Protecting citizens & consumers online

Andrew Bud

CEO & Founder, iProov

Company Overview

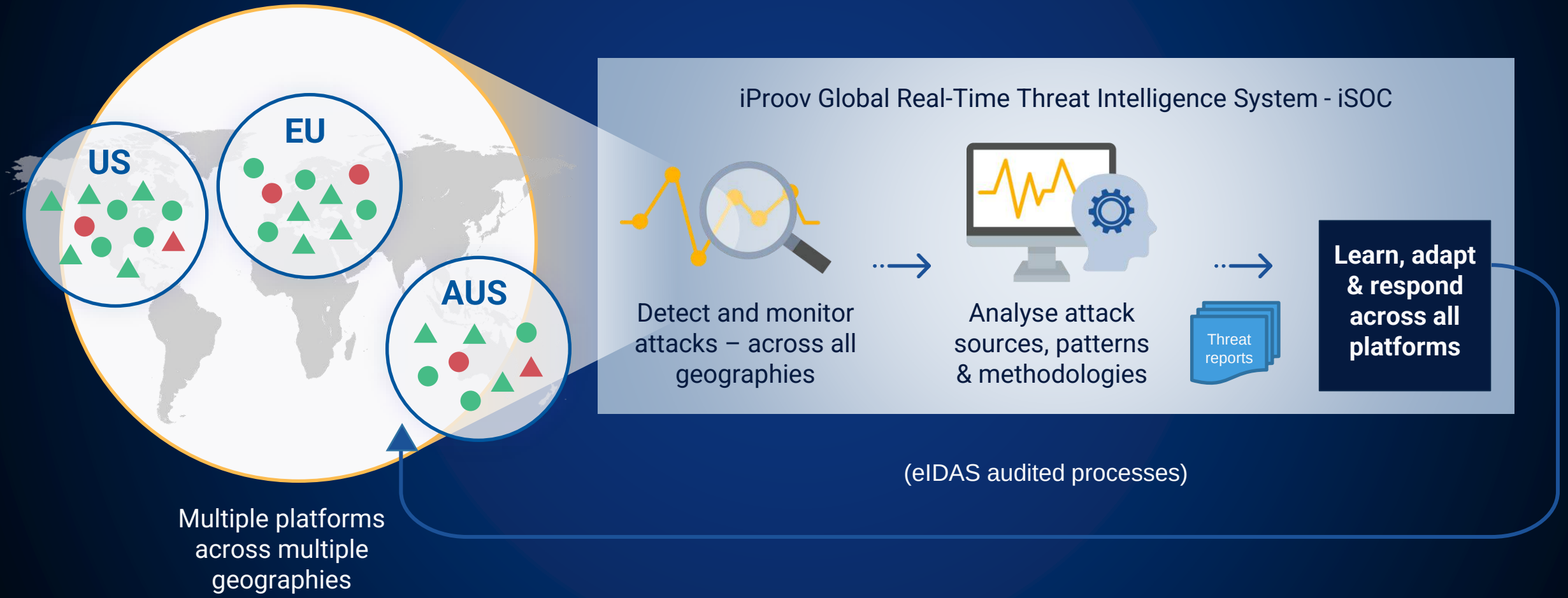
Andrew Bud CBE FREng FIET

- Founder and CEO of iProov
- Professional Engineer
- Serial entrepreneur
- Former chair of ETSI committees
- Former chair of UCL External Advisory Council on Computer Science

About iProov

- Founded in London in 2011
- 170 staff in UK, Netherlands, US, Singapore
- We provide the only means by which an online user is verified as the right person, a real person, and, critically, that they are authenticating right now, using advanced biometrics (Genuine Presence Assurance)

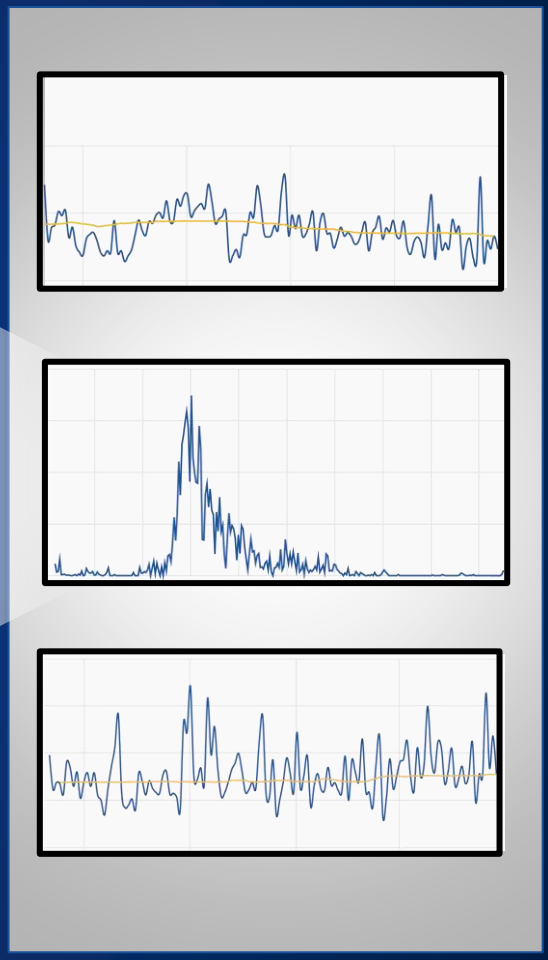
iSOC: Sourcing Biometric Threat Intelligence



Observed Threat Patterns: 2022

5X More

Digital Injection vs. Presented Attacks



Presentation attacks (ex. masks)

Presented mask attacks only

Digital injection attacks

2022 Key Trends

1 Evolution of Digital Injection Attacks

- Massive rise in the use of emulators across mobile web, native Android & iOS
  No platform is safe
- Criminals are getting much better at spoofing metadata
- Significant rise in quality of imagery used in attacks

650% Increase

Launched from desktop web, posing as mobile web, android and iOS native H2 vs. H1 2022

2 Emergence of Novel Face Swap Attacks

- Digitally injected face swaps use **real** identities that can be difficult for systems to spot, and near impossible for humans
- The rise of face swap attacks indicates that low-skilled criminals now have access to technology to launch advanced attacks

178% Increase

H2 vs. H1 2022

3 Global, Indiscriminate Attacks at Scale

- Non-targeted attacks are being launched at platforms and systems worldwide simultaneously
- Attacks are motion-based meaning active verification technology is highly vulnerable

100-200 within 24hrs

Simultaneously Launched Automated DIA Verification Attempts 3 X Per Week Worldwide

No Compromises In User-Centric Security Policy

Inclusion through user choice:
- No imposition or requirement for special device hardware or sensors
- Ability to securely authenticate on any device with a user-facing camera

Device risk mitigation:
- No reliance on users' device for security
- Mitigate risk from synthetic or compromised devices

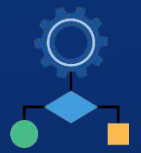
Verification integrity:
- Use inaccessible processing to prevent reverse engineering by attackers
- Mitigate threat of adversarial attack

Agile response:
- Ongoing threat intelligence to evolve defences

Inclusion through accessibility:
- Device & platform agnostic to include all users
- Robust performance and bias monitoring
- Cloud-based delivery

Robust choice pathways:
- Non-biometric enrolment option must be equally secure…
- …even if convenience is sacrificed

Identity recovery:
- Users should not be required to re-enrol when devices are changed or replaced



Relieve users of burden of responsibility:
- Implementation of new detection algorithms must not rely on or compel the user to update their personal device

Thank you

Genuine Presence Assurance

Right person, Real person, Right now