**🛡️ SECURITY DOCUMENT 🛡️**

**MOMENTUM SPORTS**

*"Built for the Journey"*

**CYBERSECURITY  
INCIDENT RESPONSE  
LOG**

IT Security & Incident Management

FY2025-2026 Incident Log  
Reporting Period: July 2025 - January 2026

**🔒 CONFIDENTIAL - INTERNAL USE ONLY 🔒**

This document contains sensitive security information.  
Distribution limited to: CTO, General Manager, IT Team, Security Committee  
  
• Store in secure location only  
• Do not forward externally  
• Report any security concerns to security@momentumsports.com.au

# EXECUTIVE SUMMARY

This Cybersecurity Incident Response Log documents all security incidents detected, investigated, and resolved during the reporting period July 2025 - January 2026. This log serves as both an operational record and compliance documentation for ISO 27001, SOC 2, and PCI DSS requirements.

## Reporting Period Overview

|  |  |
| --- | --- |
| Reporting Period: | July 1, 2025 - January 15, 2026 (6.5 months) |
| Total Incidents Logged: | 47 incidents |
| Critical/High Severity: | 5 incidents (10.6%) |
| Medium Severity: | 18 incidents (38.3%) |
| Low Severity: | 24 incidents (51.1%) |
| Data Breaches: | 0 confirmed breaches |
| Mean Time to Resolve: | 4.2 hours (target: <8 hours) |

## Incident Categories Breakdown

|  |  |  |
| --- | --- | --- |
| Category | Count | % of Total |
| Phishing Attempts | 15 | 31.9% |
| Failed Authentication | 12 | 25.5% |
| Malware Detection | 6 | 12.8% |
| Suspicious Access Patterns | 5 | 10.6% |
| DDoS Attempts | 3 | 6.4% |
| Data Exfiltration Attempts | 2 | 4.3% |
| Policy Violations | 3 | 6.4% |
| Other | 1 | 2.1% |

## Key Findings & Trends

* Phishing attempts increased 40% compared to previous period, targeting finance and HR staff
* No successful data breaches or confirmed unauthorized data access
* All critical incidents contained within 6 hours of detection
* Employee security training completion rate: 94% (target: 95%)
* Multi-factor authentication prevented 8 account compromise attempts
* Automated detection systems identified 89% of incidents before manual review

## Recommendations

* Increase phishing simulation exercises to twice quarterly (currently quarterly)
* Implement advanced email filtering rules to catch CEO fraud attempts
* Expand security awareness training to include social engineering tactics
* Review and update incident response playbooks based on recent scenarios
* Consider additional SIEM (Security Information and Event Management) capabilities

# INCIDENT CLASSIFICATION FRAMEWORK

## Severity Levels

|  |  |  |  |
| --- | --- | --- | --- |
| Level | Description | Response Time | Escalation |
| CRITICAL | Active breach, data loss, system compromise, ransomware | Immediate (0-1 hour) | CTO, GM, Board |
| HIGH | Failed breach attempt, confirmed malware, account compromise | Urgent (1-4 hours) | CTO, IT Manager |
| MEDIUM | Suspicious activity, policy violation, anomalous behavior | Standard (4-24 hours) | IT Team |
| LOW | Minor issues, false positives, low-risk events | Routine (24-48 hours) | IT Support |

## Incident Categories

|  |  |  |
| --- | --- | --- |
| Code | Category | Examples |
| PHISH | Phishing & Social Engineering | Email/SMS phishing, spear phishing, vishing, pretexting |
| AUTH | Authentication & Access | Failed logins, credential stuffing, unauthorized access attempts |
| MALW | Malware & Ransomware | Virus, trojan, ransomware, spyware detection |
| DDOS | Denial of Service | DDoS attacks, service disruption attempts |
| EXFIL | Data Exfiltration | Unauthorized data access, data transfer anomalies |
| VULN | Vulnerability Exploitation | Attempted exploitation of known vulnerabilities |
| PLCY | Policy Violation | Acceptable use violations, unauthorized software |
| PHYS | Physical Security | Unauthorized facility access, device theft |

## Response Status Codes

**DETECTED:** Incident identified by automated systems or manual report

**INVESTIGATING:** Under active investigation by IT security team

**CONTAINED:** Threat contained, no further spread, investigation ongoing

**RESOLVED:** Incident fully resolved, systems restored, root cause identified

**CLOSED:** Post-incident review complete, documentation finalized

# DETAILED INCIDENT LOG

The following section contains detailed records of all security incidents logged during the reporting period. Each incident includes detection method, investigation findings, response actions, and resolution status.

## INCIDENT #2025-047 [CRITICAL]

|  |  |
| --- | --- |
| CRITICAL SEVERITY - ATTEMPTED ACCOUNT COMPROMISE | |
| Incident Date/Time: | January 8, 2026 - 03:42 UTC |
| Category: | AUTH - Authentication & Access |
| Detection Method: | Automated alert - Microsoft Defender for Identity |
| Affected System: | Microsoft 365 / Exchange Online |
| Target Account: | taylor.singh@momentumsports.com.au (CFO) |
| Attack Vector: | Credential stuffing from botnet (2,847 login attempts from 142 IPs) |
| Source IPs: | Various (Russia, China, Brazil - botnet infrastructure) |
| Successful Logins: | 0 (MFA blocked all attempts) |
| Response Actions: | 1. Account temporarily locked (03:45 UTC) 2. Password reset enforced 3. Geographic blocking rules updated 4. User notified and educated 5. Similar patterns monitored across all accounts |
| Time to Containment: | 18 minutes |
| Data Impact: | None - no successful access |
| Status: | CLOSED - Jan 10, 2026 |
| Lessons Learned: | MFA critical for executive accounts. Credential monitoring services detected CFO password in dark web breach database. Recommended password manager adoption for all executives. |

## INCIDENT #2025-046 [HIGH]

|  |  |
| --- | --- |
| HIGH SEVERITY - CEO FRAUD PHISHING ATTEMPT | |
| Incident Date/Time: | December 19, 2025 - 14:23 AEDT |
| Category: | PHISH - Phishing & Social Engineering |
| Detection Method: | Employee report (Casey Brown, Finance Controller) |
| Attack Description: | Spoofed email impersonating GM (Alex Morgan) requesting urgent wire transfer of $47,500 USD to supplier account |
| Target: | Finance team (Casey Brown, Taylor Singh) |
| Sender Address: | alex.morgan@momentum-sport.com (note: missing 's' in domain) |
| Red Flags: | • Unusual urgency and request to bypass approval process • Slight domain variation • Request to not use normal vendor payment system • Grammar inconsistencies |
| Employee Action: | Casey Brown correctly identified as suspicious and reported to IT without responding |
| Response Actions: | 1. Email domain blocked in Exchange 2. Company-wide security alert sent 3. Finance team reminded of wire transfer approval policy 4. Similar emails identified and quarantined (3 additional attempts) 5. GM's email signature updated with warning about verification |
| Financial Loss: | $0 - No funds transferred |
| Status: | CLOSED - Dec 20, 2025 |
| Lessons Learned: | Employee training effective. Reinforced importance of verifying unusual requests via separate channel. Implemented DMARC policy to prevent domain spoofing. |

## INCIDENT #2025-041 [HIGH]

|  |  |
| --- | --- |
| HIGH SEVERITY - RANSOMWARE DETECTED & CONTAINED | |
| Incident Date/Time: | November 3, 2025 - 10:17 AEDT |
| Category: | MALW - Malware & Ransomware |
| Detection Method: | CrowdStrike Falcon EDR - Behavioral analysis |
| Affected Device: | Laptop - Rowan Mitchell (Marketing Manager) |
| Malware Type: | LockBit 3.0 ransomware variant |
| Infection Vector: | Malicious email attachment (.zip file containing executable disguised as invoice) |
| Files Encrypted: | 23 local files on device (before containment) |
| Network Spread: | NONE - EDR contained before lateral movement |
| Response Actions: | 1. Device quarantined from network (automatic - 4 seconds) 2. Device isolated and powered off 3. Network scanned for indicators of compromise 4. Device reimaged from backup 5. User files restored from SharePoint backup 6. Security training reinforcement for user |
| Data Loss: | Zero - all files recovered from backup |
| Time to Resolution: | 6 hours (device back in service same day) |
| Status: | CLOSED - Nov 4, 2025 |

## INCIDENT #2025-038 [MEDIUM]

|  |  |
| --- | --- |
| MEDIUM SEVERITY - SUSPICIOUS DATA ACCESS PATTERN | |
| Incident Date/Time: | October 14, 2025 - 02:33 UTC |
| Category: | EXFIL - Data Exfiltration Attempt |
| Detection Method: | SIEM alert - unusual data access volume |
| Affected System: | NetSuite ERP - Customer database |
| User Account: | Drew Collins (Business Analyst) - legitimate credentials |
| Anomaly: | Bulk export of 18,485 customer records at 2:33am (outside normal hours) |
| Investigation Finding: | Legitimate activity - analyst working late on quarterly report, exported data for analysis in Power BI. User confirmed and provided business justification. |
| Response Actions: | 1. User contacted and activity verified 2. Export logs reviewed (standard report format) 3. No external data transfer detected 4. Reminded analyst to log after-hours access in advance |
| Data Compromise: | None - authorized activity |
| Status: | CLOSED - Oct 14, 2025 (False positive) |
| Improvement: | Process reminder: Users should notify IT in advance of bulk data exports or after-hours access to reduce alert fatigue |

## INCIDENT #2025-034 [MEDIUM]

|  |  |
| --- | --- |
| MEDIUM SEVERITY - DDOS ATTACK ON E-COMMERCE SITE | |
| Incident Date/Time: | September 22, 2025 - 16:45 AEST |
| Category: | DDOS - Denial of Service |
| Detection Method: | Cloudflare alerts - traffic spike detection |
| Affected System: | Shopify e-commerce store (momentumsports.com) |
| Attack Details: | HTTP flood from 3,200 source IPs targeting product pages |
| Peak Traffic: | 47,000 requests/minute (normal: 800 requests/minute) |
| Attack Duration: | 2 hours 18 minutes |
| Service Impact: | Intermittent slow loading for legitimate users (15-20 second page loads) |
| Response Actions: | 1. Cloudflare DDoS protection engaged automatically 2. Rate limiting rules activated 3. Challenge pages deployed for suspicious traffic 4. Traffic analyzed and blocked by country/ASN 5. Shopify support contacted (confirmed platform-level mitigation) |
| Revenue Impact: | Estimated $3,200 in lost sales during attack window |
| Status: | CLOSED - Sep 22, 2025 |
| Post-Incident: | Enhanced Cloudflare rules implemented. DDoS protection moved to 'always-on' mode. Bot detection improved. |

## COMPLETE INCIDENT SUMMARY TABLE

The following table provides a high-level summary of all 47 incidents logged during the reporting period.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Date | Severity | Category | Description | TTR | Status |
| 2025-047 | Jan 8 | CRITICAL | AUTH | Account compromise attempt | 18 min | CLOSED |
| 2025-046 | Dec 19 | HIGH | PHISH | CEO fraud attempt | 2 hrs | CLOSED |
| 2025-045 | Dec 12 | LOW | AUTH | Failed MFA attempts | 24 hrs | CLOSED |
| 2025-044 | Dec 7 | MEDIUM | PHISH | Credential harvesting email | 6 hrs | CLOSED |
| 2025-043 | Nov 28 | LOW | PLCY | Unauthorized software install | 48 hrs | CLOSED |
| 2025-042 | Nov 15 | MEDIUM | AUTH | Brute force login attempts | 4 hrs | CLOSED |
| 2025-041 | Nov 3 | HIGH | MALW | Ransomware contained | 6 hrs | CLOSED |
| 2025-040 | Oct 29 | LOW | AUTH | Expired password resets | 24 hrs | CLOSED |
| 2025-039 | Oct 21 | MEDIUM | PHISH | Amazon Prime phishing | 12 hrs | CLOSED |
| 2025-038 | Oct 14 | MEDIUM | EXFIL | Suspicious data access | 3 hrs | CLOSED |
| 2025-037 | Oct 8 | LOW | PLCY | USB device policy violation | 48 hrs | CLOSED |
| 2025-036 | Sep 30 | MEDIUM | PHISH | LinkedIn credential phish | 8 hrs | CLOSED |
| 2025-035 | Sep 25 | HIGH | VULN | Critical patch not applied | 4 hrs | CLOSED |
| 2025-034 | Sep 22 | MEDIUM | DDOS | E-commerce DDoS attack | 2 hrs | CLOSED |
| 2025-033 | Sep 18 | LOW | AUTH | Mobile device login anomaly | 24 hrs | CLOSED |
| ... (32 more incidents) | Jul-Sep | Various | Various | Various incidents logged | - | CLOSED |

# INCIDENT RESPONSE PROCEDURES

## Standard Response Workflow

All security incidents follow a standardized response workflow to ensure consistent, effective handling.

**1. DETECTION & IDENTIFICATION**

* Automated detection via security tools (SIEM, EDR, IDS/IPS)
* Manual detection via user reports or security monitoring
* Initial classification of severity and category
* Incident ticket created in IT service management system

**2. CONTAINMENT**

* Isolate affected systems to prevent spread
* Disable compromised accounts or credentials
* Block malicious IPs, domains, or email addresses
* Preserve evidence for investigation
* Notify stakeholders per escalation matrix

**3. INVESTIGATION & ANALYSIS**

* Examine logs and forensic data
* Identify root cause and attack vector
* Assess scope of impact (systems, data, users)
* Document timeline and attacker tactics
* Determine if external notification required (regulatory)

**4. ERADICATION & RECOVERY**

* Remove malware, backdoors, or malicious access
* Apply security patches and close vulnerabilities
* Restore systems from clean backups if needed
* Reset compromised credentials
* Verify systems are clean before restoration

**5. POST-INCIDENT REVIEW**

* Conduct lessons learned session within 48 hours
* Update incident response procedures if needed
* Implement preventive controls
* Share findings with relevant teams
* Close incident ticket with full documentation

## Escalation Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Immediate Notification | Within 4 Hours | Within 24 Hours |
| CRITICAL | • CTO • General Manager • IT Team | • Board Chair • Legal Counsel • External IR firm | • All employees • Customers (if data breach) • Regulators (if required) |
| HIGH | • CTO • IT Manager • Affected dept head | • General Manager • Security Committee | • Executive team |
| MEDIUM | • IT Team • Affected users | • CTO • Dept manager | - |
| LOW | • IT Support | • IT Manager | - |

# METRICS & PERFORMANCE ANALYSIS

## Response Time Metrics

|  |  |  |  |
| --- | --- | --- | --- |
| Metric | Target | Actual | Status |
| Mean Time to Detect (MTTD) | < 15 minutes | 8.3 minutes | ✓ PASS |
| Mean Time to Respond (MTTR) | < 1 hour | 23 minutes | ✓ PASS |
| Mean Time to Contain (MTTC) | < 4 hours | 2.1 hours | ✓ PASS |
| Mean Time to Resolve (MTTR) | < 8 hours | 4.2 hours | ✓ PASS |

## Trend Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Month | Incidents | Critical/High | Trend |
| July 2025 | 5 | 0 | Baseline |
| August 2025 | 6 | 1 | ↑ Slight increase |
| September 2025 | 8 | 2 | ↑ Seasonal activity |
| October 2025 | 7 | 1 | → Stable |
| November 2025 | 9 | 1 | ↑ Holiday phishing |
| December 2025 | 7 | 1 | → Stable |
| January 2026 (partial) | 5 | 1 | → Normal |

## Security Posture Indicators

|  |  |  |  |
| --- | --- | --- | --- |
| Indicator | Current | Benchmark | Assessment |
| Phishing Click Rate | 3.2% | Industry Avg: 4.7% | ✓ Better than avg |
| MFA Adoption Rate | 98% | Target: 95% | ✓ Above target |
| Patch Compliance | 94% | Target: 95% | ⚠ Slightly below |
| Security Training Completion | 94% | Target: 95% | ⚠ On track |
| Password Reuse Detection | 12 accounts | Target: 0 | ⚠ Needs improvement |
| Unencrypted Devices | 0 | Target: 0 | ✓ Compliant |

# RECOMMENDATIONS & ACTION ITEMS

## Priority 1 - Immediate Action (Q1 2026)

|  |  |  |  |
| --- | --- | --- | --- |
| Action Item | Description | Owner | Due Date |
| Phishing Simulation Program | Increase frequency to twice quarterly. Focus on CEO fraud and credential harvesting scenarios. | Rowan Mitchell | Feb 2026 |
| Password Manager Rollout | Deploy 1Password to all employees. Target 100% adoption for executives by March 31. | Charlie Nguyen | Mar 2026 |
| Email Security Enhancement | Implement advanced email filtering and DMARC enforcement to prevent domain spoofing. | Charlie Nguyen | Feb 2026 |
| Security Training Update | Add social engineering and CEO fraud modules to mandatory training. | Finley Adams | Mar 2026 |

## Priority 2 - Near Term (Q2 2026)

|  |  |  |  |
| --- | --- | --- | --- |
| Action Item | Description | Owner | Due Date |
| SIEM Enhancement | Evaluate and implement advanced SIEM capabilities for better threat detection. | Charlie Nguyen | May 2026 |
| Incident Response Tabletop | Conduct tabletop exercise for ransomware scenario with executive team. | Charlie Nguyen | Apr 2026 |
| Vulnerability Management | Implement automated vulnerability scanning and patch management. | Skyler Bennett | Jun 2026 |
| Third-Party Risk Review | Assess security posture of top 10 vendors/partners. | Taylor Singh | Jun 2026 |

## Priority 3 - Strategic (H2 2026)

* Cyber insurance policy review and potential coverage increase
* Security Operations Center (SOC) feasibility study
* Zero Trust Architecture roadmap development
* Advanced threat intelligence platform evaluation
* Business continuity and disaster recovery plan update

# APPENDIX

## A. Incident Reporting Contacts

|  |  |  |
| --- | --- | --- |
| Contact | Role | Contact Method |
| Charlie Nguyen | CTO (Primary) | charlie.nguyen@momentumsports.com.au +61 4xx-xxx-7821 (24/7) |
| Alex Morgan | General Manager | alex.morgan@momentumsports.com.au +61 4xx-xxx-3492 |
| IT Security Team | Security Operations | security@momentumsports.com.au IT Helpdesk: x4357 |
| Employee Reporting | All Staff | phishing@momentumsports.com.au (for suspicious emails) |

## B. Regulatory Notification Requirements

Under various data protection regulations, certain incidents require external notification:

**Australian Privacy Act:** Notifiable Data Breaches (NDB) scheme - notify OAIC within 30 days if likely serious harm

**GDPR (Europe):** Notify supervisory authority within 72 hours of becoming aware of qualifying breach

**PCI DSS:** Notify payment brands and acquiring bank immediately upon suspected card data compromise

**PIPEDA (Canada):** Report to Privacy Commissioner if real risk of significant harm

## C. Security Tools Inventory

|  |  |
| --- | --- |
| Category | Solution |
| Endpoint Detection & Response | CrowdStrike Falcon |
| Email Security | Microsoft Defender for Office 365 |
| Web Application Firewall | Cloudflare |
| Identity Protection | Microsoft Defender for Identity |
| SIEM | Microsoft Sentinel |
| Vulnerability Scanner | Qualys |
| Password Manager | 1Password Teams |
| Backup & Recovery | Veeam |
| Mobile Device Management | Microsoft Intune |

**END OF INCIDENT LOG**

Next Review: April 15, 2026

© 2026 Momentum Sports. All Rights Reserved.

**🔒 CONFIDENTIAL - INTERNAL USE ONLY 🔒**