Staying ahead in a rapidly evolving threat landscape

→ Anna Webb

Head of Global Security Operations | Kocho

Kocho

BECOME GREATER

Introduction

Who am I?

- → Head of Global Security Operations at Kocho
- → Passionate about cyber security and building resilient security operations for clients

Why this session matters?

- → The evolving cyber threat landscape
- → Attackers are adapting
- → How we can proactively address these challenges

What we'll cover today

- → Recent breaches and threat trends
- → Evolving Social Engineering
- → Kocho SecOps strategies and solutions

Anna Webb

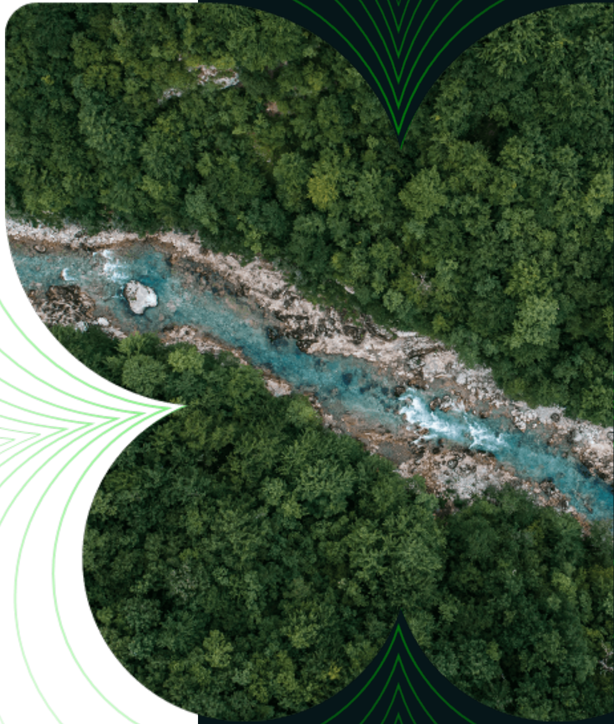
Head of Global Security Operations

A wake-up call – Recent breaches

M&S - April 2025 – Ransomware attack
Nationwide disruption
Customer data exposed

Co-Op Group – April 2025 – Cyberattack
Internal Systems Disrupted – logistics and stock-ordering
Personal data of Co-Op Members

Harrods – April/May 2025 – Unauthorised activity
No disruption to customer-facing services
No confirmed data breach



Live from the Kocho SOC – Threat Trends

Phishing quality over quantity

- → Traditional mass phishing is declining
- → AI-Powered phishing
- → Business Email Compromise (BEC)

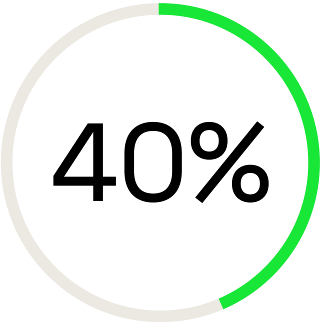
Token Theft

- → How passwords are no longer the target
- → MFA Fatigue and exploitation
- → HTTP Clients used to replay stolen OAuth tokens

Improved Social Engineering Tactics

- → Unusual delivery methods - Fake CAPTCHA
- → Trusted Sources – suppliers & internal staff
- → Taking time to understanding the target better

Identity - Still the number 1 target



40% Rise in Identity incidents in Q1 2025 (Microsoft)

99% of attacks involve identity (Microsoft)

Rise of high-quality, targeted attacks

- → Attackers now invest more effort in reconnaissance and social engineering, leading to more convincing phishing lures.
- → Comprised Credentials
- → Consent phishing
- → Legacy Authentication

Quick Wins – how can we look to protect

- → Conditional Access
- → Block legacy authentication

BECOME GREATER
KOCHO.CO.UK

Evolving social engineering

Deepfake Audio and Video

- → AI-Generate voices and videos used to impersonate people we know
  - → CEO voice cloned to approve a fraudulent payment

QR Code Phishing (“Quishing”)

- → QR Codes being used in everyday scenarios
  - → Malicious QR Codes lead to spoofed login pages
  - → Bypasses email link filtering

AI Chat Scams

- → AI-Powered chat bots being exploited
  - → Mimic customer service, recruitment teams or even internal IT support
  - → Dangerous in high-stress situations – time is key, and guard is down

Defensive Tactics – how can we look to protect

- → Training
- → Simulations
- → Culture change – Security First

Smarter attackers need smarter defenders

Living-off-the-land (LOTL)

- Attackers using built in system tools
- Blends into NORMAL system activity

Supply chain abuse

- Attackers are compromising trusted vendors and software providers
- You can have a strong perimeter – but a weak link in your supply chain can still open the door

Chained misconfiguration exploits

- Attackers are combining vulnerabilities
- Like a death by a thousands paper cuts – attackers are getting better at stitching those cuts together

Living-off-the-land (LOTL)

- Restrict script execution
- Monitor for unusual use Admin tools - use advance threat detection

Supply chain abuse

- Vet 3rd parties carefully
- Enforce least privilege for partner access and MONITOR 3rd party integrations

Chained misconfiguration exploits

- Conduct regulate config reviews
- Use tools to support - Defender for Cloud or Compliance Manager
- Align to frameworks like NIST or CIS for baselines

Predictions

- End Users will remain the #1 entry point
  - Phishing will continue evolving to bypass security controls
  - More AI-assisted threats
- Social Engineering will adapt
  - More fake CAPTCHAs and other browser-based tricks will increase
  - SMBs will be targeted via supply chains
- Attackers will play the long game
  - Lay dormant, staying undetected for weeks or months.
  - Understand business workflows before striking.
- Identity posture is going to be in focus for more businesses
- Increased pressure from NIS2 and DORA - Security is no longer just an extension of IT

Kocho SecOps: Making cyber risk clearer for the Board

ClearVue

Real-time PowerBI reporting provides a single pane of glass to C-Level and technical teams.

→ Get detailed breakdowns of the threats in your environment

→ See risky sign-ins by user and location at a glance

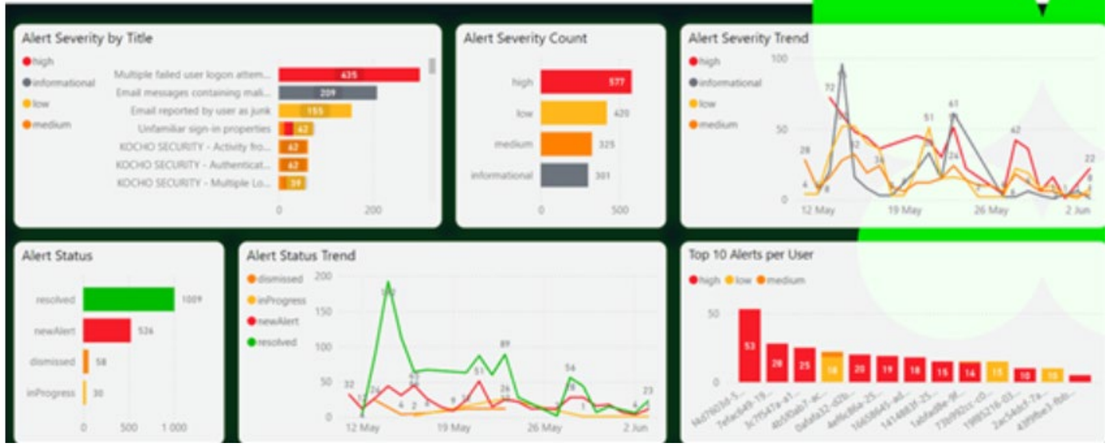
→ Understand risky devices and software gaps in your system

→ Receive recommendation for security posture improvements

The Visible SOC with ClearVue™

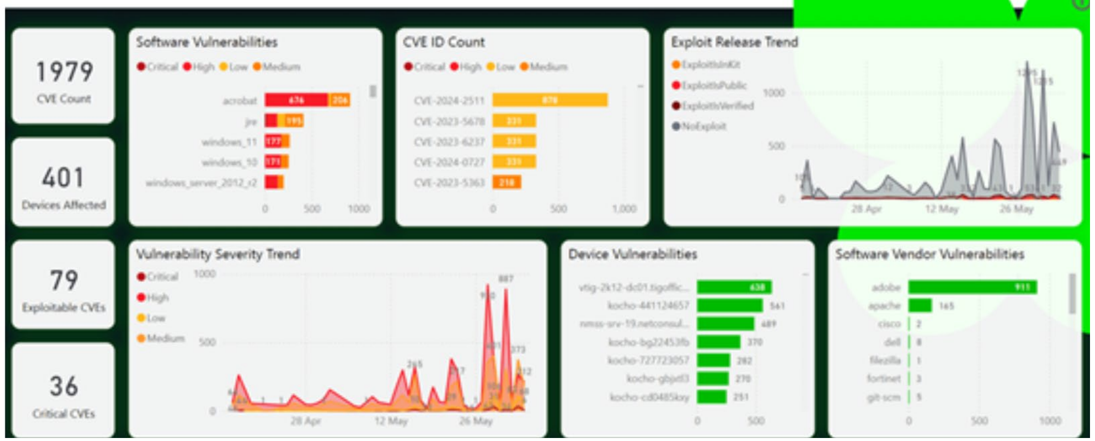
Alert Status Summary

Includes information from Microsoft 365 Defender and Sentinel with the focus on the Status and Severity of the events that occurred in the past month.



Software Vulnerability Summary

Shows software vulnerability information reported by Defender for Endpoint and includes counts of verified exploits and their severity.



BECOME GREATER
KOCHO.CO.UK

Takeaways and practical actions

→ **Review Identity strategy** - MFA, Legacy auth, Conditional Access

→ **Educate Staff** - phishing and social engineering in general

→ **Tune detection rule** – are you see the wood for the trees?

→ **Build board -friendly reporting** - make it easier to get that support

→ **Use your SOC as a strategic partner** - they should be your strongest arm not your weakest link