Time Is Money When A Network Is Breached **Detect The Threat Immediately**

It is a fact, that the quicker a cyber-attack is identified the more damage costs are reduced (Ponemon,2018). With the average cyber-criminal spending 197 days inside a network before being discovered, it is critical for organisations to detect cyber threats as soon as possible by using the core component of **Citadel Detect – Security Information Event Management (SIEM).**

Achieve a real-time view of internal and external threats to your network through consolidated threat information and intelligence enabling identification. Not only detect an external attack on your organisation, but identify internal threats to your business by addressing unauthorised or unsanctioned user behaviour. Gain better insight, make better decisions and respond faster to advanced threats.

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.

Antonis Patrikios, head of cyber-security at law firm Fieldfisher, said the ruling was likely to be a *"game-changer"* for firms. *"The key questions for organisations are:*

Are we taking appropriate steps to protect the data and are we appropriately prepared to respond to incidents that put the data at risk?"

Threat Detection Security Challenges:

- ◯ Lack of resources
- ◯ Too many security devices
- ◯ Lack of expertise
- ◯ Lack of visibility
- ◯ Compliance pressures
- ◯ Budget restrictions
- ◯ Systems complexity

CITADEL
DIGITAL SECURITY

SIEM-as-a-Service
Rapid Insights Into Threats

Key Features

- 24 x 7 Advanced Threat Detection & Security Intelligence

- Integrates multi-vendor security tools into one unified view

- Removes the need for developing/retaining specialist skills in-house

- Integrates with Celerity Data Custodian and Intuition Data Visualisation

- Proactive service underpinned by a team of data protection & SC cleared security specialists

- No setup, licence or hardware fees

- ITIL Service Desk for all service management, monitoring and detailed reporting

- Increase operational efficiency with the ability to deploy and scale systems rapidly and flexibly

- Confirmed data sovereignty, data always remains within the UK

- Aligned to CESG GPGs and Accredited to ISO27001:2013

Cyber Attackers Are Smart

Be Smarter with Citadel Threat Detect

SIEM-as-a-Service allows businesses to confidently defend against cyber-attacks; providing visibility and alerting to events and activity which could pose a risk to data and service integrity.

Comprehensive Visibility
A single, highly scalable platform reducing thousands of security events into a consolidated list of suspected offenses across on-premise, SaaS & IaaS environments.

Real-time Threat Detection
Automatically analyse logs and network flows to detect threats and generate prioritised alerts as attacks progress through the kill chain.

Manage Compliance
Automate internal and regulatory compliance with data collection, correlation & reporting.

Eliminate Manual Tasks
Centralise threat information into a single view to eliminate manual tracking processes, allowing your team to focus on response and remediation.

External Threats
Man-in-the-Middle Attack · Hackers · Ransomware · SQL Injection Attack · Phishing · Zero Day Exploit · Malware

ORGANISATION

Insider Threats
Disgruntled employee deleting/downloading data onto a USB

Uneducated employee clicking on malicious links in emails

40% of breaches are caused by insider threats and these cyber-attackers are smart. They proactively cover their tracks by deleting log histories, hiding within volumes of normal traffic, stealing legitimate user credentials and exfiltrating data in small, infrequent batches. In order to uncover these stealthy attackers, your organisation needs comprehensive visibility of:

- Asset Activity
- Network Activity
- User Activity

Citadel SIEM-as-a-Service allows businesses to simply and easily detect internal and external threats, manage insider risks and respond quickly against evasive perpetrators.
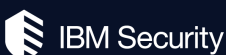
CELERITY

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

ISO 27001 CERTIFIED
UKAS British Assessment Bureau

CYBER ESSENTIALS

Powered by
IBM Security

Take control of your Digital Security & Cyber Defence.

Speak to a Celerity Security expert today.

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

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

www.celerity-uk.com