digital14

protect. transform. nurture.

Zero Threats in Cyber Sphere

Mitigating and Responding to Cyber Threats

August, 2020

Cyber Threat Landscape has Increased Exponentially

Digital14 is seeing sophisticated actors actively targeting organisations in the UAE

Most Orgs

being or expected to be breached, including data exfiltrated in IT, Cloud, and OT (critical infrastructure).

Nation State

groups actively involved based on D14 threat intelligence and managed SOC operations.

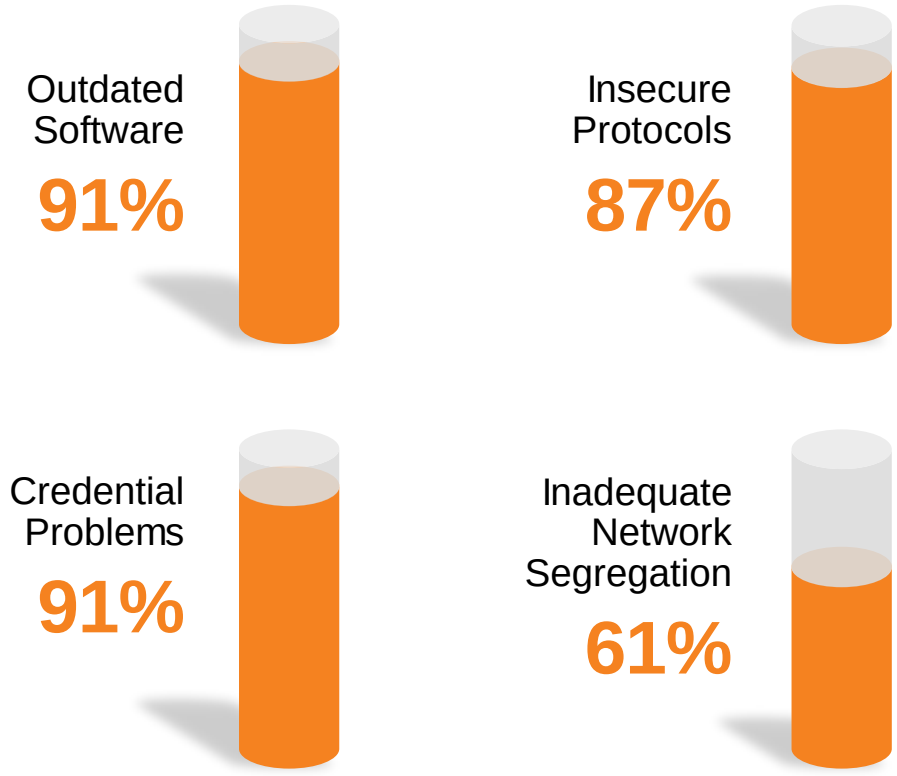
Cyber 4.0

transformation model needed to drastically change the cyber operating model for all organisations across region.

Months of

undiscovered reconnaissance by cyber intruders prior to breach discovery. The average dwell time is over 275 days globally.

Common Issues Impacting Cyber Resilience



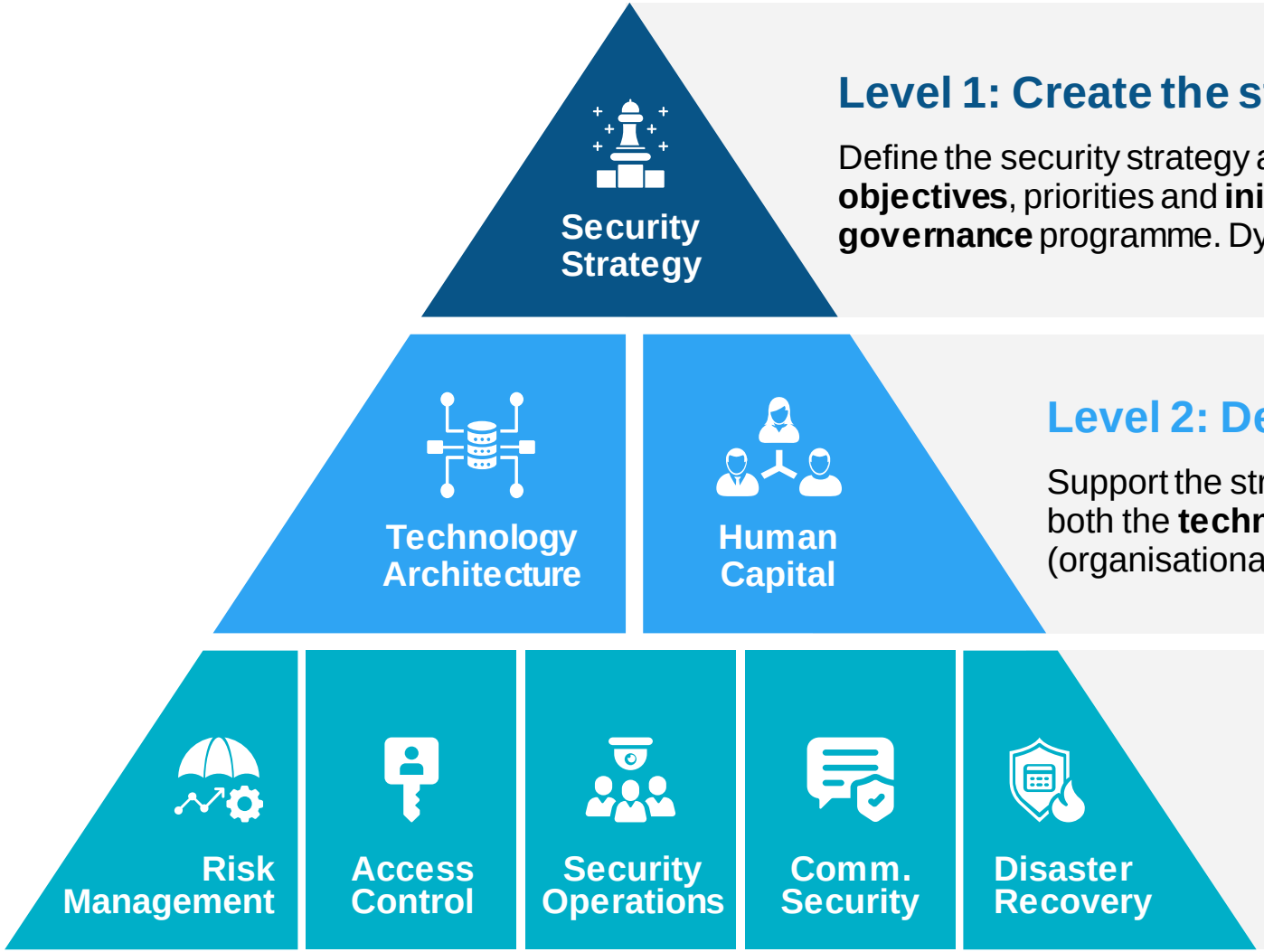
Number of these **attacks** succeed due to problems with **common issues** like outdated software, weak credentials, usage of insecure protocols, poor configuration or inadequate network segregation.

Poor visibility into the security posture and maturity of various group companies can have a catastrophic impact on organisations. The impact of **low security maturity** and **lack of visibility** can be significant:

- **Disruption** of critical and essential services severely **inconveniencing citizens**
- **Disclosure** of sensitive data leading to **loss of company reputation** at a national and global level
- **Tampering** of critical records potentially **damaging investor confidence** in UAE as a safe investment destination

Cyber Resilience Strategic Framework

Digital14 is committed to comprehensively advancing cybersecurity maturity



Level 1: Create the strategy

Define the security strategy and roadmap **aligned** to organisation's **strategic objectives**, priorities and **initiatives**. Maintain oversight via an **effective governance** programme. Dynamically adjust for evolving L2 and L3 requirements

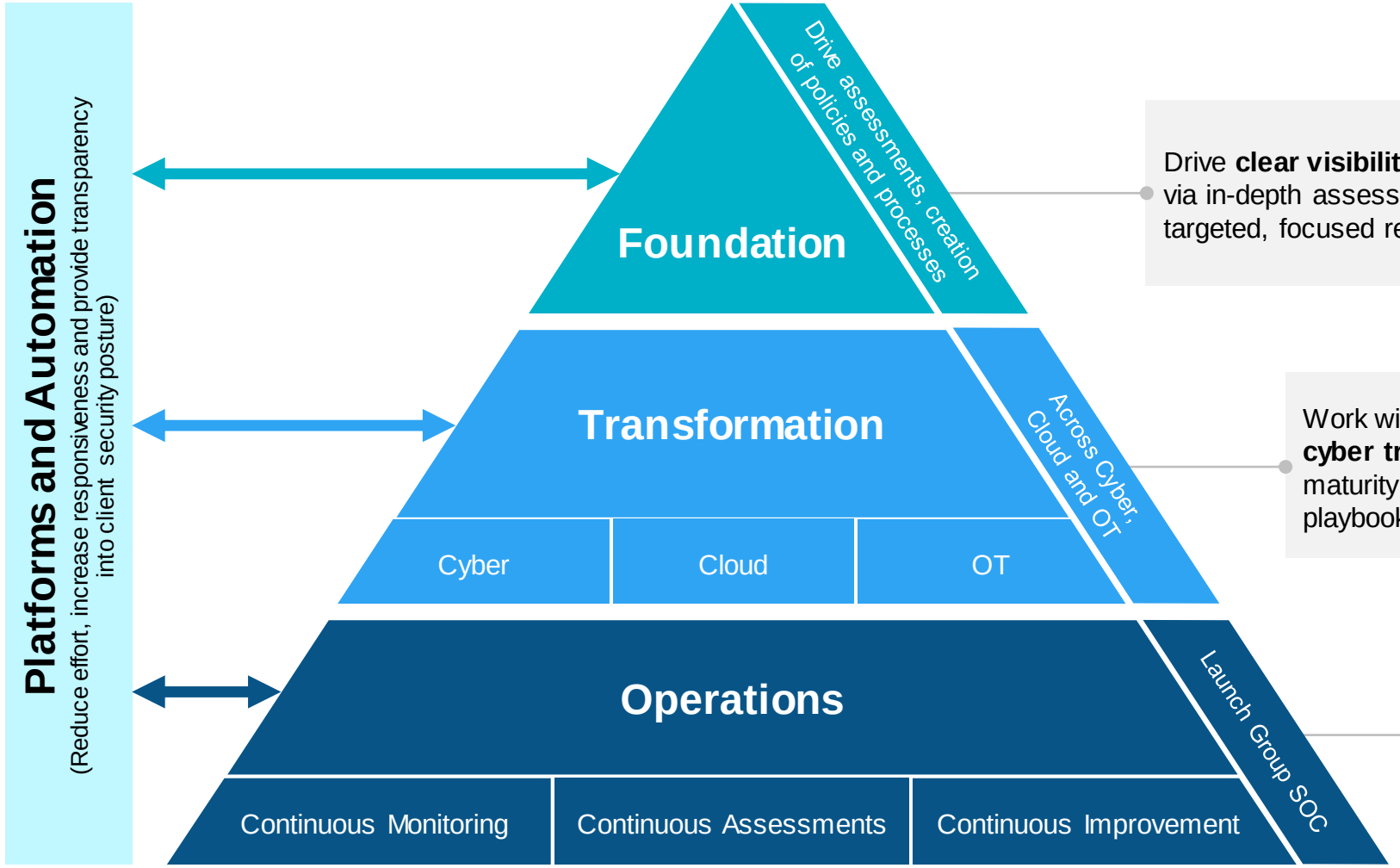
Level 2: Define the operating model

Support the strategy with a detailed **operating model** covering both the **technology** (security architecture) and **people** (organisational design).

Level 3: Execute the strategy

Codify and operationalise various initiatives and implement controls, transformational services and products aligned to the organisation's **strategy, roadmap** and the **operating model**

Zero Threat: End to End Cyber Resilience



Drive **clear visibility** into the current state of a client organisation via in-depth assessment programme to **enhance maturity** via targeted, focused remediation steps

Work with **client** to drive proactive, rapid and holistic **cyber transformations**. Help client attain **best-in-class** maturity via our standardised security stack and playbooks. Transformation covers **Cyber**, **Cloud** and **OT**.

Deploy cyber intelligence and operations fusion centre to proactively defend client. **Monitor, defend and proactively respond** to any threats.