

The background features a light gray trapezoidal shape on the left side, with a white area to its right. A dark blue horizontal band runs across the bottom, and a black band is at the very bottom. Two lines, one black and one yellow, originate from the top center and extend downwards towards the right, crossing the blue and black bands.

▶ **CONTINUOUS SECURITY**

CAN SECURITY TESTING REALLY BE
CONTINUOUS?

The background features a layered design with a light grey top section, a dark blue middle section, and a black bottom section. A thin black line and a thin yellow line run diagonally across the image, starting from the top left and extending towards the bottom right. The yellow line is positioned slightly above the black line.

WHO WE ARE

OUR VALUES

- ▶ Informed by innovation
- ▶ Continue with confidence
- ▶ See opportunities, not threats
- ▶ Your very own security fingerprint
- ▶ Priceless protection, value for money

▶ **REDEFINING SECURITY.**

Be protected, informed and empowered.

OUR SERVICES

- ▶ Security Testing
- ▶ Security Consulting
- ▶ Continuous Intelligence

▶ TAKE CONTROL

of what matters to you

CONTINUOUS vs. AD-HOC

CONTINUOUS

- ▶ Security appliances and software run continuously
 - Firewalls
 - Anti-virus/malware
 - Email filtering (spam, malware etc)

AD-HOC

- ▶ ISO27001, PCI-DSS audits
- ▶ Penetration testing
- ▶ Policy and updating security documentation
- ▶ Data discovery exercises
- ▶ Training

▶ IS CONTINUOUS SECURITY
A NECESSITY?



THE THREAT IS CONSTANT

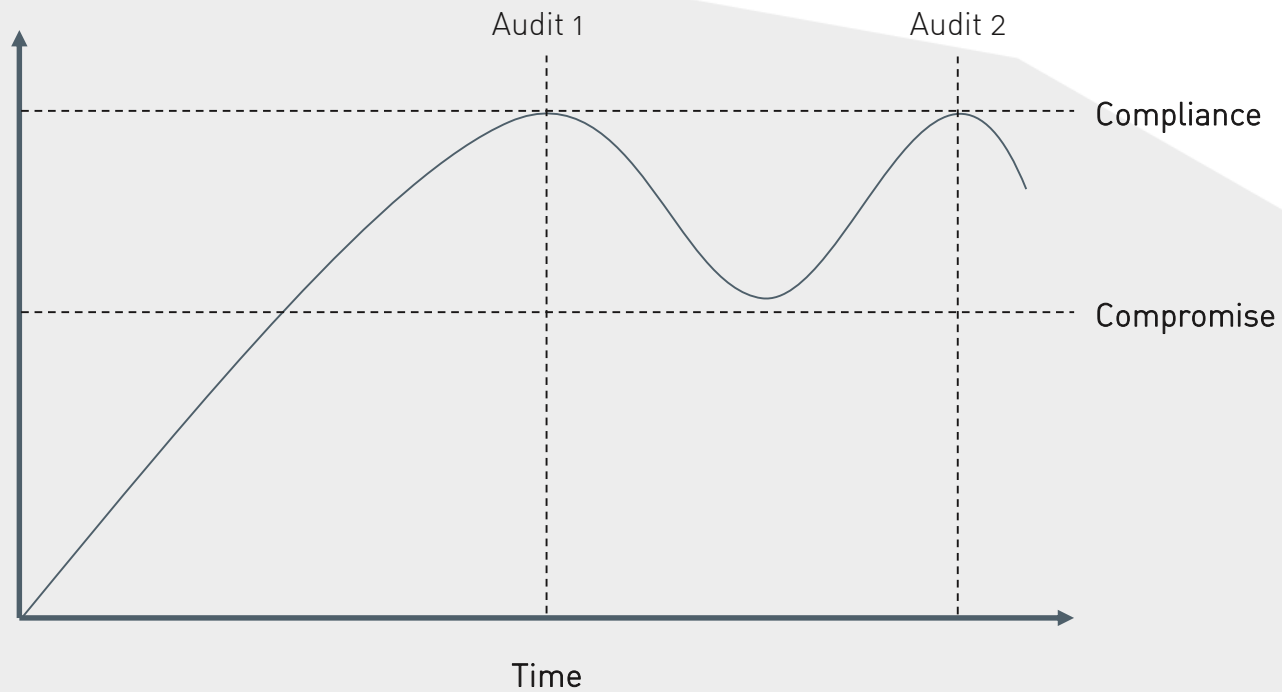
THE PROBLEM

- ▶ Snapshot audits/tests present a view of security at **THAT** moment in time.
- ▶ Window of opportunity or the unknown.
- ▶ Audit out of date as soon as you've completed the audit.

▶ **SNAPSHOT**

A false sense of security?

COMPLIANCE CURVE



REAL WORLD EXAMPLES

TalkTalk

- Annual penetration testing used
- Security auditing was spot checked (were PCI-DSS compliant)
- Disparate management of assets amongst group

Yahoo!

- Spot checked their systems
- Security auditing met compliance
- Fragmented group company could not control or manage risk

The background features a dark blue-grey gradient with a light grey area at the top. A yellow line and a black line both start from the top center and trend downwards towards the right, with the yellow line being slightly higher and steeper than the black line. The text is positioned on the left side of the slide.

AN EXAMPLE

APPLYING CONTINUOUS SECURITY TO SECURITY TESTING

THE CHALLENGE

- ▶ Online assets in constant change and not always visible
- ▶ Risk management is disparate
- ▶ New assets have unknown risk
- ▶ 3rd party suppliers are not aligned to your risk level
- ▶ Low confidence in external view of assets

▶ **CONTINUOUS VISIBILITY IS NEEDED FOR CONTINUOUS CONFIDENCE**



ANALOGY



An MOT performed all of the time with onboard engineers

INFORMER

Continuous

Infrastructure
Penetration Testing

Web Application
Security Testing

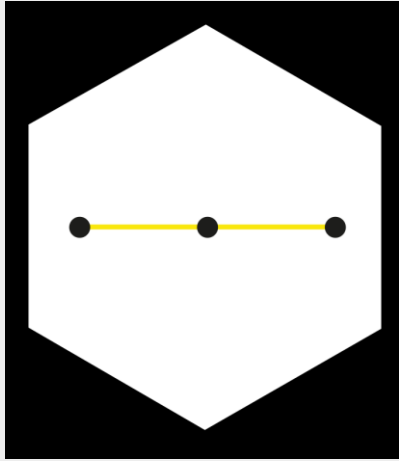
Online Exposure
Assessment

Data Mapping

Vulnerability
Assessment



INFORMER



TRACK ONLINE ASSETS

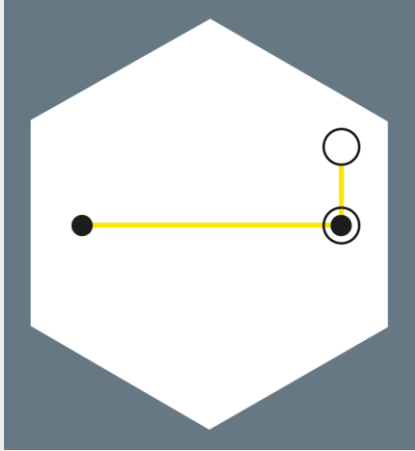
ENVIRONMENT CHANGES

- Marketing depts. commissioning new sites
- IT adjusting firewall rules and other defences

HOW

- Search engines
- DNS – passive/active
- SSL certificates
- WHOIS/IP Registration databases (RIPE etc)
- Active scraping/crawling

INFORMER

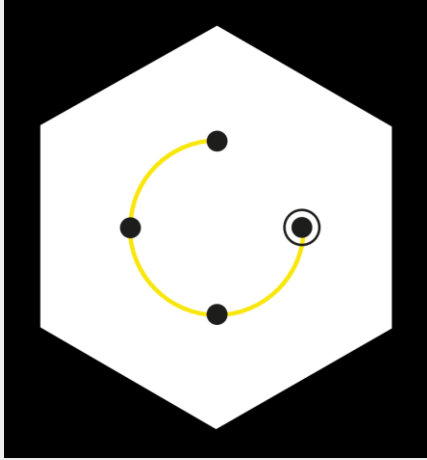


FIND EXPOSED DATA

DATA THAT IS COLLECTED ON THE WEB

- Contact forms (Personal data)
- Login forms (user credentials)
- Email addresses (for social engineering attacks)

INFORMER



REGULATION & COMPLIANCE

LOCATION OF DATA?

- Cloud
- Country
- Shared server with other organisations
- Shared platform with less secure applications

REGULATIONS AND COMPLIANCE

- Is EU data leaving the EU?
- Global regulations that expose organisation

INFORMER



TRACK VULNERABILITIES

- Near real-time vulnerability identification
- Vulnerabilities identified as and when they are released
- Discovered as assets are discovered

WELL-KNOWN GYM

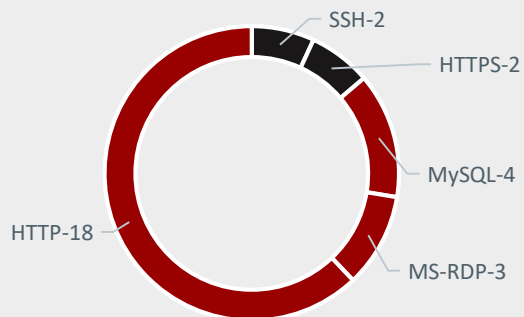
5 / 59
DOMAINS

142 / 193
SUBDOMAINS

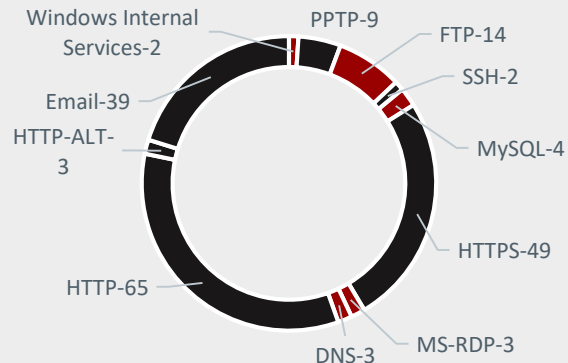
37
WEBSITES

109
IP ADDRESSES

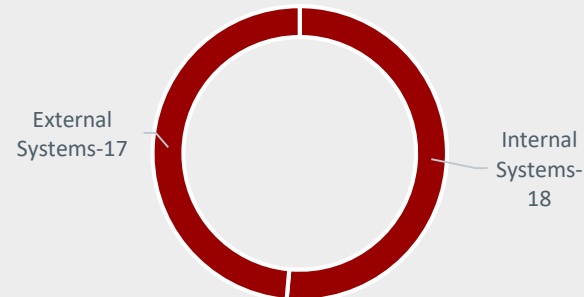
ADMINISTRATIVE SERVICES



AVAILABLE SERVICES

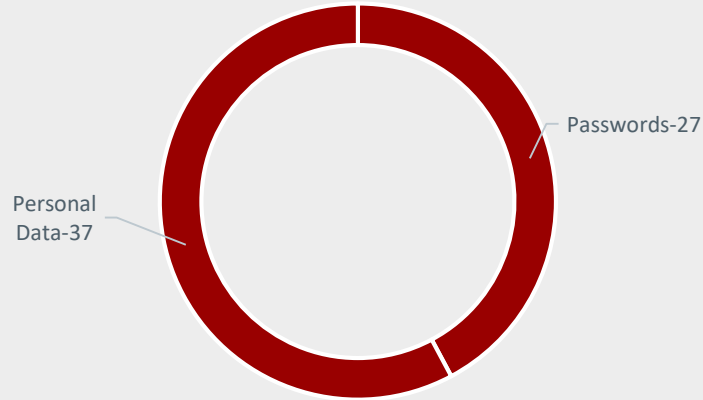


LOGIN DATA OVER UNENCRYPTED SERVICES

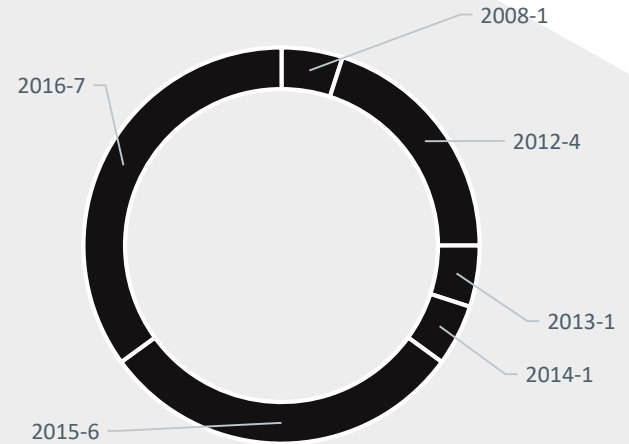


WELL-KNOWN GYM

UNENCRYPTED SENSITIVE DATA



COPYRIGHT DATES



WELL-KNOWN GYM



TAKE CONTROL.

To find out more about The Security Bureau
call us on **+44 1273 855 269** or email
info@thesecuritybureau.com

THE SECURITY BUREAU