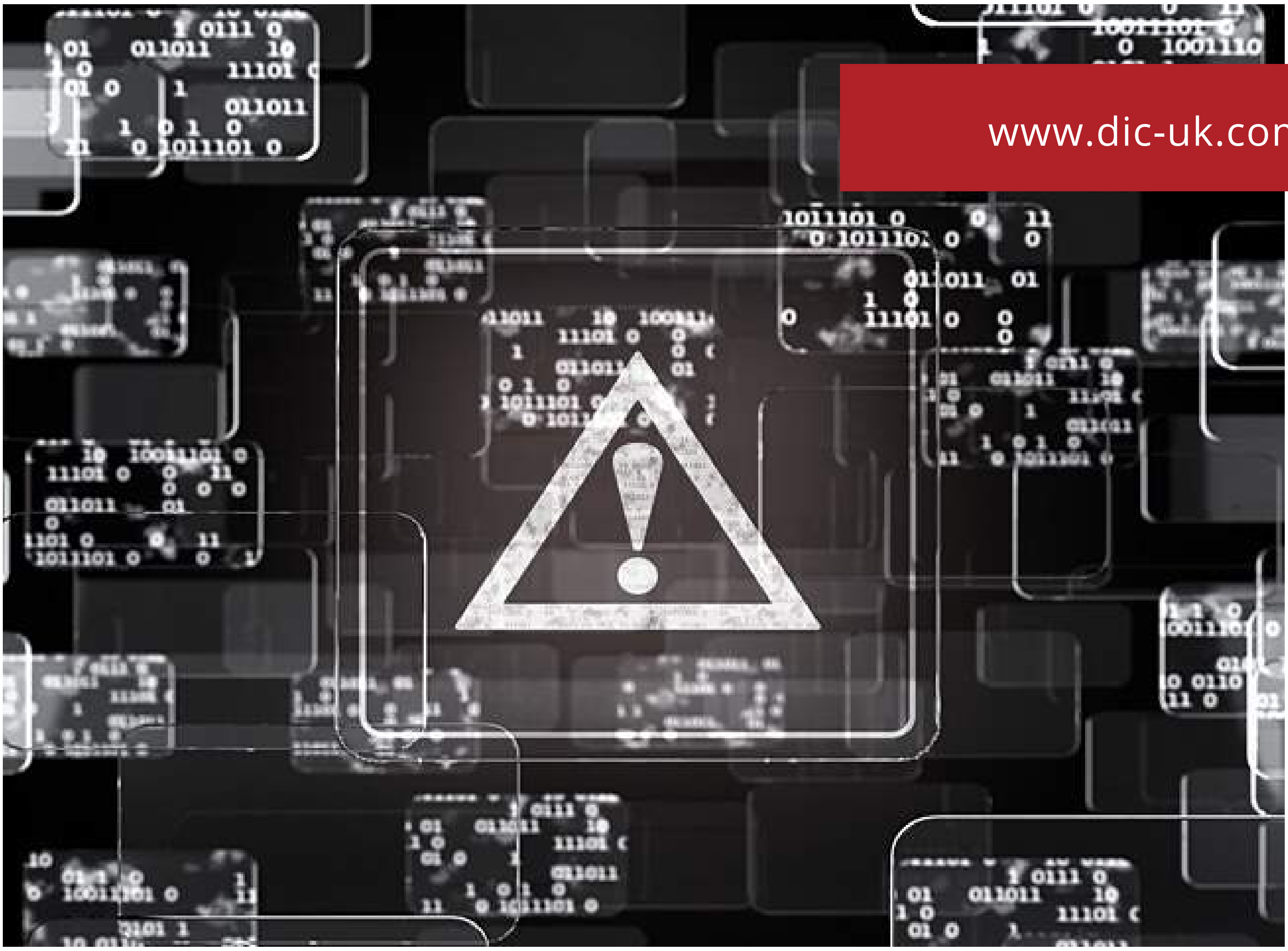
Digital Insights

TRIAGE INVESTIGATE REPORT



www.dic-uk.com

- DIGITAL FORENSICS
- OFFENSIVE SECURITY
- MANAGED SECURITY SERVICES
- IMPLEMENTATION

TRIAGE INVESTIGATE REPORT

DIGITAL **FORENSICS**

INCIDENT RESPONSE

We provide a full range of Cyber Security Incident Response (CSIR) solutions from advice to data collection, bespoke investigations, remediation and evidential statements and expert services.

Cyber investigations are complex and will include the examination of data from computers, servers, the cloud, switches, routers and many other network devices.

Digital Insights has the experience and ability to isolate a “rogue” digital footprint whilst gathering evidence of the “cyber event”, all of which is essential to help identify the root cause and to be able to identify malicious intruders.

Digital Insights offers real-time solutions to ensure your data assets and ongoing business operations remain safe. Our Incident Response teams skill fully identify, triage and investigate the incident, providing speedy, efficient resolution. Whatever the threat, your security is our priority.

CYBER THREAT HUNTING

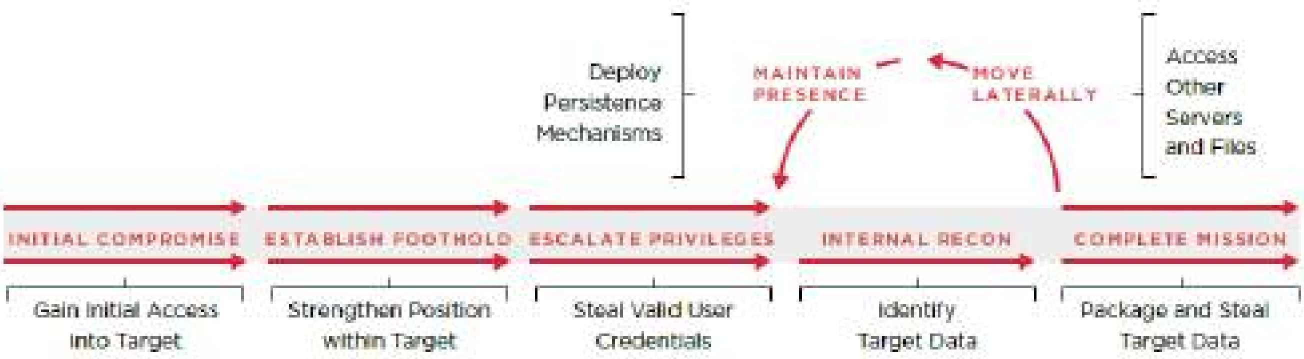
We perform cyber threat hunting in order to keep up with the deluge of new cyber threats and malware attacks! Cybercriminals continue to get more adept at using techniques and building tools that make it extremely difficult for traditional signature-based technologies to detect them. So difficult in fact, that it’s fairly common for an organization to not know an intrusion has occurred for days, weeks, or even months. Passively monitoring for signs of malware and relying on traditional signature-based technology is not effective. That’s why we’re seeing a shift to a more proactive approach, including hunting for potential network threats, by many organizations.

We define threat hunting as a focused and iterative approach to searching out, identifying, and understanding adversaries internal to the defender’s networks. It’s a method of searching through networks and datasets to find advanced persistent threats that evade existing security defenses.

FORENSIC DATA RECOVERY

Your company’s operations depend on critical business data being accessible, secure, and integrated. A hack or breach can steal or corrupt your data, causing you a massive loss of information and revenue. Our Forensic Data Recovery teams quickly salvage previously removed data by using precision data recovery methods and the latest tools. With Digital Insights, Dubai, on the job, you can rest at ease

OFFENSIVE **SECURITY**



Deploy Persistence Mechanisms
MAINTAIN PRESENCE
MOVE LATERALLY
Access Other Servers and Files
INITIAL COMPROMISE
ESTABLISH FOOTHOLD
ESCALATE PRIVILEGES
INTERNAL RECON
COMPLETE MISSION
Gain Initial Access into Target
Strengthen Position within Target
Steal Valid User Credentials
Identify Target Data
Package and Steal Target Data

COMPROMISE ASSESSMENT

We carryout Compromise Assessment which is a combination of extensive experience and responding to intrusions carried out by advanced threat actors. Industry-leading threat intelligence and cutting edge technology is used to deliver an assessment that:

- Identifies ongoing or past intrusions within your organization.
- Assesses risk by identifying weaknesses in security architecture, vulnerabilities, improper usage or policy violations and system security misconfigurations.
- Increases your organization’s ability to respond effectively to future incidents.

High-profile data breaches in the news represent only a fraction of the intrusion activity carried out globally. Knowing whether your organization has been breached and identifying ways to reduce risk is crucial to preventing your organization from becoming the next major data breach headline.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Digital Insights combine Penetration Testing with Vulnerability Assessment to identify and validate threats or weaknesses that could compromise IT security. Our security experts use hands on scanning techniques to perform vulnerability assessments that identify the highest potential risk to your environment. Then conduct Penetration Test (Ethical Hacking) to manually simulate real-world network attacks, mimicking the tactics employed by malicious outsiders. The result is an IT security report of findings and a detailed risk analysis with actionable recommendations to help a client to protect their IT security including network infrastructure, critical systems and confidential data.

The types of VAPT performed depends on the following:

- **NETWORK VAPT**

This is the assessment procedure that is conducted by our experts on the user's network for identifying possible vulnerabilities that the attackers might exploit. The primary objective of a network penetration test is to recognize exploitable vulnerabilities in systems, networks, network devices (i.e., switches, routers), and hosts before hackers can discover as well as exploit them.

- **WEB APP VAPT**

Web Application Security Assessment will comprehensively appraise the security of an application. These tests are carried out from both the authenticated and unauthenticated perspective and will offer an evaluation of the sites security posture from both valid users who aim to escalate access privileges and unauthorized users.

- **MOBILE APP VAPT**

A Mobile Application Security Assessment looks at the security and compliance risks of your entire solution from the app on the device, the backend systems, the network the app connects to, and the interaction and data flow between them. Our experts are well-versed finding the weaknesses and will thoroughly evaluate your security controls and provide actionable steps you can take.

- **VOIP**

We assess your VOIP infrastructure and evaluate the VoIP components deployed from a security perspective including investigating for the authentication mechanisms, as well as the potential interception, interruption or manipulation of the exchanged information between the client and VoIP server to maintain the confidentiality, integrity, and availability of the environment.

MANAGED SECURITY **SERVICES**

SOC AS A SERVICE

Organizations, especially large ones, need to protect sensitive information and data to remain competitive and secure. This includes data about their employees, partners, clients and more. With the growing number of cyber crimes, threats, and attacks, protecting your operations is a continuously evolving and challenging task. Investing in and managing a Security Operations Centre (SOC) is today a crucial element of your network security. Our SOC as a Service can protect against cybersecurity threats by monitoring, detecting and responding to incidents within your network infrastructure.

It is fully staffed, professionally managed, and equipped with the latest technology to provide 24/7 monitoring of your network. The SOC is equipped to detect, mitigate and resolve cybersecurity threats and/or attacks that might be attempting to access your network. Our experts analyse trends and work with your team to constantly test and strengthen your network. The WatchTower365 offering can be easily customized to your operations and aligned to the specific environment and issues that are unique to your organization.

SOC IN A BOX

Smaller companies have a higher risk of a cyber attack due to the lack of robust cyber security which usually come at a high cost. Digital Insights offers SOC services in one portable, plug and play device called WatchTower S.M.A.R.T 365 SOC in a Box! Get threat detection and alerting abilities of Security Information & Event Management (SIEM), 24x7 Network Monitoring of your network infrastructure and Endpoint Detection and Response, all in one Box. This aims to reduce staff requirements, remove redundancies and lower your cost of a breach by transferring risk.

MANAGED ENDPOINT DETECTION & RESPONSE

Tn a post-perimeter world, organizations must rely on managed endpoint detection and response (MEDR) to provide the first line of defense against a cyberattack. Yet, existing solutions require advanced expertise and time to use effectively.

Our Managed Endpoint Detection & Response service incorporates:

- 24 X 7 Monitoring
- Remote Remediation
- Support Suspicious Activity Monitoring
- Investigate | Isolate | Recover
- Guided Investigation
- Ransomware Rollback
- Global Threat Intelligence

IMPLEMENTATION

CLOUD OPTIMISATION

Reduce costs, optimize resource allocation and access data solutions securely, remotely and efficiently. With our Cloud-based expertise and solutions, you can concentrate on your core business and grow!

By organizing and maintaining your IT infrastructure, Digital Insights, Dubai collaborates with you to take your organization, products, and services to the next level.

SECURE INFRASTRUCTURE

Maximize the integration between your IT environment and your business – use the Digital Insights network architecture solutions, today! We architect, optimize and maintain your data centers, infrastructural services, and hybrid cloud-based and virtualized infrastructures. We help your organization boost efficiency and resource allocation, letting you always stay ahead of the competition.

10 staggering cybersecurity statistics for 2019

1

0%

The cybersecurity unemployment rate is approaching 0%

2

$8bn

in cost to businesses in 2018 due to ransomware

3

The threat of ransomware now extends to nations and their critical national infrastructure

4

87%

of healthcare organisations will have started using IoT technology in some way in 2019

5

7/10

Around 7 out of 10 businesses are not prepared to respond to a cyber-attack

6

The next big threat comes with the increase in mobile attacks and targeting mobile platforms

7

92%

of malware attacks are via malicious emails

8

32%

of UK businesses identified a breach in 2018

9

It's estimated that by 2025 we will see 64 billion connected IoT devices

10

146bn

records are projected to be exposed in the five year period between 2018 and 2023

1 - Source: Cybersecurity Jobs Report 2018-2021
2 - Source: Cybersecurity Ventures
3 - Source: ENISA Threat Landscape Report 2018
4 - Source: Aruba Networks
5 - Source: Hiscox's 2018 Cyber Readiness report
6 - Source: Cybersecurity Ventures
7 - Source: Verizon's 2018 Breach Investigations Report
8 - Source: DCMS
9 - Source: Business Insider, IoT Analytics; Gartner, Intel
10 - Source: Juniper's 2018 study

OFFENSIVE security OSCP
OFFENSIVE security OSCE
GIAC
www.giac.org
CREST.
CERTIFIED ISO 9001:2015 COMPANY
Information Security Management ISO 27001 Certified
C|EH v9
Certified Ethical Hacker
C|HFI
CERTIFIED HACKING FORENSIC INVESTIGATOR

"DIGITAL FORENSICS IS AN EXACT SCIENCE - NOT PROCEDURES BUT RESULTS" - EDEWEDE ORIWICH

Tel.: +44 (0)203 130 1723

Email: contact@dic-uk.com

Midsummer Court, 314 Midsummer Boulevard, Milton Keynes
MK9 2UB, United Kingdom