ukcloud

Keeping Pace With the Evolving Threat

Chris Wright

Account Director

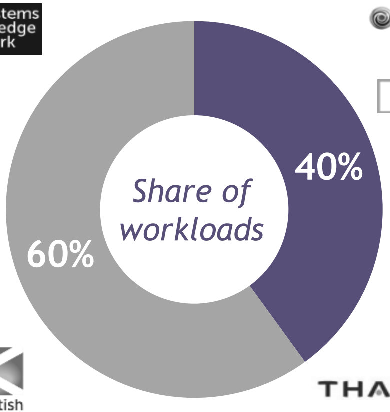
UKCloud at-a-glance

THE POWER BEHIND UK BASED CLOUD TECHNOLOGY

- 8 years old Founded 2011
- 250+ UK employees
- Built for UK public sector
- Award Winning
- Market Leading
- 250+ UK public sector projects

50+ direct customers

Cabinet Office
[dstl]
Environment Agency
Ecosystems Knowledge Network
www.parliament.uk
Driver & Vehicle Licensing Agency
Genomics england
Foreign & Commonwealth Office
Home Office
hscic Health & Social Care Information Centre
Land Registry
Department for Work & Pensions
HM Revenue & Customs
Ministry of JUSTICE
The Insolvency Service
Met Office
Ministry of Defence
learndirect
NHS
BANK OF ENGLAND
Devon & Cornwall Police Authority
The Scottish Government



Ecosystem of 300+ partners

AIRBUS DEFENCE & SPACE
aridhia
BAE SYSTEMS INSPIRED WORK
ARES
babylon
bjss
Ctrl O
CACI
Capgemini
CAPITA
CDG
Clearvision
Datatank
Deloitte.
docman
egress
EQUINITI
FIVIUM
HTK
i2N
leidos
kainos
MDS TECHNOLOGIES
nine23
Roc Technologies
saadian
serco
SYNAPTIC SOFTWARE
sopra steria
THALES
tolomy
vysiion
WigglyAmps
xtravirt
ZAIZI

- Public Cloud First
- Social Value Act
- CCS Approved
- Cloud Security Principles
- Greening ICT
- GDPR Ready

ENABLING TRANSFORMATION OF PUBLIC SERVICES

Making transformation happen.

- **Disrupting IT which underpins public services**
  - Challenging the status quo
  - Reducing the cost of IT
  - Driving agility and value
- **We focus on cloud so you can focus on outcomes**
  - Continuous innovation in multi-cloud
  - Optimised for UK public services
  - Enriched by a community of solution providers
- **Proven and successful**
  - 100% UK – high calibre local skills in cyber, cloud and digital
  - Market leading – we serve hundreds of digital programmes across the UK public sector
  - Award winning innovation and customer service

ukcloud ukcloud health ukcloud X

Cabinet Office [dstl] Environment Agency Ecosystems Knowledge Network www.parliament.uk

Driver & Vehicle Licensing Agency Genomics england Foreign & Commonwealth Office Home Office NHS Digital 70 YEARS OF THE NHS 1948-2018

Land Registry Department for Work & Pensions HM Revenue & Customs

Ministry of JUSTICE The Insolvency Service Met Office Ministry of Defence

learndirect

NHS BANK OF ENGLAND Devon & Cornwall Police Authority The Scottish Government

accenture aridhia AIRBUS DEFENCE & SPACE A.R.E.S CORPORATION BAE SYSTEMS INSPIRED WORK babylon

bjss CACI Capgemini CAPITA CDG Clearvision

Ctrl O Datatank Deloitte. docman egress EQUINITI FIVIUM

HTK smarter customer contact i2N leidos kainos MDS TECHNOLOGIES nine23 QINETIQ

Roc saadian serco SYNAPTIC SOFTWARE sopra steria TASER

THALES tolomy vysiion WigglyAmps xtravirt ZAIZI

Queen's Awards for Enterprise: Innovation 2017

THE SUNDAY TIMES TECH TRACK 100 2016 HISCOX

UK CUSTOMER EXPERIENCE AWARDS '17

DIGITAL LEADERS WINNER 100

The way in which people do IT has changed …

Expectation is for online services

24/7 is now the norm

What’s being shared is sensitive

Device Sprawl

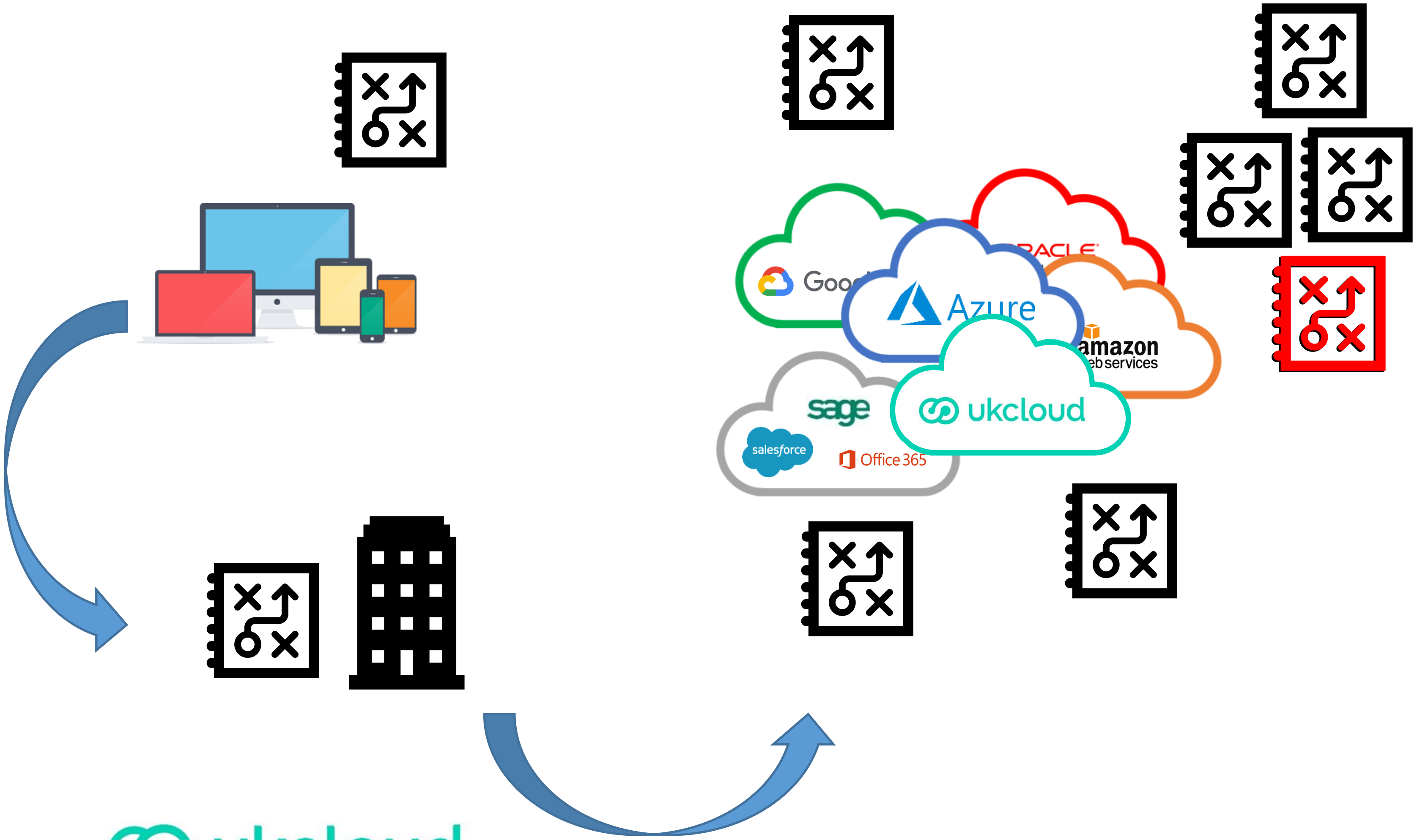
Workforce Mobility

Goo
RACLE
Azure
amazon
eb services
sage
salesforce
Office 365
ukcloud

Cloud Services

ukcloud

It’s ALL about the data

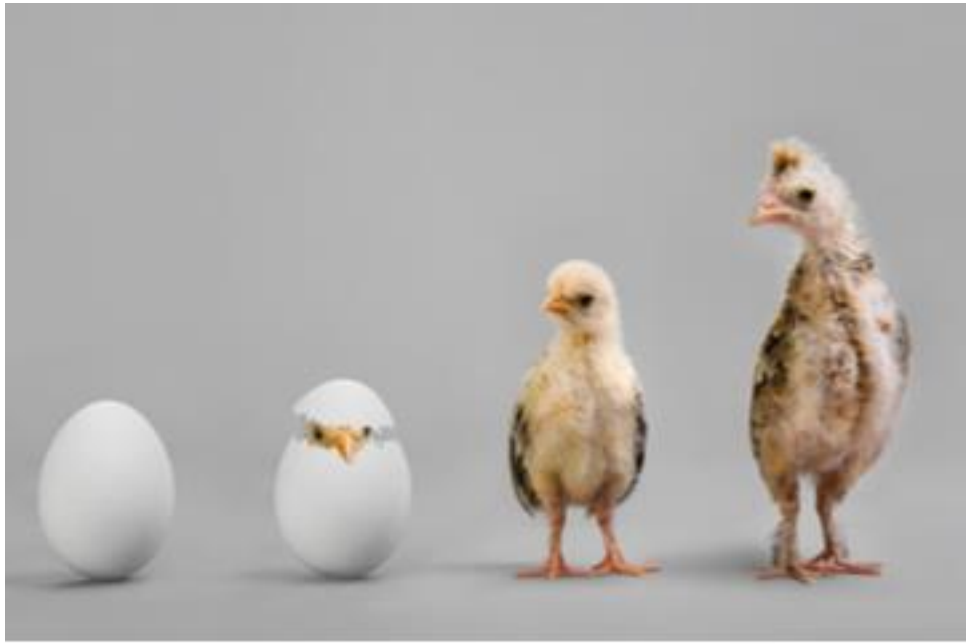


1. Data Sprawl: Data now exists in multiple locations (the DC boundary model is dead)

2. Data generation: New services creates new data

3. Data integrity: Modified data is as damaging as stolen data

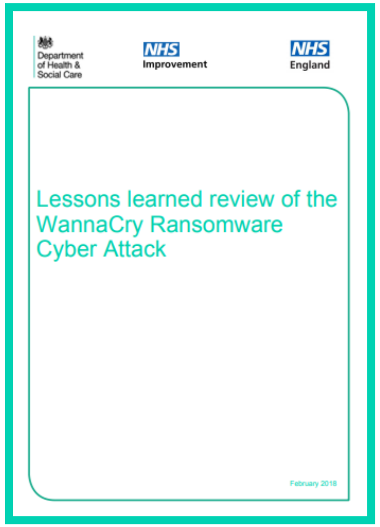
And the threat - is growing up too!!



- State actors
- Organised Crime Groups
- Single device to global networks
- Techniques, tools, processes more sophisticated
- Weaponisation of code

It’s a global business!!

The real impact of data breaches



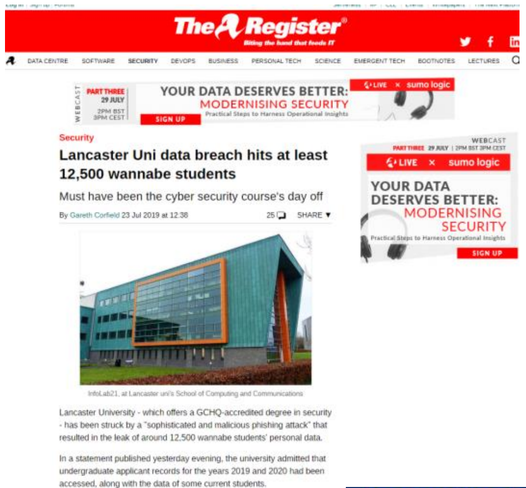
Department of Health & Social Care

NHS Improvement

NHS England

Lessons learned review of the WannaCry Ransomware Cyber Attack

February 2018



The Register®
Biting the hand that feeds IT

Security

Lancaster Uni data breach hits at least 12,500 wannabe students

Must have been the cyber security course's day off

By Gareth Corfield 23 Jul 2019 at 12:38 25 SHARE ▾

InfoLab21, at Lancaster uni's School of Computing and Communications

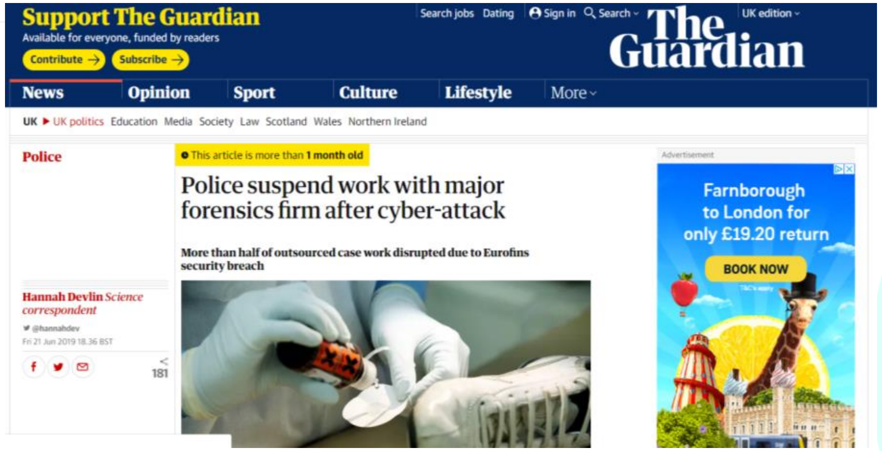
Lancaster University - which offers a GCHQ-accredited degree in security - has been struck by a "sophisticated and malicious phishing attack" that resulted in the leak of around 12,500 wannabe students' personal data.

In a statement published yesterday evening, the university admitted that undergraduate applicant records for the years 2019 and 2020 had been accessed, along with the data of some current students.

Information accessed by whoever the hackers were - so far Lancaster

£183M

BRITISH AIRWAYS



Police

This article is more than **1 month old**

Police suspend work with major forensics firm after cyber-attack

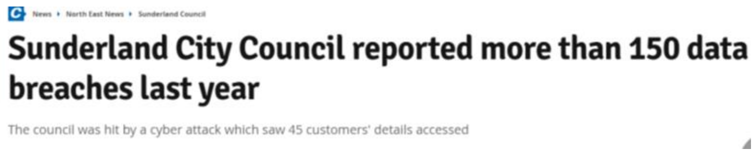
More than half of outsourced case work disrupted due to Eurofins security breach

Hannah Devlin *Science correspondent*

@hannahdev

Fri 21 Jun 2019 18.36 BST

181



News ▸ North East News ▸ Sunderland Council

Sunderland City Council reported more than 150 data breaches last year

The council was hit by a cyber attack which saw 45 customers' details accessed

ukcloud

Protection of data principles

Know you’re being attacked [detect]

Do you know what is happening?
Do you know what data you have, and where it is?
Do you know where it is happening?
Do you know the type of attack?

Deal with it immediately [defend]

Who’s responsible?
Who’s reacting to the incident?
What about out of hours?
Who needs to remediate?

Know what happened to your data [analyse]

Do you know what happened?
Do you know what you lost and who is impacted?
Did you plug the gap?
Who has to explain it?
How did it impact your brand?

Help yourself

Map where your data is, and what it is

Review or build your processes for dealing with data loss

Identify who in the business is responsible

The Capability Journey there is no silver bullet!

Secure Platform & Self Monitoring	Dedicated Portal & Collaboration	Secure Access	Malware Analysis Terminals	Discovery	Asset Management	Software Inventory
Network & Asset Map	Whitelisting	Threat Intel	UEBA	Machine Learning	Network Behaviour Analysis	Deep Packet Inspection (DPI)
Network Intrusion Detection (NIDS)	Endpoint Detection & Response (EDR)	SIEM & Log Management	File Integrity Management (FIM)	Remote User Visibility	Orchestration	Incident Response
Cyber Status	Wiki & Knowledge Share	Vulnerability Management	Active Defence	Mitre Att&ck Detections	Playbooks	Threat Hunting

ukcloud

How can we help?

What is CloudSOC?

ukcloud

CloudSOC is a cloud hosted, Cyber Security capability as a Service. Continually iterated to ensure it can detect and defend your organisaiton from the latest cyber threats.

Let our experts monitor and advise, do that yourself, or develop a hybrid model.

End to End Cyber Protection as a Service

Multi-Source – One Tool – Expert Support

LogRhythm The Security Intelligence Company · IBM · coverity · splunk> · paloalto NETWORKS · FIREEYE · CISCO · BlueCoat · Symantec · McAfee

CloudSOC

Application

- Web App Security
- App security Testing
- Web App Firewalls (WAF)
- Intrusion Detection Systems

Network

- Firewalls
- Network Intrusion
- Security Information and Event Management (SIEM)
- Secure Web Gateways
- Threat Intel
- Advanced Malware Analysis
- Security Analytics

Endpoint / Inf

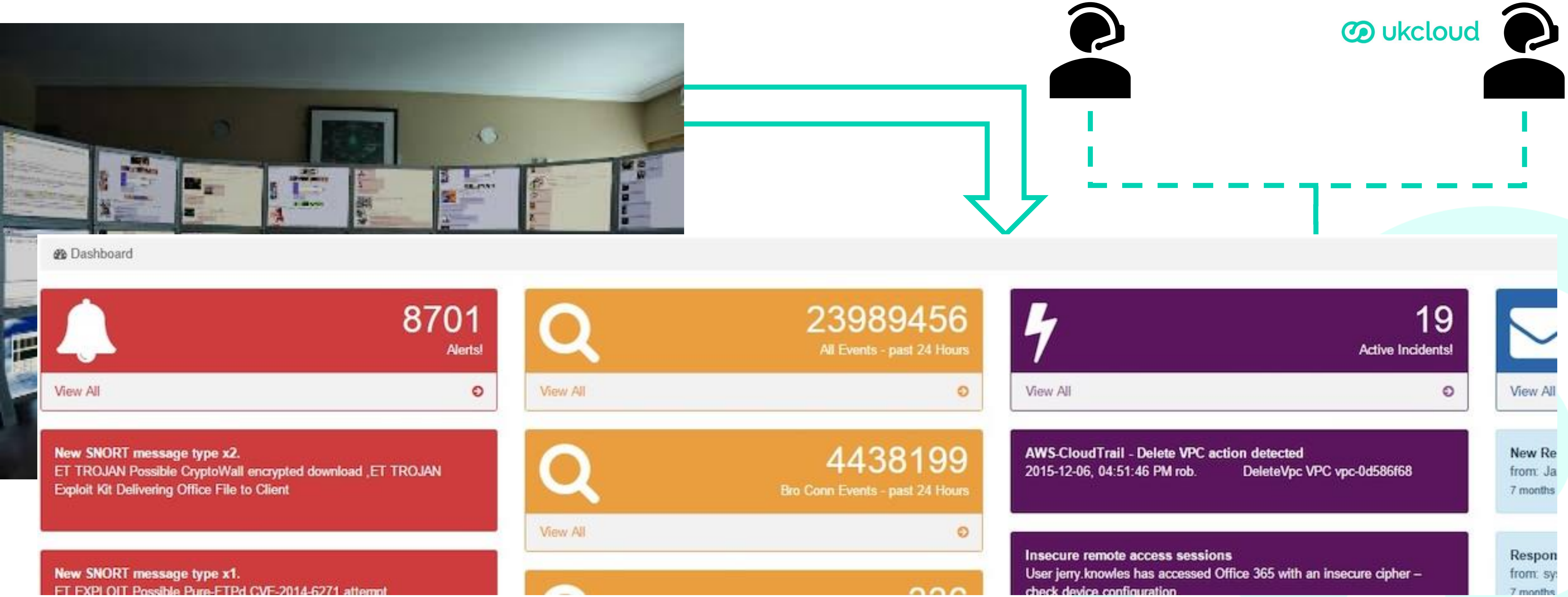
- Anti-Virus
- Personal Firewalls
- Patch and Config
- Data loss prevention tools
- Host Intrusion Detection

Cloud

- Cloud malware/anomaly detection
- SaaS Protection

ukcloud

CloudSOC - One tool ....



Dashboard

8701
Alerts!
View All

23989456
All Events - past 24 Hours
View All

19
Active Incidents!
View All

View All

New SNORT message type x2.
ET TROJAN Possible CryptoWall encrypted download ,ET TROJAN Exploit Kit Delivering Office File to Client

4438199
Bro Conn Events - past 24 Hours
View All

AWS-CloudTrail - Delete VPC action detected
2015-12-06, 04:51:46 PM rob. DeleteVpc VPC vpc-0d586f68

New Re
from: Ja
7 months

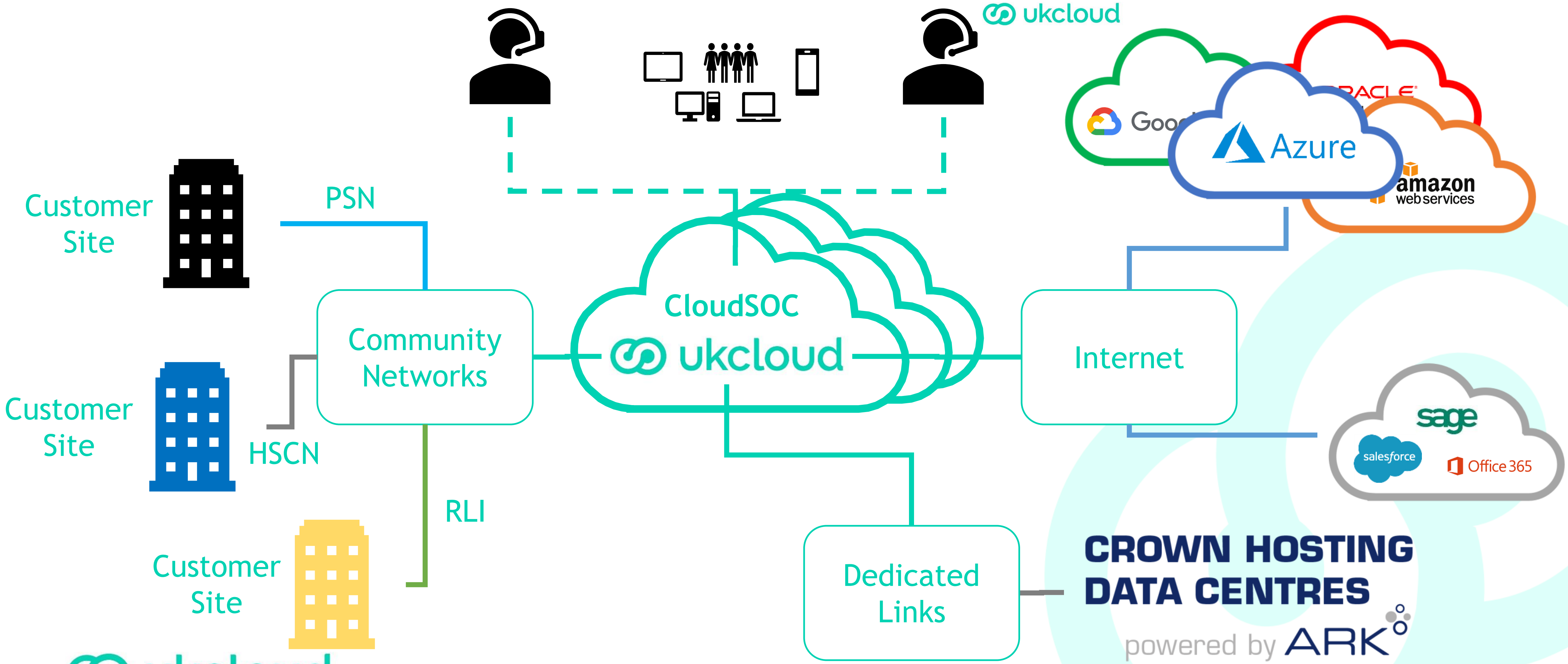
New SNORT message type x1.
ET EXPLOIT Possible Pure-FTPd CVE-2014-6271 attempt

Insecure remote access sessions
User jerry.knowles has accessed Office 365 with an insecure cipher – check device configuration

Respon
from: sy
7 months

ukcloud

… that can see your entire world



ukcloud

ukcloud

Thank You