2025

seceon

Turning 94,000 Threats into 380% ROI:

AI-Powered Security for Australian Finance

Transforming Australian Financial Institutions with AI-Driven, Unified Threat Management for APRA CPS 234 Compliance and Beyond

Executive Summary

Australia’s financial services sector is grappling with an escalating cybersecurity crisis marked by unprecedented frequency and sophistication of cyberattacks. In FY2023-24 alone, over 94,000 cyber incidents were recorded nationwide, with financial institutions accounting for 24% of all targeted attacks. This surge underscores the sector's high-risk profile and the urgent need for robust, coordinated defensive strategies.

In response, the Australian Prudential Regulation Authority (APRA) has introduced the CPS 234 Information Security Standard, elevating cybersecurity from a technical issue to a critical board-level responsibility. The standard imposes direct fiduciary obligations on senior management and boards, mandating proactive risk management, rapid incident response, and continuous assurance of information security capabilities.

To navigate this evolving threat landscape, financial institutions must adopt a holistic and strategic approach to cybersecurity, integrating governance, risk, and compliance with advanced threat detection and response frameworks. Failure to act decisively could result in significant operational, financial, and reputational damage.

The Escalating Cybersecurity Landscape in Australian Finance

1. **Industry-Wide Threat Statistics**
   - 94,000+ cyber incidents in FY2023–24, up 23% year-over-year.
   - 24% of all attacks targeted financial institutions, the single most targeted sector.
   - AUD $8.2M average breach cost for financial institutions.
   - Business impact exceeds AUD $45M per breach when factoring in churn and penalties.
2. **Evolving Attack Methods**
   - **APTs**: State-sponsored campaigns maintaining stealth access for months.
   - **AI-Powered Attacks**: Personalized phishing and malware that bypass legacy detection.
   - **Supply Chain Compromises**: Vendor breaches are spreading across entire ecosystems.
   - **Ransomware 2.0**: Double extortion models targeting banks and insurers.
   - **Fraud & BEC**: 340% increase in business email compromise schemes.
3. **Business Impact**
   - 12% customer attrition following major breaches.
   - Long-term reputational damage is often irreversible.
   - Regulatory penalties under CPS 234 can reach 4% of global revenue.

Why Fragmented Security Approaches Fail

Most Australian financial institutions operate with dozens of disjointed tools:

- 83+ tools from 29 vendors, each with separate dashboards.
- High CAPEX/OPEX due to licensing and staffing costs.
- Rule-based SIEMs produce up to 85% false positives.
- Manual compliance preparation requires weeks of staff hours.

This approach leads to alert fatigue, compliance risk, and higher breach likelihood. In contrast, Seceon’s platform consolidates capabilities into one AI-driven ecosystem.

Seceon’s Unified Cybersecurity Platform

Seceon’s OTM platform is purpose-built for financial services, unifying detection, response, compliance, and analytics in a single solution.

1. **Core Components**
   - aiXDR: Monitors networks, endpoints, cloud, and financial transactions in real time. Detects suspicious payments, ATM/POS anomalies, and insider fraud.
   - aiSIEM: Processes logs from 500+ financial systems, providing CPS 234 dashboards, APRA reporting automation, and risk quantification.
   - aiSOAR: Automates incident response with financial-sector playbooks (e.g., freezing compromised accounts, SWIFT notification automation).
   - aiBAS360: Provides behavioral baselines for employees, customers, and vendors. Detects account takeovers, insider trading, and unauthorized data access.
2. **Technology Differentiation**
   - Predictive AI/ML models for financial fraud and cyberattacks.
   - Unified data model reducing silos and detection delays.
   - Single-pane-of-glass management for streamlined operations.
   - Native CPS 234 compliance automation, including 72-hour breach reporting.

Sector-Specific Applications

The Australian financial services sector is diverse, with each subsector facing unique cyber challenges. Seceon’s platform provides tailored protections that directly address these sector-specific needs.

1. **Major Banks**
   - **Key Challenges:**
     - Continuous onslaught of millions of attempted cyber intrusions each month.

- SWIFT interbank messaging vulnerabilities leading to fraud attempts.
- Legacy mainframe systems integrated with modern digital platforms, creating visibility gaps.
- Increasingly targeted nation-state-backed attacks aimed at destabilizing financial stability.

- **Seceon's Role:**
  - **aiXDR** delivers cross-domain monitoring across core banking, digital platforms, and cloud.
  - **aiSOAR** provides specialized playbooks for SWIFT-related incidents, automating alerts, freezing suspicious transactions, and sending immediate notifications.
  - **aiSIEM** integrates data from legacy systems and modern APIs into a single compliance-ready dashboard.
  - **aiBAS360** builds behavioral baselines for executive accounts and privileged users, identifying anomalous high-value transactions or insider compromise.
- **Outcomes:**
  - 85% reduction in incidents.
  - 380% ROI over three years from fraud prevention and operational efficiency.
  - Improved customer retention and reputation preservation by eliminating high-profile breaches.

2. Insurance Companies

- **Key Challenges:**
  - Manipulation of claims databases to fabricate or exaggerate claims.
  - Theft of actuarial models, pricing algorithms, and proprietary data.
  - Third-party ecosystem risk from adjusters, health providers, and partner systems.
- **Seceon's Role:**
  - **aiBAS360** analyzes claims-processing behaviors to detect fraud rings and suspicious submission patterns.
  - **aiSIEM** continuously monitors sensitive data access in compliance with the Privacy Act 1988.

        - **aiSOAR** automates responses by flagging and isolating fraudulent claim activities in real time.
        - **aiXDR** secures integration points with third-party providers to prevent supply-chain fraud.
    - **Outcomes:**
        - Millions saved annually by preventing false claims.
        - Regulatory compliance is maintained seamlessly.
        - Improved public confidence through demonstrable fraud prevention capabilities.

3. **Superannuation Funds**
    - **Key Challenges:**
        - Long-term custody of member data spanning decades.
        - Member portals targeted by credential-stuffing attacks.
        - Insider threats from employees or third-party administrators misusing sensitive data.
        - Protection of investment trading platforms against manipulation.
    - **Seceon's Role:**
        - **aiBAS360** detects suspicious employee access, unauthorized transactions, and account takeovers.
        - **aiSIEM** ensures regulatory compliance by monitoring data flows across member lifecycle systems.
        - **aiXDR** provides real-time monitoring of investment platforms, protecting against unauthorized access or trade manipulation.
        - **aiSOAR** automatically locks compromised member accounts while alerting administrators.
    - **Outcomes:**
        - 92% improvement in insider threat detection.
        - Protection of AUD $3.5T in assets under management.
        - Stronger member trust through demonstrable data security.

4. **Fintech & Digital Banks**
    - **Key Challenges:**
        - Rapid scaling creates blind spots in security.
        - API-driven environments open to exploitation.
        - Regulatory compliance under AFSL requires agile but strict adherence.
        - Cloud-native infrastructures increase attack surfaces.
    - **Seceon's Role:**
        - **aiXDR** secures APIs, cloud workloads, and mobile banking platforms in real time.
        - **aiSIEM** integrates seamlessly with CI/CD pipelines, ensuring DevSecOps alignment.
        - **aiSOAR** automates breach responses, ensuring no downtime even under attack.
        - **aiBAS360** establishes fraud and anomaly baselines, flagging abnormal customer behavior without disrupting user experience.
    - **Outcomes:**
        - Resilient cloud-native security enabling rapid business expansion.
        - AFSL compliance through automated reporting and monitoring.
        - Maintained agility and innovation without compromising resilience.

Detailed Case Studies

Case studies demonstrate how Seceon's platform delivers measurable business outcomes in real-world financial environments. Each example highlights the specific challenges faced, the Seceon solutions applied, and the tangible results achieved.

Case Studies – Real-World Impact

Case Study 1: Global Credit Union

Context:

A multinational credit union with over 5 million members was struggling with excessive false positives and compliance overheads. With a small SOC team, they were unable to keep up with manual investigations and regulatory requirements.

Challenges:

- Over 100,000 daily alerts, 85% of which were false positives.
- Delays in incident response often take up to 12 hours.
- Heavy compliance burden for cross-border financial regulations

Solution:

The institution implemented a unified monitoring system across branches, ATM networks, and digital banking platforms. Logs from more than 400 sources were consolidated into a single compliance-ready dashboard, while regulatory workflows were automated to ease the burden on SOC teams.

Outcomes:

- Alert fatigue reduced by 85%.
- Incident detection and response time dropped from 12 hours to under 30 minutes.
- Automated compliance reports saved ~2,000 staff hours annually.
- Continuous uptime and breach resilience strengthened customer trust.

Case Study 2: Major Australian Bank

Context:

One of Australia's leading banks, managing billions in daily transactions, was under regulatory and market pressure to modernize its cybersecurity framework. Its legacy tools were fragmented and unable to prevent fraud effectively.

Challenges:

- Increasing fraud through wire transfers and digital channels.
- Compliance with CPS 234 requires breach reporting within 72 hours.
- Rising costs due to overlapping vendor tools.
- High exposure to insider threats.

Solution:

The bank adopted real-time monitoring across high-value transaction systems, including SWIFT, ATM, and mobile banking. Automated playbooks were deployed to freeze suspicious accounts instantly, while behavioral analytics tracked privileged users and third-party vendors.

A compliance dashboard streamlined CPS 234 reporting and APRA notifications.

Outcomes:

- Prevented AUD $91.5M in fraud-related losses within three years.
- Achieved 380% ROI, with payback in less than 6 months.
- 100% adherence to CPS 234 with zero penalties.
- Improved customer retention through stronger transparency and trust.

Case Study 3: Australian Insurance Provider

Context:

A top-tier insurance provider managing millions of policies was targeted by organized fraud rings and insider abuse. Fraudulent claims were increasing at an unsustainable rate, damaging both profitability and reputation.

Challenges:

- Fraudulent claims networks are manipulating claims data.
- Insider access to actuarial and pricing models.
- Difficulty in monitoring third-party partners.

Solution:

Fraudulent claims were identified by analyzing submission patterns across geographies. Integration with actuarial systems allowed tracking of sensitive data usage, while automated investigations flagged high-risk cases for review. APIs connecting to health and partner systems were secured against external exploitation.

Outcomes:

- Organized fraud rings were disrupted within six months.
- Millions saved annually by preventing fraudulent payouts.
- Strengthened compliance with the Privacy Act 1988.
- Fair and transparent claims process enhanced customer trust.

Case Study 4: Superannuation Fund

Context:

A superannuation fund managing assets worth AUD $200B faced challenges in securing member portals and investment platforms while complying with CPS 234.

Challenges:

- Credential stuffing attacks on member accounts.
- Long-term exposure of sensitive member data.
- Insider threats from administrators with privileged access.
- Protection of trading systems against manipulation.

Solution:

Insider activity and account anomalies were continuously monitored. Trading systems and member portals were safeguarded from credential-based attacks, while compliance dashboards generated audit-ready reports. Automated workflows lock compromised accounts instantly.

Outcomes:

- 92% improvement in insider threat detection.
- Prevention of large-scale credential stuffing campaigns.
- Seamless regulatory compliance with minimal manual effort.
- AUD $200B in assets under management safeguarded.

Case Study 5: Fintech & Digital Bank

Context:

A rapidly growing digital-only bank needed to secure its API-driven ecosystem and mobile-first platforms while scaling services nationwide.

Challenges:

- Cloud-native workloads are creating blind spots.
- Compliance requirements under AFSL.
- Customer-facing apps targeted by malware and fraud campaigns.

Solution:

Security was embedded directly into the bank's DevSecOps pipelines, ensuring protection across APIs, mobile platforms, and cloud-native workloads. Automated responses minimized downtime, while customer transaction behavior was continuously analyzed to detect fraud in real time.

Outcomes:

- Enabled secure scaling of services without slowing innovation.
- Seamless AFSL compliance
- Prevented high-profile fraud campaigns targeting mobile apps.
- Stronger competitiveness through uninterrupted, secure customer services.

ROI and Strategic Value

Financial ROI

- Breach prevention saves AUD $8.2M per incident.
- Example: aiXDR flags wire transfer fraud before execution.

Risk Avoidance Value

- aiBAS360 detects insider misuse early, preventing reputational and financial harm.
- Example: Super funds avoid decades-long member data exposure.

Operational Efficiency

- aiSIEM automates reporting, reducing weeks of audit prep to minutes.
- Example: CPS 234 compliance reports are generated instantly.

Regulatory Compliance

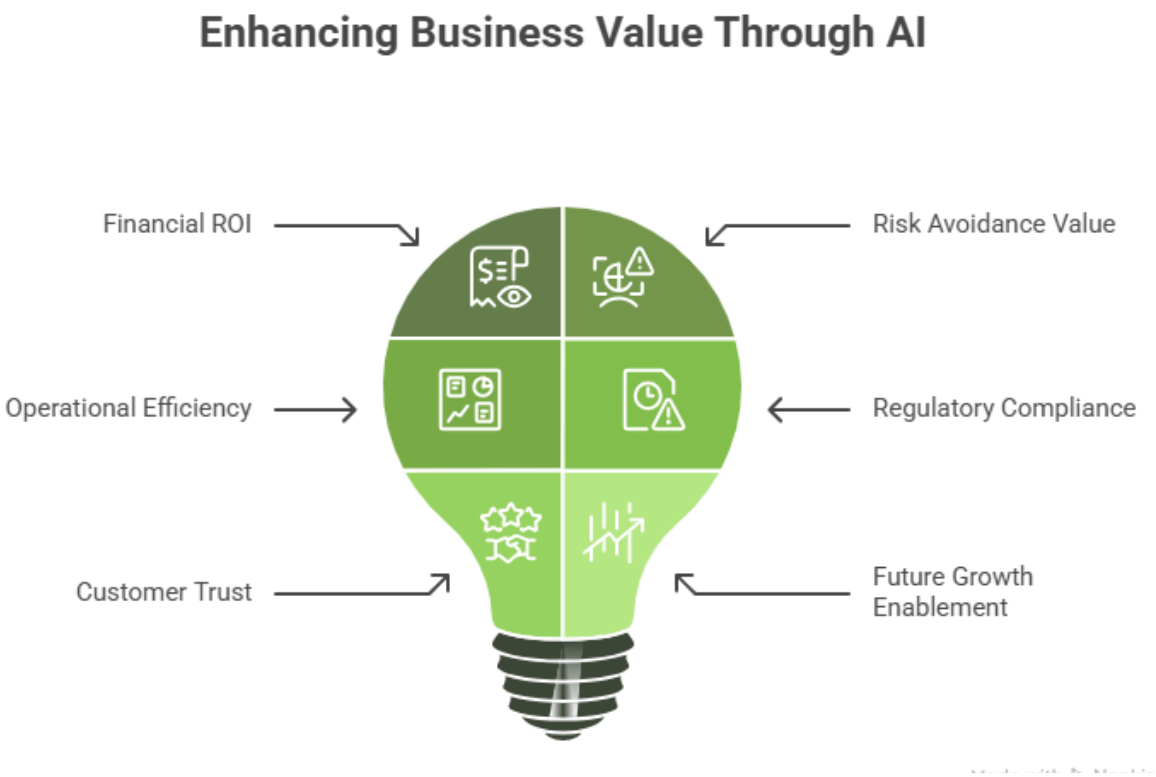
- aiSOAR ensures 72-hour APRA notifications.
- Example: Automated incident workflow prevents fines of up to 4% global revenue.

Customer Trust

- aiBAS360 + aiXDR prevent fraud with 99.8% accuracy.
- Example: Insurers detect fraud early, improving customer retention.

Future Growth Enablement

- Cloud-native scalability supports fintech expansion.
- Example: Digital banks secure open APIs without slowing innovation



Reinventing Cybersecurity in Australian Finance

Leveraging AI to Tackle 94,000 Cyber Incidents and AUD $8.2M Breach Costs

94K+
Cyber Incidents in FY2023-24
+23% Year-over-Year

24%
Of All Attacks Target Financial Institutions

$8.2M
Average Breach Cost for Financial Institutions

$45M+
Total Business Impact Including Churn & Penalties

Critical Challenges Facing the Industry

Fragmented Security
83+ tools from 29 vendors creating operational chaos and blind spots

Alert Fatigue
85% false positives from rule-based SIEMs overwhelming security teams

Compliance Burden
Manual CPS 234 preparation requiring weeks of staff hours

Advanced Threats
AI-powered attacks, APTs, and ransomware 2.0 bypassing legacy defenses

Seceon's Unified AI-Driven Solution

aiXDR
Real-time monitoring across networks, endpoints, cloud, and financial transactions

aiSIEM
Processes 500+ financial systems with CPS 234 dashboards and APRA automation

aiSOAR
Automated incident response with financial-sector playbooks and SWIFT notifications

aiBAS360
Behavioral analytics for employees, customers, and vendors to detect insider threats

380%
ROI Achieved by major Australian bank

85%
Reduction in Security Incidents

92%
Improvement in Insider Threat Detection

99.8%
Accuracy in Fraud Detection

65%
Cost Reduction Through Consolidation

Conclusion – Detailed Analysis

1. **85% Reduction in Incidents:** Unified detection eliminates blind spots, lowering breach volume.
2. **Regulatory Excellence:** Automated CPS 234 compliance ensures institutions stay ahead of enforcement.
3. **Fraud Detection Leadership:** aiBAS360 + aiXDR deliver 99.8% accuracy in fraud detection.
4. **Operational Efficiency**: Consolidation cuts costs by 65%, freeing resources for innovation.
5. **Customer Trust:** Superior security translates to higher retention and valuation premiums.
6. **Future-Ready Growth:** AI/ML-powered adaptability secures digital banking, fintech, and superannuation futures.

Seceon is more than a security vendor; it is a strategic partner enabling Australian financial institutions to excel under regulatory scrutiny while gaining a competitive advantage.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 680 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

References and Citations:

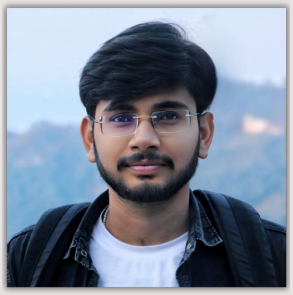
This whitepaper is based on research and data from:

- Australian Cyber Security Centre – Annual Cyber Threat Report 2023–2024
- Reuters – APRA Cyber Risk Warnings
- VBP Australia – Financial Services Cyber Risks
- RiskOnnect – CPS 234 Guide
- Seceon – BFSI Cybersecurity Platform
- CyberMatters – Australian Case Studies
- ThreatConnect – Credit Union Transformation
- Seceon – Case Study: AI & ML in BFSI
- CrowdStrike – Platform Consolidation
- IBS Intelligence – Unified Security in Finance
- Blumira – Finance Cybersecurity Analysis
- VMware – ROI in Financial Services

About the Author

Anand Prasad

AI/ML Cybersecurity Engineer, Seceon Inc.



Anand with expertise in SOC operations, SIEM & XDR platforms, threat intelligence, and incident response. He strengthens enterprise cyber defense, streamlines security workflows, and ensures compliance across IT, OT, IoT, and cloud environments. Passionate about AI/ML-driven security, Anand focuses on reducing risk exposure and delivering measurable ROI.

About the Author

Anamika Pandey

AI/ML Cybersecurity Engineer, Seceon Inc.

Anamika leverages artificial intelligence, machine learning, and Dynamic Threat Modeling (DTM) to fortify IT, OT, IoT, and cloud infrastructures. Her expertise lies in advancing AI-driven defense strategies that not only ensure compliance and resilience but also deliver measurable ROI. Through Seceon's OTM Platform, she helps organizations anticipate, detect, and mitigate evolving cyber threats—empowering them to stay secure, adaptive, and future-ready.