation TA0004 8 covered, 2 partial, 2 gap **75%**	**Stealth** TA0005 11 covered, 4 partial, 3 gap **72%**	**Defense Impairment** TA0112 5 covered, 1 partial, 2 gap **69%**	**Credential Access** TA0006 10 covered, 2 partial, 2 gap **79%**	**Discovery** TA0007 7 covered, 3 partial, 2 gap **71%**
Lateral Movement TA0008 6 covered, 1 partial, 1 gap **81%**	**Collection** TA0009 5 covered, 2 partial, 2 gap **67%**	**Command and Control** TA0011 7 covered, 2 partial, 1 gap **80%**	**Exfiltration** TA0010 5 covered, 1 partial, 1 gap **79%**	**Impact** TA0040 7 covered, 1 partial, 1 gap **83%**

Weighted coverage counts Partial as one half. Tactics follow the current ATT&CK Enterprise matrix as retrieved in November 2026. Overall: 160 prioritised techniques, 107 covered, 26 partial, 27 gaps, 75% weighted.

75%
WEIGHTED COVERAGE
September: 66%

107
COVERED TECHNIQUES
of 160 prioritised

27
GAPS
down from 33

11
NEW OR IMPROVED RULES
this month

Detail by tactic

Tactic	ID	Prioritised	Covered	Partial	Gap	Weighted %
Reconnaissance	TA0043	8	4	1	3	56%
Resource Development	TA0042	6	2	1	3	42%
Initial Access	TA0001	11	9	1	1	86%
Execution	TA0002	12	10	1	1	88%
Persistence	TA0003	16	11	3	2	78%
Privilege Escalation	TA0004	12	8	2	2	75%
Stealth	TA0005	18	11	4	3	72%
Defense Impairment	TA0112	8	5	1	2	69%
Credential Access	TA0006	14	10	2	2	79%
Discovery	TA0007	12	7	3	2	71%
Lateral Movement	TA0008	8	6	1	1	81%
Collection	TA0009	9	5	2	2	67%
Command and Control	TA0011	10	7	2	1	80%
Exfiltration	TA0010	7	5	1	1	79%
Impact	TA0040	9	7	1	1	83%

Largest remaining gaps and plan

Area	Why it matters	Plan
Reconnaissance and resource development	Mostly outside your network. Visibility depends on threat intelligence.	Brand-abuse and lookalike-domain monitoring added in November
Stealth (log tampering, masquerading)	Attackers hide after initial access	Add audit-policy change and log-clearing rules for 12 server groups
Discovery on endpoints	Early signal of intrusion, but noisy	Behavioural baselines for admin tooling, tested in December
Collection (staging of data)	Precursor to exfiltration	Extend DLP and file-access analytics to the lending database share

SAMPLE

5. Log source health and retention

Source	Type	Avg events per second	Health (month)	Retention (days)	Location	Status
Perimeter firewalls (2)	Network	2,140	99.98%	365	India	OK
Core and branch switches	Network	610	99.90%	180	India	OK
Identity provider and directory	Identity	480	99.99%	365	India	OK
EDR (1,240 endpoints)	Endpoint	3,020	99.70%	180	India	OK
Web application firewall	Web	1,330	99.95%	365	India	OK
Cloud audit logs	Cloud	540	99.95%	180	India region	OK
Email security gateway	Email	260	99.90%	180	India	OK
Core lending application	Application	190	99.60%	180	India	OK
Legacy ERP application	Application	35	98.20%	90	India	Action
Branch router syslog (14 sites)	Network	75	97.40%	180	India	Watch

CERT-IN LOG RETENTION CHECK

The CERT-In Directions of 28 April 2022 require logs of all ICT systems to be enabled and maintained securely for a rolling 180 days within Indian jurisdiction. All monitored sources meet the period except the legacy ERP application, which is set to 90 days. A change request has been raised with the application owner. Time synchronisation was also checked: 56 of 58 sources are within one second of the reference source; two branch routers drifted by 4 to 6 seconds and have been re-pointed to the corporate NTP server, which is itself synchronised to NIC or NPL servers.

Health issues this month

- Branch router syslog: three sites dropped for up to 11 hours because of a link outage. No security-relevant gap identified from other telemetry.
- EDR agents: 14 endpoints out of contact for more than 7 days. IT asked to confirm decommissioning or repair.
- Onboarding: 2 new sources (payments gateway logs, HR system audit logs) are planned for November.

SAMPLE

6. SLA performance

Clocks start when the alert is raised. Acknowledgement means an analyst has taken ownership. Response means containment has begun or a documented decision has been made.

Severity	Acknowledge target	Respond target	Incidents	Median acknowledge	Median respond	SLA met
Critical P1	15 min	60 min	1	7 min	22 min	1 of 1
High P2	30 min	4 h	4	7 min	1 h 12 min	4 of 4
Medium P3	4 h	24 h	13	31 min	5 h 20 min	12 of 13
Low P4	1 business day	3 business days	9	2 h 10 min	1 business day	9 of 9

Service-level summary

Measure	Target	Achieved	Trend
Alert acknowledgement within target	95%	97.8%	Up 1.1 points
Incident response within target	95%	96.3%	Up 0.4 points
Monthly report issued by working day 5	Yes	Yes (5 November)	Stable
Critical alerts handled by Tier 2 within 15 minutes	100%	100%	Stable
Platform availability (SIEM)	99.5%	99.93%	Stable

SLA exception

INC-2610-023 (P3) exceeded its resolution target by 3 hours because the confirmation needed from the application owner arrived the next morning. No security impact. We have agreed a named delegate for out-of-hours confirmations.

Resolution time by severity, median (hours)



SAMPLE

7. Threat intelligence and exposure

Relevant advisories and campaigns

Theme	Relevance to the client	SOC action
Phishing kits targeting financial services sign-in pages	Directly relevant (see INC-2610-004)	Lookalike-domain watchlist, mail gateway rule, user alert issued
Password spraying on remote access	Seen this month (INC-2610-009)	Conditional access review, weak-password audit
Exploitation of internet-facing web components	Scanning observed (INC-2610-021)	Patch verification and WAF virtual patch review
CERT-In advisories received and reviewed	17 advisories this month	9 applicable, 9 actions closed, 0 pending

External exposure snapshot

Measure	September	October	Comment
Internet-facing hosts	46	47	One new host, owner confirmed
Critical or High exposures open	5	3	Two patched; one in change window
Expired or expiring certificates (30 days)	2	1	Renewal booked
Leaked credentials found in monitored sources	4	7	All forced to reset; none linked to a successful login
Lookalike domains registered	2	3	Takedown requests filed

Phishing simulation and reporting

Users reported 214 suspicious emails this month, up from 168. Median time from user report to SOC verdict was 14 minutes.

SAMPLE

8. Tuning actions

Tuning keeps analysts focused on real activity. Each change is tested in a staging mode against seven days of history before release, and rolled back if true positives are lost.

Rule or use case	Issue	Change	False positives before	After
Impossible travel (identity)	VPN exit nodes caused false alerts	Excluded corporate VPN ranges, added device trust check	310	64
Brute-force on VPN	Threshold too low for password spraying	Added per-source and per-account windows	40	12
PowerShell encoded command	Admin scripts flagged	Allow-list signed scripts by hash	188	41
Large outbound transfer	Backup jobs flagged	Excluded backup service accounts with time window	96	18
WAF scanning noise	Duplicate alerts	Grouped by source over 15 minutes	420	95
New admin account	Provisioning flow flagged	Correlated with approved change tickets	52	7
Rare process on server	Patch cycle noise	Maintenance window suppression	126	30
Email forwarding rule (new)	No rule existed	Added after INC-2610-004; 0 false positives to date	-	0

New detections released

- Inbox rule creation with external forwarding (T1114.003).
- Sign-in from a new device after impossible-travel signal, combined with mailbox rule change.
- Cloud storage upload from non-corporate devices to three consumer services.
- Audit policy change and log-clearing on domain controllers.
- Legacy authentication attempts, by protocol.
- Rare parent-child process for Office applications (two variants).

9. Recommendations and next month

#	Recommendation	Why	Owner (suggested)	Priority	Target
1	Disable legacy authentication tenant-wide and enforce phishing-resistant MFA for finance and privileged users	INC-2610-004 root cause	IT and security	High	30 days
2	Raise ERP log retention to 180 days, confirm India-resident storage	CERT-In direction (iv)	Application owner	High	30 days
3	Enforce a password blocklist and review service-desk accounts	INC-2610-009	IT	Medium	30 days
4	Complete EDR coverage on 14 silent endpoints	Coverage	IT	Medium	15 days
5	Add payments gateway and HR audit logs	Coverage of critical applications	SOC and application owners	Medium	45 days
6	Run a tabletop exercise on data breach notification (CERT-In 6 hours, regulator and DPDP process)	Readiness	CISO, Compliance, SOC	Medium	Q1
7	Name an out-of-hours delegate for change confirmations	SLA exception	Head of IT	Low	15 days

Planned for November

- Purple-team exercise on the six highest-priority ATT&CK techniques.
- Two new log sources onboarded.

SAMPLE

- Quarterly service review with the CISO and a refresh of the threat model.

Decisions we need from you

- Approval for conditional access changes on the VPN gateway (recommendation 1).
- Confirmation of the named delegate for out-of-hours change confirmation.

Annex. Definitions and conventions

Term	Definition
Event	A single log record
Alert	A correlation match raised by a detection rule
Incident	One or more related true-positive alerts that require response
MTTD	Median time from first malicious activity visible in logs to alert (measured on incidents with a known start)
P1 to P4	Critical, High, Medium, Low by impact and urgency, agreed in the service schedule
False positive	Alert reviewed and judged not to be malicious or a policy violation
Covered, Partial, Gap	Detection coverage categories used in section 4
SOAR	Security orchestration, automation and response
EDR	Endpoint detection and response
DLP	Data loss prevention
NTP	Network time protocol

All names, systems, incidents and figures are fictional. MITRE ATT&CK is a registered trademark of The MITRE Corporation.

SAMPLE