CLARITAS

# ARGUS

## Your defence against phishing attacks and unauthorised access.

**Phishing attacks involved tricking a victim into taking some action that benefits the attacker. These attacks range from simple to complex, and can be spotted with the right awareness.**

Human error and complacency inside an organisation are the biggest source of risk, prompting cyber attackers to focus on human weaknesses as well as complex technical attacks. As a result, phishing remains the number one type of cyber attack, accounting for 84% of business breaches according to the National Cyber Security Breaches Survey 2024.

**ARGUS automates the SOC process to provide the two things a CISO desperately needs in order to mitigate this specific risk; Confidence and Visibility.**

## Our ARGUS solution helps to mitigate this risk by establishing patterns of user behaviour and alerting discrepancies likely to be the result of stolen credentials or access tokens, much like your bank does if you make unusual transactions.

Organisations have moved to Cloud deployments of back office systems that are accessed from any WiFi access point, often using a personal device and from any location. In this context CISO's, Operations Directors and IT Directors can mitigate their security risk by hardening endpoints, requiring VPN's and enforcing Identity Access solutions. However, these are technical solutions, which is why attackers focus on the human vulnerabilities via phishing.

Many companies adopt a security posture that relies on Cloud providers to underwrite their data and application security. But as the majority of attacks do not breach the Cloud provider security - they use valid user credentials and access tokens - which even large SIEM and SOC management solutions do not prevent. There may be a delay between a successful phishing attack and any stolen credentials being used so it won't be obvious that an accidental click on a rogue email presents a substantial risk to the organisation.

### Confidence

Our AI core learns normal user patterns based on key signals and indicators which cannot be spoofed by an attacker combined with an understanding of user behaviour and their connected devices. RoboSOC / vSIEM Analyst analyses from the network up to understand each user's behaviour and devices across multiple cloud platforms. RoboSOC/vSIEM can take automatic action to reset a user's access to your cloud platforms, requiring the user re-authenticate, or force the user though a password change process if credentials have been stolen. The machine learning of user patterns combined with automated alerts and response ensure malicious activity is halted and the dominant threat to your data and reputation is neutralised.

### Visibility

Modern organisations have users who travel frequently, or employees in many different countries. ARGUS provides visibility of who is accessing your cloud platforms and from where, through regular reporting on activity and immediate alerting when something suspicious or malicious is detected. If it is a hacker, they will not be able to gain access and will not see the password reset option even in a man-in-the-middle attack.


**To learn more about ARGUS, please contact:**
**sales@claritasinsight.com**

**www.claritasinsight.com**