CELERITY

security | integrity | agility

TIME IS MONEY WHEN YOUR NETWORK IS BREACHED

It can take 197 days on average for an organisation to detect a cyber-attacker in their system. The longer attackers are in your network the more damage can be caused and the longer it can take for your business to recover.

The average organisation faces **200,000** security events a day

Lack of resources

Findings show that only 10% of the IT budgets are spent on cyber security and as a result of this, companies don't have the necessary resource to overcome key cyber challenges.

Compliance pressures

GDPR compliance has been an ongoing stressor for organisations managing data and now that the Information Commissioners Office (ICO) has begun delivering record-breaking fines (£183m to British Airways) to organisations who have suffered a data breach due to a cyber-attack, the compliance pressure continues to mount for businesses.

Lack of visibility

IT managers need to have clear insight to overcome cyber threats. Manual tasks and human error increase the risk of cyber breaches. You can't defend against what you can't see.

Budget restrictions

87% of organisations* have an insufficient cyber security budget despite security being at the top of organisation's agendas. They are having to do more with less whilst staying competitive in their sectors.

Lack of expertise

60% of all cyber-attacks are being carried out by insiders. Compromised or malicious users pose a real threat to your organisation and can be damaging to your brand.

> In 2015 a former Morrisons employee was convicted of leaking employee payroll records of nearly 100,000 staff. The supermarket chain was ruled liable for the employee's misuse of data and incurred £2m costs relating the data breach.

Too many tools

On average, an enterprise uses 75 security products** to secure their network and nearly half of the security risk that organisations face stems from having multiple security vendors and products. The more systems in play, the more complex the management & reporting of potential threats becomes.

**Do you need a better defense strategy - IBM Security

*EY Global Information Security Survey 2018–19

CITADEL DIGITAL SECURITY

Threat Detect – SIEM

Citadel Threat Detect - SIEM is a fully managed service that allows organisations to offload your cyber threat detection to a team of proactive security experts, enabling your IT department to focus on priority tasks at hand and meeting core organisational objectives set by the business.

- Supported by Celerity's Service Desk for all service management, monitoring and detailed reporting.
- Removes the need for developing/retaining specialist skills in-house.
- Increases operational efficiency with the ability to deploy and scale systems rapidly and flexibly.
- Anomaly Detection - Detects "normal" behavioural patterns over time and identifies deviations from the known normal that may indicate a threat.
- No setup, licence or hardware fees.
- Threat Intelligence - Compares event attributes against up-to-date threat information, such as malicious domains or hashes, to more accurately identify the latest known threats.
- Pattern Analysis - Analyses event attributes in real-time against patterns of known malicious activities to quickly identify and classify active threats.
- 24 x 7 Advanced Threat Detection and Security Intelligence.
- User Behaviour Analysis -Continuously analyses individual user behavior to detect deviations that can help identify compromised user credentials and malicious insider activity.
- Aligned to CESG GPGs and Accredited to ISO27001:2013
- Integrates multi-vendor security tools into one unified view.
- Proactive service underpinned by a team of data protection and SC cleared security specialists.

Efficiently detect internal and external threats, manage insider risks and respond quickly against evasive perpetrators with Citadel Threat Detect

Offload your cyber threat detection to a team of proactive security experts, enabling your IT department to focus on priority tasks at hand and meeting core organisational objectives set by the business.

CELERITY

Celerity, working in partnership with NCSC, regional cyber protection units & certifies industry specialists to fight the war on cyber-crime.

IBM Security

Head Office: 11 St. George's Court, Kirkham, Preston, PR4 2EF

Take control of your Digital Security & Cyber Defence.

Speak to a Celerity Security experty today.

T: **+44(0) 1772 542 450**

E: **info@celerity-uk.com**

www.celerity-uk.com