Classida

Abnormal AI

An Evidence Based Approach To AI driven email Security

Local Government Council - Victoria

Executive Summary

A Local Government Council in Victoria, Melbourne, undertook a Proof of Value (POV) engagement with Abnormal AI to assess the effectiveness of its existing email security stack, comprising a legacy Secure Email Gateway (SEG) and Microsoft 365 native defences, against modern, socially engineered attacks.

Over the course of the engagement, Abnormal AI retrospectively analysed four weeks of historical mail flow via API integration. Within days, Abnormal AI uncovered a wide range of advanced email threats, including credential phishing, business email compromise (BEC), vendor impersonation, and internal account compromise, that had bypassed existing controls and reached user inboxes.

> The results were compelling: Abnormal AI detected over 400 advanced threats missed by their legacy SEG, many of which had passed all standard authentication checks (SPF, DKIM, DMARC). Following the success of the POV, the council made the decision to move to full production.

Environment Overview

Email Platform
Microsoft O365 E3 & E5 licensing

Email Security Stack
Legacy SEG + Microsoft Native Protection

Email Inboxes
1300+

POV Objectives
Visibility into bypassed threats, zero-day protection, internal account compromise detection, SOC workload reduction, SEG replacement justification

Key Outcomes from the POV

- 400+ advanced threats uncovered in historical email traffic
- Zero disruption to mail flow or user experience
- Over 99% reduction in false positive investigations from user-reported emails
- Instant removal of malicious messages with automatic remediation
- Confirmed evidence of credential phishing and MFA bypass attempts
- Detection of compromised internal accounts and inter-council spoofing
- Full SOC workflow optimisation with automation of triage and prioritisation

Threats Missed by Legacy SEG

Credential Phishing

Phishing emails using legitimate Microsoft login portals and proxy sites to steal user credentials and bypass MFA.

BEC and Executive Impersonation

Highly targeted messages impersonating finance and executive teams to trick staff into action.

Vendor and Domain Spoofing

Attackers mimicking trusted vendors and other councils, exploiting inter-council trust relationships.

Internal Threats

Compromised internal accounts were used to distribute phishing campaigns within the organisation.

These threats were often invisible to static and rules-based detection methods, passing all authentication checks and containing no known malware.

Abnormal AI Security Impact

SOC Workflow Improvements

Automated Prioritisation

Abnormal AI triaged user-reported emails, flagging only high-risk messages, reducing manual investigation time significantly.

Noise Reduction

Over 99% of user reported emails were identified as safe by Abnormal and automatically deprioritised, reducing manual triage and alert fatigue

VIP Targeting

High-risk users such as finance and C Level executives were auto-prioritised for SOC Visibility.

Inline & Retrospective Detection

Threats missed by legacy SEG were identified via both lookback and live detection.

Instant Remediation

Confirmed malicious emails missed by the SEG were removed from all affected inboxes with a single click.

Security Posture Management

Abnormal AI also provided visibility into OAuth app risks, identity anomalies, policy changes, and privilege escalations, strengthening the council's overall Microsoft 365 posture.

Why Local Councils Should Run a POV

- Uncover live threats missed by legacy SEG systems
- Identify lateral threat movement and inter-council spoofing
- Validate and improve SOC efficiency
- No operational risk – no changes to MX records or user workflow
- Deploys in minutes via API

Next Steps

The Abnormal AI POV is a no-obligation, API-based deployment that can be deployed in under 10 minutes and an analysis completed in days. It provides real-time evidence of gaps in existing defences using your council's actual environment and mail flow.

Running a POV will allow other councils to

- See what threats are in inboxes right now
- Quantify risk exposure with real metrics and attack types
- Present an internal business case for replacing or augmenting legacy SEG

Why Partner with Classida

Classida successfully delivered and supported this POV in a complex local government environment. With deep experience in email security and public sector workflows, Classida helps councils deploy Abnormal AI quickly and extract maximum insight and impact from the engagement.

Securing the Future

The increasing sophistication of email threats, and their ability to exploit public sector trust networks, demands a modern, AI-native behavioural defence strategy. This case shows that traditional SEG's and Microsoft defences alone are no longer enough.

By running a POV with Abnormal AI & Classida, councils will gain immediate visibility into what threats are being missed, reduce operational overhead, and build a strong case to present to council executives to improve protection across their organisation and community.

Get in Touch

info@classida.com.au
ABN: 71604032912
Melbourne, Australia