Borderless CS
CYBER SAFE TOGETHER

CYBER SECURITY RECRUITMENT

Managed Security Operations Centre (SOC)

Customer success story

CLIENT: **CYBER SECURITY RECRUITMENT**

INDUSTRY: **HUMAN RESOURCES**

CLIENT WEBSITE: **HTTPS://CYBERSECURITYRECRUITMENT.COM.AU**

SERVICE: **MANAGED SECURITY OPERATIONS CENTRE (SOC) SERVICES**

Managed Security Operations Centre - Customer Success Story

Client Overview:

Cyber Security Recruitment is a specialised recruitment and workforce solutions provider focusing exclusively on the cybersecurity industry. With a portfolio of over 3,000 screened candidates, hundreds of enterprise clients, and partnerships with universities and government initiatives, CyberSecHire plays a critical role in solving Australia's cyber skills shortage.

Their services include:

- Executive search for CISO, GRC, and Red Team roles
- Contract staffing and SOC analyst placement
- Graduate hiring through university and TAFE alliances
- Resume marketplace and industry job board platform

With growing data volumes, high client expectations, and expanding digital infrastructure, CyberSecHire required enterprise-grade cybersecurity that could match the industries it serves.

The Business Problem

Despite being a security-focused business, CyberSecHire faced increasing cyber risks:

1. High-Value Data Target

CVs, employment records, reference checks, and onboarding documents were stored in their CRM and applicant tracking systems. Exposure would compromise candidate confidentiality and harm employer trust.

2. Credential Harvesting and Impersonation Attempts

The brand became a target of phishing campaigns using spoofed email domains, aiming to trick jobseekers and HR contacts into sharing sensitive information or downloading malware.

3. Recruitment Platform Security

With a SaaS job board and client dashboard integrated into Microsoft Azure and Microsoft 365, CyberSecHire needed:

- Secure access control
- Continuous vulnerability monitoring
- Zero-day alerting

4. Compliance Requirements for Government Clients

To win government or defence-sector recruitment contracts, the firm had to prove cyber maturity through frameworks like **ISO 27001**, **NIST CSF**, **Essential Eight**, and **GDPR**.

The Solution: SOC-as-a-Service by Borderless CS

Borderless CS implemented a **tailored, fully managed Security Operations Centre (SOC)-as-a-Service solution** that aligned with the firm's operational model, regulatory pressures, and reputation needs.

1. **24/7 Threat Monitoring & Detection**
   - Integrated logs from:
     - Microsoft 365
     - Recruitment SaaS platform
     - Web application firewall (WAF) and load balancers
     - Endpoint agents on staff and contractor devices
   - SIEM correlation rules tuned for:
     - Suspicious login patterns (Foreign IP, no MFA)
     - Large file exports from recruitment dashboards
     - Brute force attempts or excessive failed logins
     - Use of outdated or revoked credentials
2. **Identity & Access Management (IAM) Security**
   - Azure Entra ID Conditional Access and Identity Protection deployed
   - Privileged accounts segmented (Recruiters vs admins vs contractors)
   - Risky sign-in alerts connected to Borderless CS's SOAR platform for automated investigation
3. **Email Security and Brand Spoofing Prevention**
   - Defender for Office 365 and SPF/DKIM/DMARC setup
   - Simulation of phishing campaigns for staff training
   - Monitoring for registered lookalike domains attempting impersonation.

4. **SOC Dashboards and Board Reporting**
    - Monthly threat intelligence briefs for the executive team
    - Compliance reporting aligned with NIST CSF categories
    - Risk heat maps and detection trends by user, endpoint, and cloud system.

5. **Incident Response Playbooks & Rapid Containment**
    - Pre-built playbooks for:
        - Credential leakage
        - Suspicious email forwarding rules
        - Suspicious mass CV download by recruiters
    - Response actions included user lockdown, token revocation, and geo-blocking within 15 minutes of confirmed detection

The Results

Enhanced Security Posture and Client Confidence

- Successfully passed cyber due diligence by four enterprise clients and two public sector agencies
- Used SOC capabilities as a differentiator during proposal submissions

Reduced Risk of Data Breach

- Over 1,200 potential phishing emails blocked in the first 90 days
- 5 credential harvesting attempts detected and mitigated before exploitation
- Hardened cloud infrastructure with Zero Trust principles applied across all systems

Business Growth and New Contract Wins

- Enabled the firm to bid on high-value cyber recruitment tenders requiring evidence of 24/7 security monitoring
- Supported the onboarding of multiple high-profile clients from the financial services and health sectors

Compliance & Assurance

- Monthly reports provided assurance to Cyber Security Recruitment's insurance provider, reducing premiums
- Supported ongoing internal alignment with **ISO 27001** policies for future certification readiness

SOC Technology Stack

- Borderless CS SIEM & SOAR platform
- Microsoft 365 Defender Suite
- Azure Entra ID Integration
- Endpoint Detection & Response (EDR)
- Threat Intelligence & Domain Monitoring
- Secure Email Gateway (SEG) with DKIM/SPF/DMARC
- File Integrity Monitoring and Vulnerability Assessment
- Malware Detection Module

Why This Partnership Matters

Recruitment firms working in cybersecurity must demonstrate operational integrity, data protection, and proactive threat management. **Borderless CS enables this through its enterprise-grade SOC platform**, adapted for mid-sized firms who want big-league protection without building an in-house SOC.

Together, we're not just protecting systems — we're safeguarding careers, candidates, and the future of Australia's cybersecurity workforce.

Explore SOC Services for Your Industry

Whether you're a recruitment firm, consulting agency, or HR-tech provider, **SOC-as-a-Service from Borderless CS** delivers:

- Fast deployment
- Continuous monitoring
- Trusted advisory
- Proven risk reduction