Cyber Security: Cyber Ops and Stress Testing

Cyber Security

Quick Introduction

Cyber Security is not as simple as it used to be

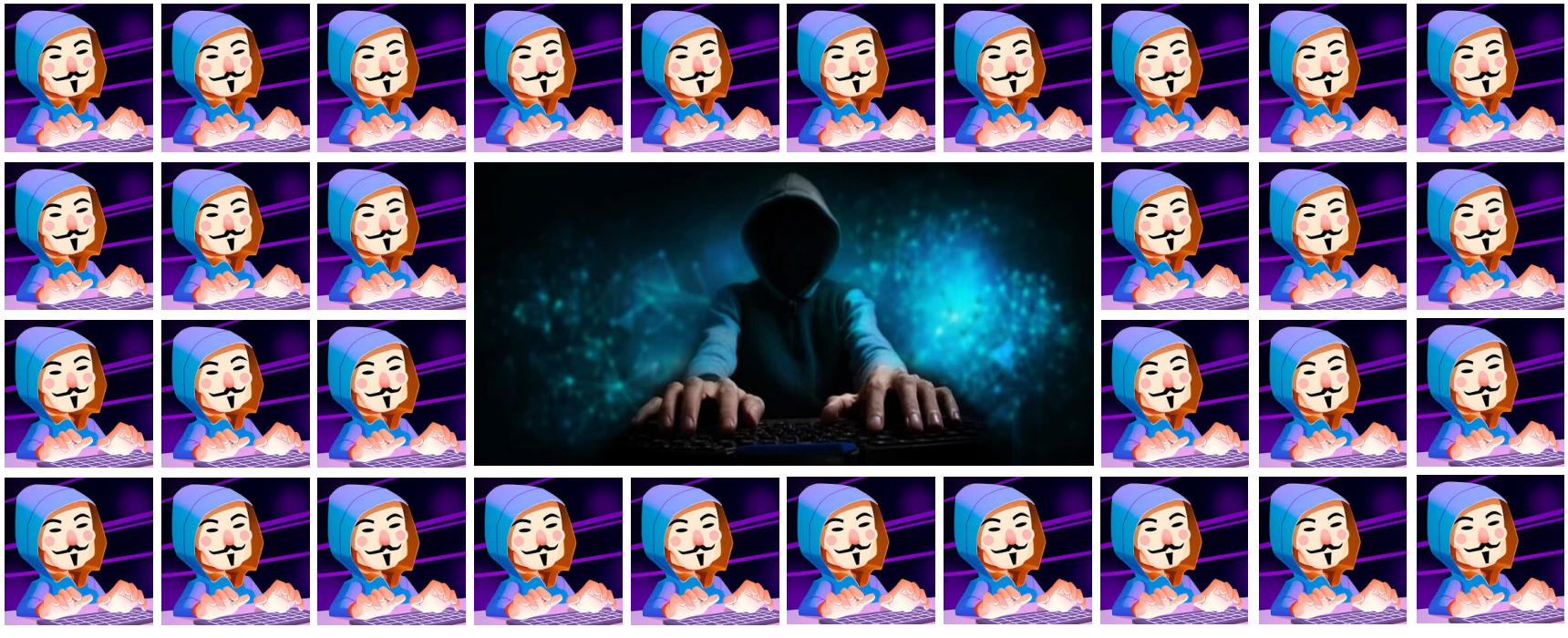
Back in the good old days, everything and everyone was on premise,

making Cyber Security the job of the people that build the wall and dig the moat

Today technology has made applications, data but also employees and clients much more mobile,

making Cyber Security the job of everyone in both IT **and** business

And on top of that opposition is ramping up



There's a load of different types of attack and almost as many ways to classify them

1. Aimed at the **company**
    - DDOS
    - Ransomware
    - Malware
    - …
2. Aimed at the **clients**
    - Phishing
    - Man in the middle
    - Banker at home
    - …

For this introduction we'll use the NIST framework as a guide

You need to know what you need to protect

1. Everything starts with an asset inventory that is up to date
    - Hardware: servers, laptops, network devices, printers…
    - Software: apllications (both own built and bought), websites, cloud solutions
    - Data

2. That also means
    - Robots
    - EUC applications

Protection is the most visible part of Cyber Security

1. Passwords, MFA and user authorisations are a common thing now and are what users can see

2. Behind the scenes there's a lot more

   - DDOS protection
   - Firewall
   - Network Access Control
   - Network design
   - Profiling
   - Biometrics
   - Encryption
   - …

Detection is a big data business

1. Everything that happens on corporate networks, devices and applications is logged and monitored by SOC

2. This means millions and millions and millions of events every day

    - Use cases to search for the relevant ones
    - Cross referencing events across platforms to find abnormal patterns
    - AI
    - …

Once detected, anomalies need a response

1. Responses can have a lot of forms
    - Revoking user or device access is the easiest
    - Isolating traffic
    - Sandboxing abnormal activities
    - Forensics

2. Coordination by
    - CyberSecurity Incident Response Team

If all else fails, fast recovery saves the day

1. Data back ups are the corner stone
2. But if e.g. a ransomware attack succeeds, you need a lot more
   - ….

Cyber Resilience

And Stress Testing to prove it

Cyber Resilience as part of regulation

1. New regulatory requirements are imposing better designed and testing Cyber Resilience
    - DORA contains very specific requirements
    - ECB Cyber Stress Test
2. But it’s not just regulation, clients are moving in the same direction
    - More and more requests to prove Cyber Resilience

All initiatives moving in the same direction

1. Recovery capabilities from Cold Back Up
    - Restoring applications from back-ups that are several days old
    - Time to establish that recovery has to be limited

2. Detection and protection capabilities need to be extensive
    - Threat Led Penetration Testing as part of DORA (based on TIBER initiatives)