INTRODUCTION

FOR A MORE SECURE SOCIETY

Assume breach and prepare

Ad Bresser

September 8, 2021

Agenda

1. Some introductions

2. Assume breach and prepare

3. What makes us different

AD BRESSER

Business Security consultant

- Since march 1, 2020 at Fox-IT
- Previously: Volmac / Cap Gemini, Planet Internet, KPN, independent, SIDN.
- Favorite podcasts: Security Now & Darknet Diaries

FOX-IT AT A GLANCE

1999

Foundation
Fox-IT is founded as a consultancy firm for forensic expertise.

2001

First SOC in Europe
Fox-IT is the first company to launch a Security Operations Centre (SOC) in Europe.

2003

Philips Crypto takeover
Fox-IT takes over Philips Crypto technology to focus more on advanced cryptography for the government.

2006

Threat Intelligence
Fox-IT sets up the Threat Intelligence Research Centre aimed at financial institutions.

2015

NCC Group
Fox-IT becomes part of NCC Group

2019

Universiteit Maastricht
On 23 December 2019, there is a serious cyberattack against Maastricht University (UM). Experts repair the damage and reactivate all systems. Fox-IT assist in crisis management, charting the attack and conducting forensic investigations and advises during the recovery process.

2020

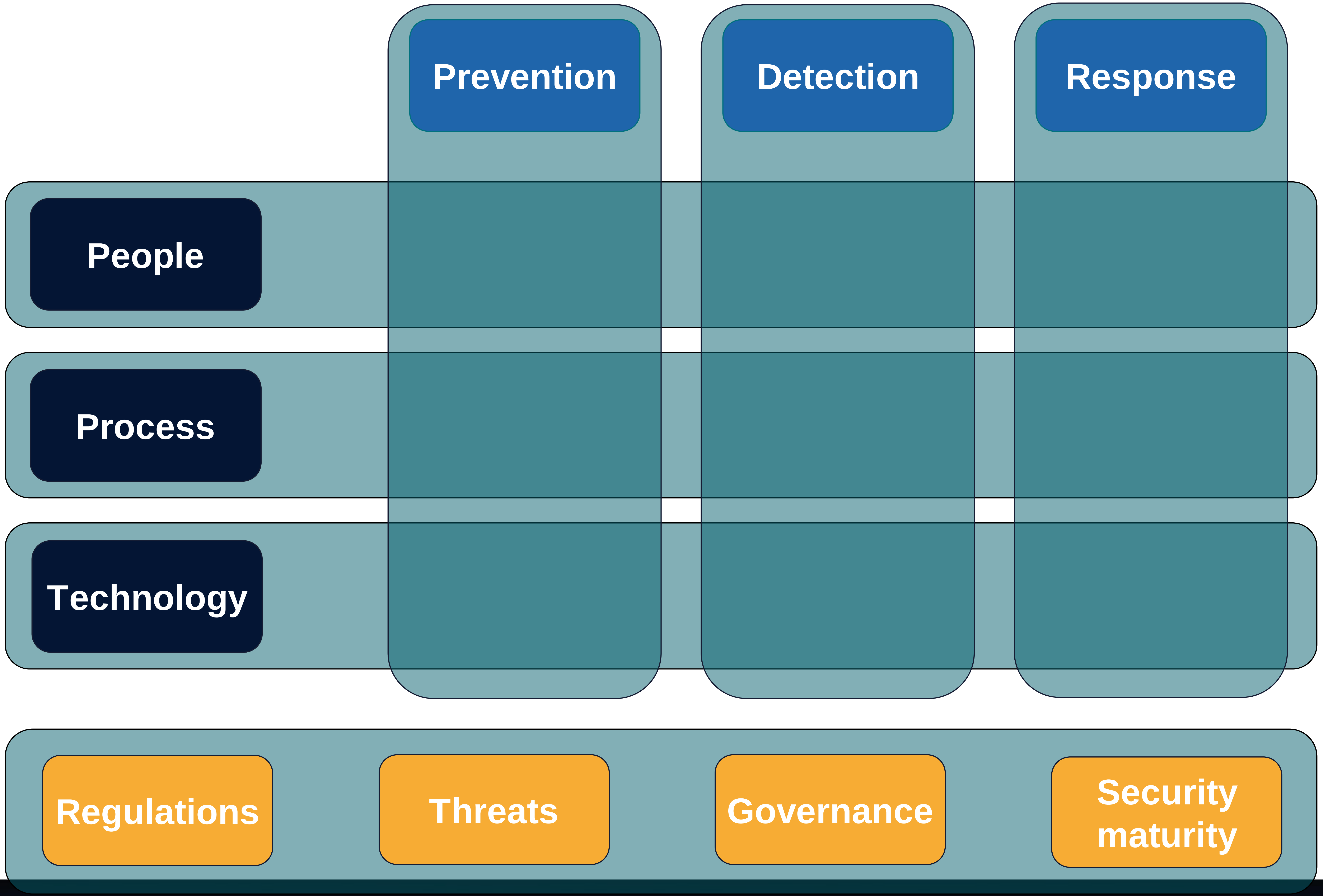
Evil Corp/ WastedLocker
WastedLocker is a new ransomware locker we have detected being used since May 2020. We believe it has been in development for several months prior to May 2020.

Major trend: targeted ransomware

From our latest quarterly Threat Report Update:

- Threefold increase in targeted ransomware attacks in 2021
- Continuing waves of digital extortion in the form of targeted ransomware
- Between April and June
  - 22% of ransomware data leaks attributed to Conti ransomware (now inactive)
  - Avaddon ransomware linked to 17% of ransomware data leaks
- Significant trend: double extortion - threatening to leak the stolen sensitive data of non-paying victims to damage organizational reputation
- One notable example is the Colonial Pipeline ransomware attack in June, carried out by affiliates of the DarkSide ransomware.

Take a broad security view



Prevention

Detection

Response

People

Process

Technology

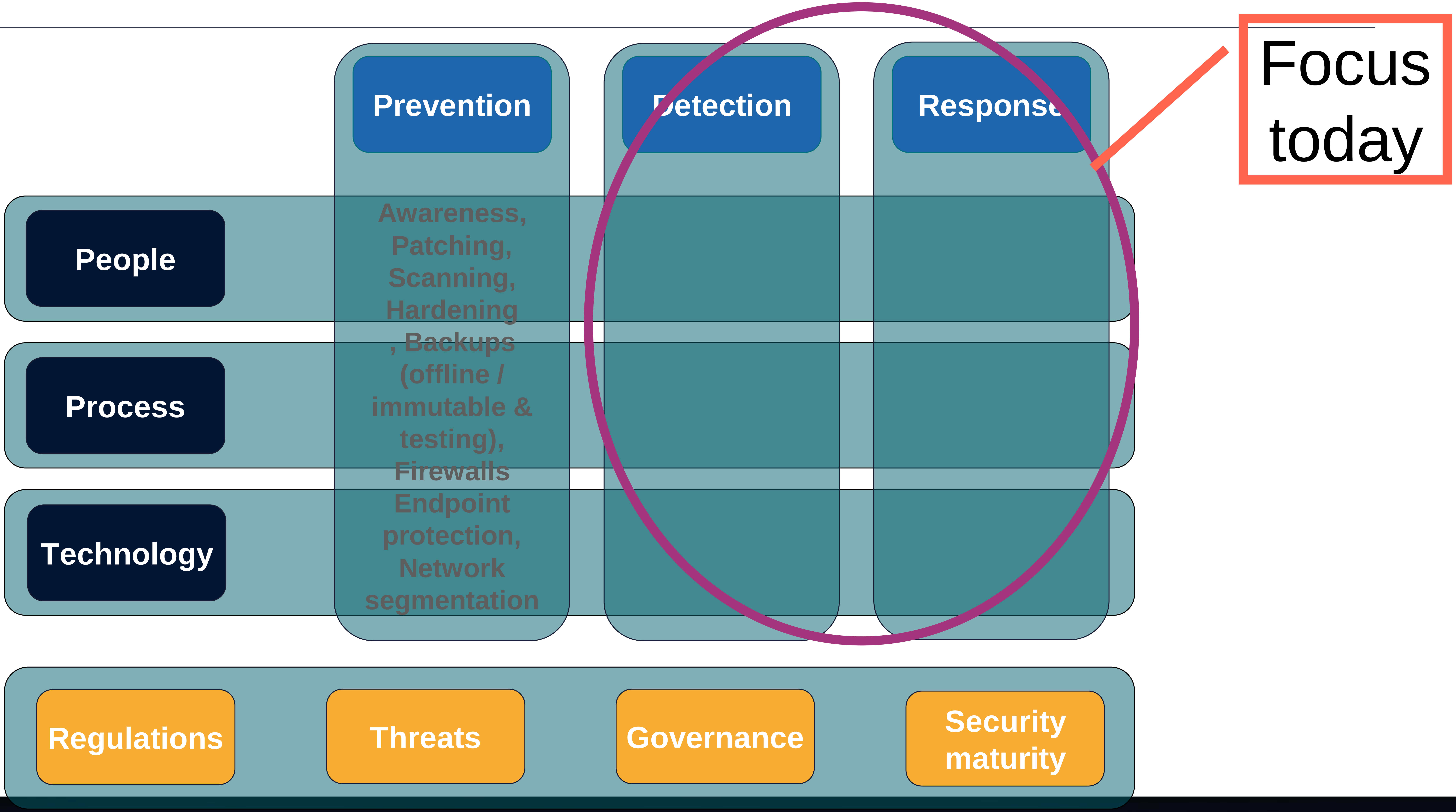
Regulations

Threats

Governance

Security maturity

Assume breach and prepare



Prevention

Detection

Response

Focus today

People

Process

Technology

Awareness, Patching, Scanning, Hardening , Backups (offline / immutable & testing), Firewalls Endpoint protection, Network segmentation

Regulations

Threats

Governance

Security maturity

Security incident detection by Employees

- People
  - Attentive employees are crucial; work on awareness
  - Test with Phishing campains
- Process
  - Easy reporting, swift follow-up
- Technology
  - Email box

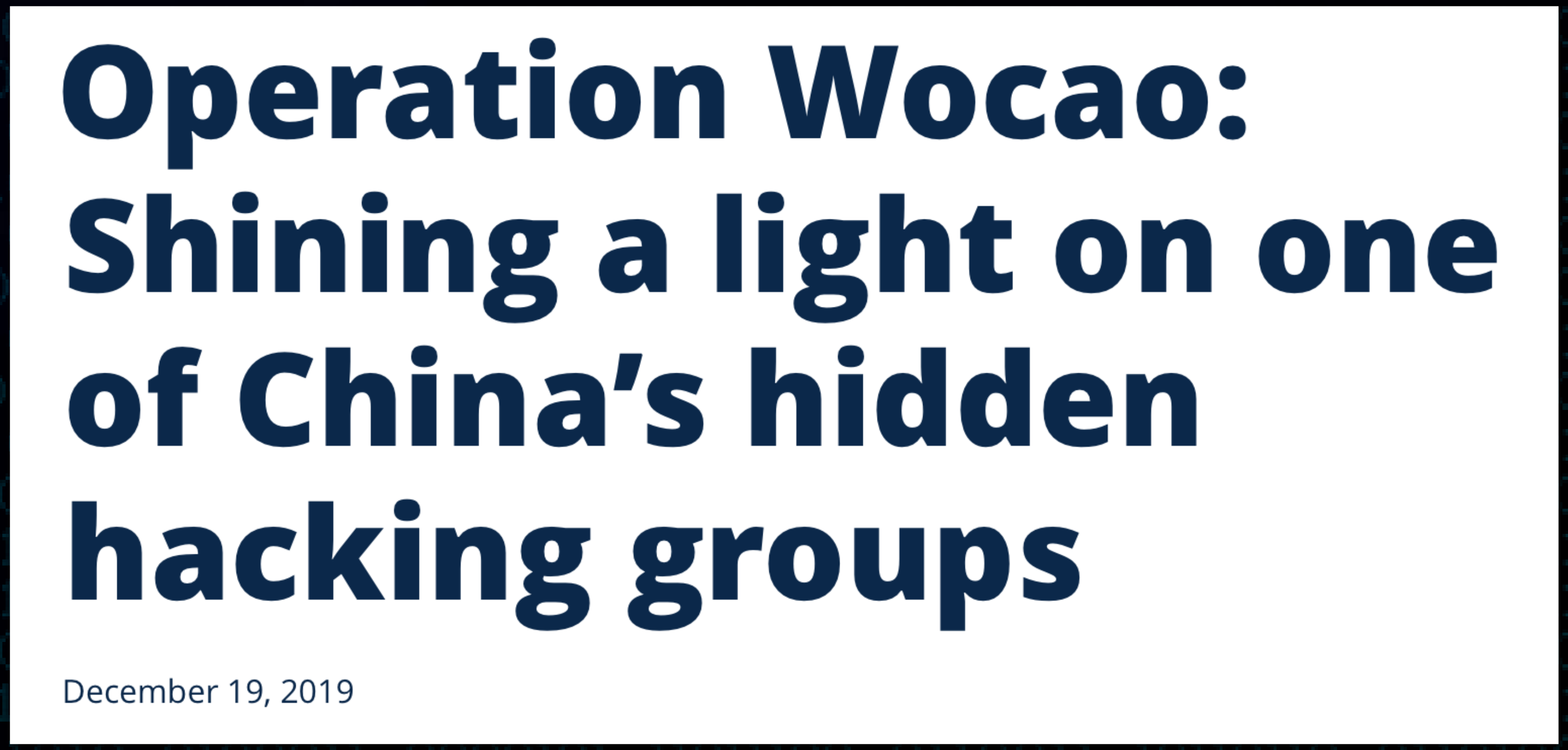
Security incident detection by technology

- Technology
  - IDS / Sensor, EDR (Endpoint detection and response), Logforwarding (e.g. firewall, proxy), SIEM (Security information and event management), Honeypots, Leaked information monitoring
- Process
  - AI, ML, Usecases
  - Classification, SOC
- People
  - Security analysts

Security incident response

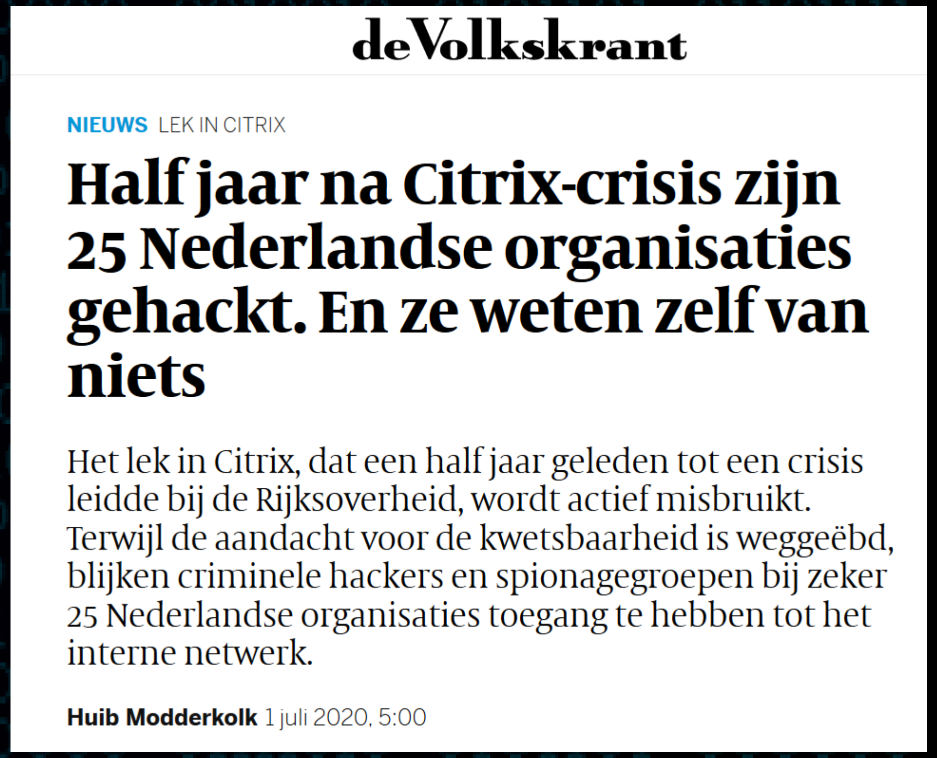
- People
  - Forensic experts
  - Crisis organization
- Process
  - Forensic readiness: log-file retention, access / cooperation at suppliers
  - Retainer (secure capacity)
  - Playbooks
  - Restore backups (off-line / immutable)
  - PRACTICE!
- Technology
  - Log-file analytics tooling

WHAT MAKES US DIFFERENT?



Operation Wocao: Shining a light on one of China's hidden hacking groups

December 19, 2019



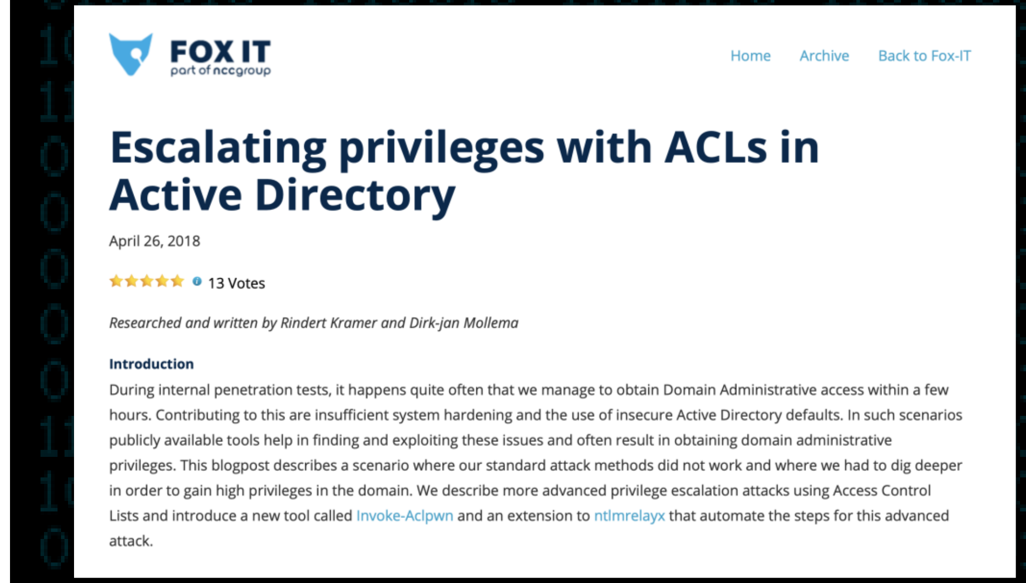
deVolkskrant

NIEUWS LEK IN CITRIX

Half jaar na Citrix-crisis zijn 25 Nederlandse organisaties gehackt. En ze weten zelf van niets

Het lek in Citrix, dat een half jaar geleden tot een crisis leidde bij de Rijksoverheid, wordt actief misbruikt. Terwijl de aandacht voor de kwetsbaarheid is weggeëbd, blijken criminele hackers en spionagegroepen bij zeker 25 Nederlandse organisaties toegang te hebben tot het interne netwerk.

Huib Modderkolk 1 juli 2020, 5:00



FOX IT part of nccgroup — Home Archive Back to Fox-IT

Escalating privileges with ACLs in Active Directory

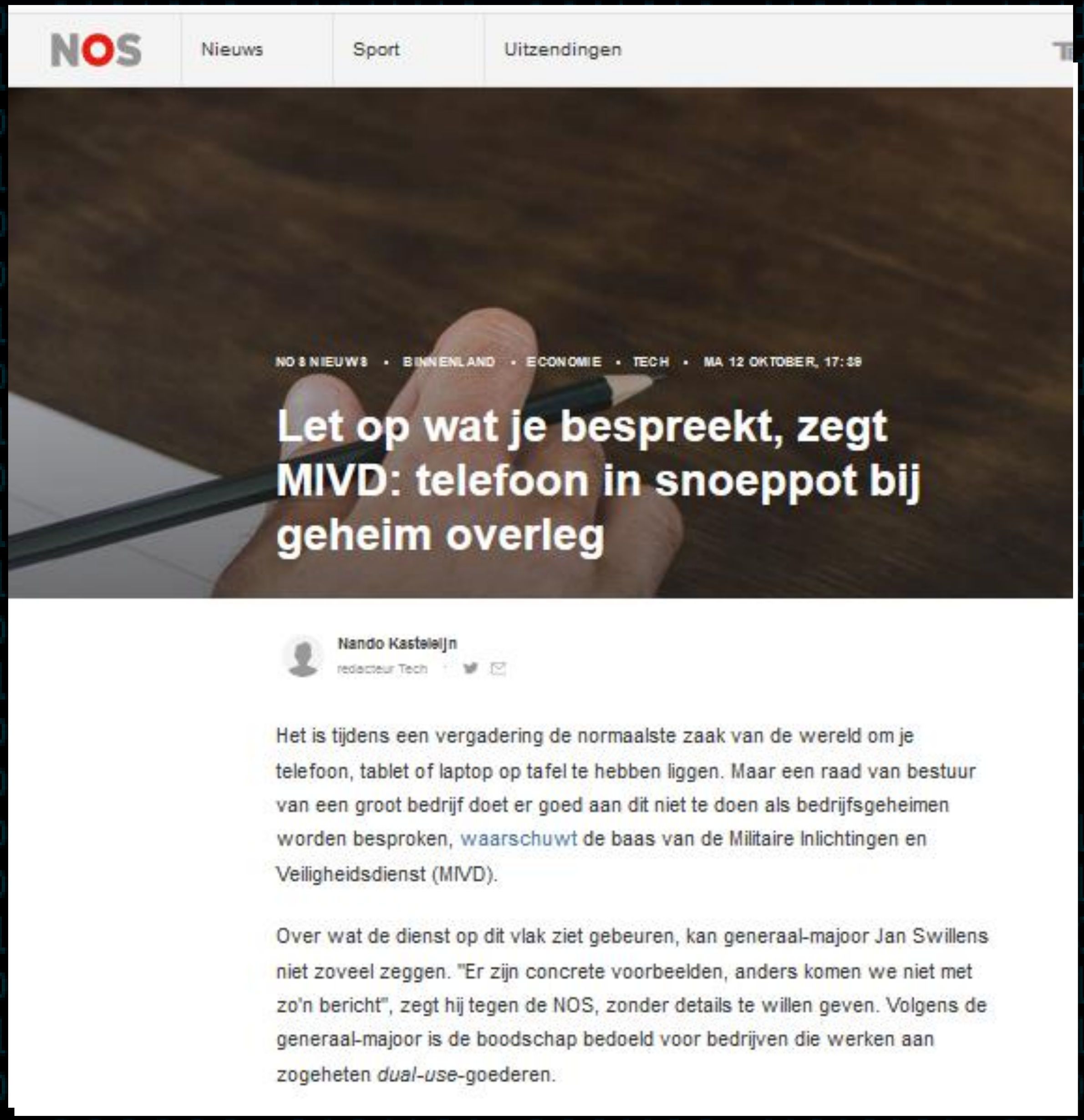
April 26, 2018

★★★★★ 13 Votes

Researched and written by Rindert Kramer and Dirk-jan Mollema

Introduction

During internal penetration tests, it happens quite often that we manage to obtain Domain Administrative access within a few hours. Contributing to this are insufficient system hardening and the use of insecure Active Directory defaults. In such scenarios publicly available tools help in finding and exploiting these issues and often result in obtaining domain administrative privileges. This blogpost describes a scenario where our standard attack methods did not work and where we had to dig deeper in order to gain high privileges in the domain. We describe more advanced privilege escalation attacks using Access Control Lists and introduce a new tool called Invoke-Aclpwn and an extension to ntlmrelayx that automate the steps for this advanced attack.



NOS — Nieuws Sport Uitzendingen

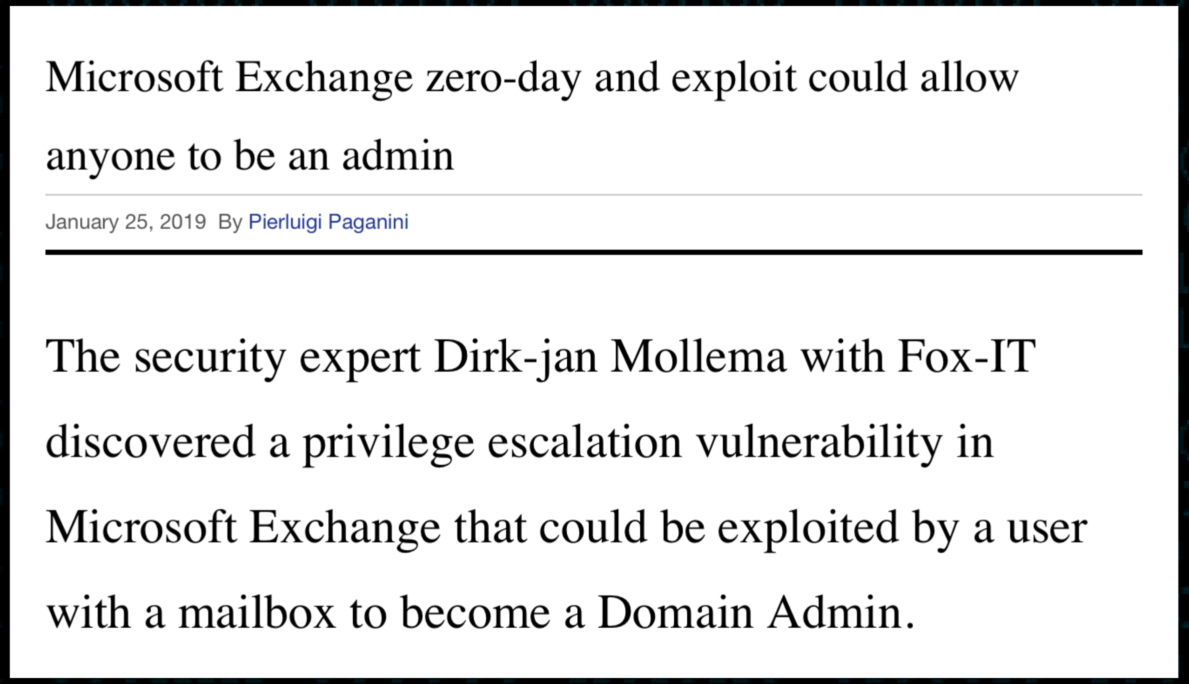
NOS NIEUWS • BINNENLAND • ECONOMIE • TECH • MA 12 OKTOBER, 17:39

Let op wat je bespreekt, zegt MIVD: telefoon in snoeppot bij geheim overleg

Nando Kasteleijn
redacteur Tech

Het is tijdens een vergadering de normaalste zaak van de wereld om je telefoon, tablet of laptop op tafel te hebben liggen. Maar een raad van bestuur van een groot bedrijf doet er goed aan dit niet te doen als bedrijfsgeheimen worden besproken, waarschuwt de baas van de Militaire Inlichtingen en Veiligheidsdienst (MIVD).

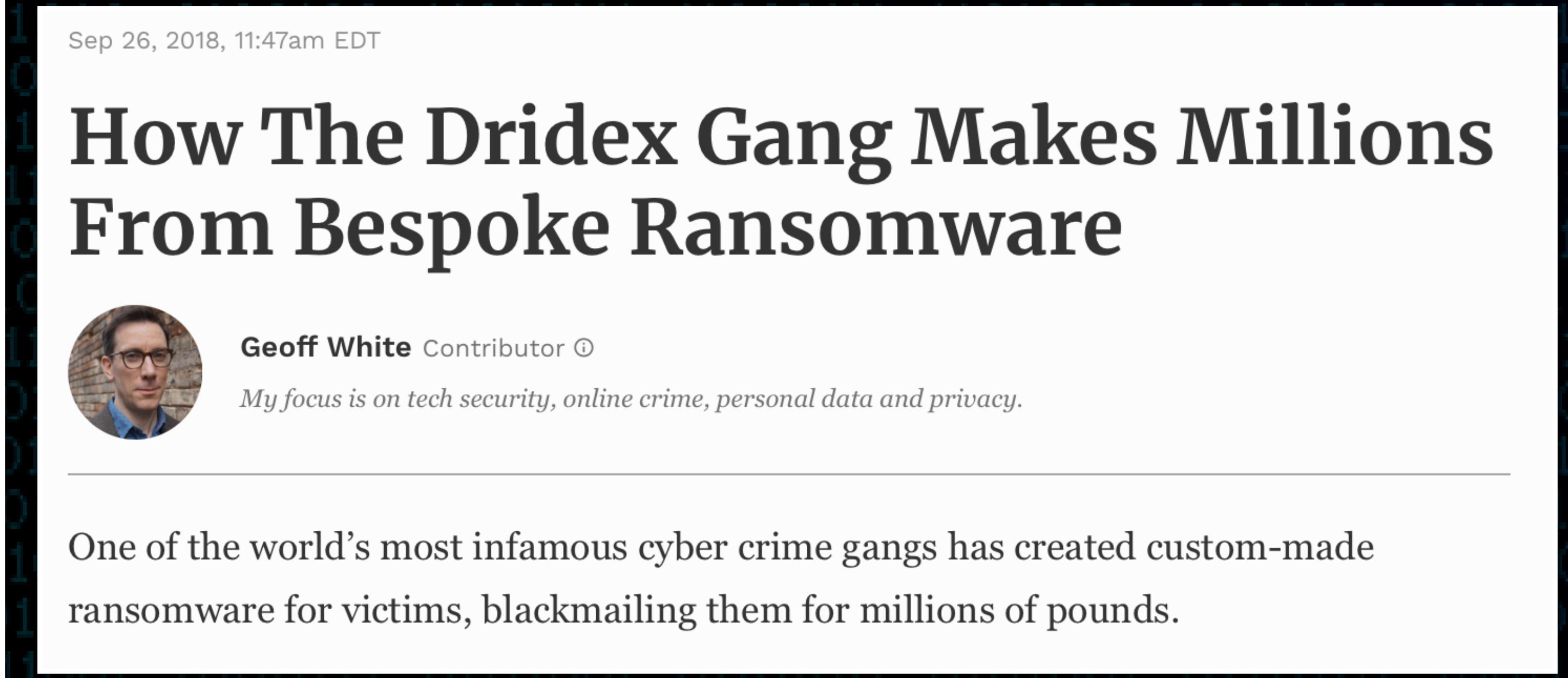
Over wat de dienst op dit vlak ziet gebeuren, kan generaal-majoor Jan Swillens niet zoveel zeggen. "Er zijn concrete voorbeelden, anders komen we niet met zo'n bericht", zegt hij tegen de NOS, zonder details te willen geven. Volgens de generaal-majoor is de boodschap bedoeld voor bedrijven die werken aan zogeheten *dual-use*-goederen.



Microsoft Exchange zero-day and exploit could allow anyone to be an admin

January 25, 2019 By Pierluigi Paganini

The security expert Dirk-jan Mollema with Fox-IT discovered a privilege escalation vulnerability in Microsoft Exchange that could be exploited by a user with a mailbox to become a Domain Admin.

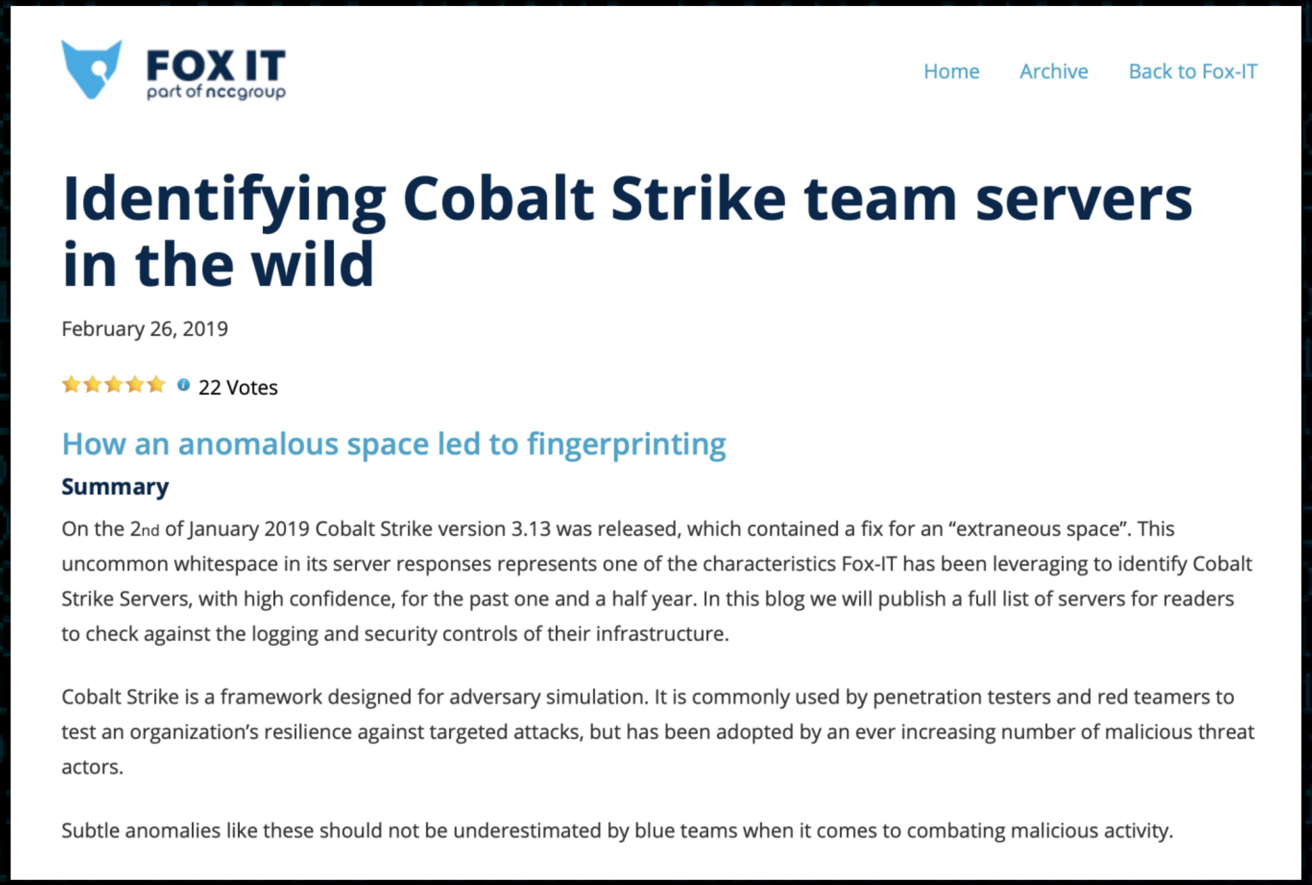


Sep 26, 2018, 11:47am EDT

How The Dridex Gang Makes Millions From Bespoke Ransomware

Geoff White Contributor
My focus is on tech security, online crime, personal data and privacy.

One of the world's most infamous cyber crime gangs has created custom-made ransomware for victims, blackmailing them for millions of pounds.



FOX IT part of nccgroup — Home Archive Back to Fox-IT

Identifying Cobalt Strike team servers in the wild

February 26, 2019

★★★★★ 22 Votes

How an anomalous space led to fingerprinting

Summary

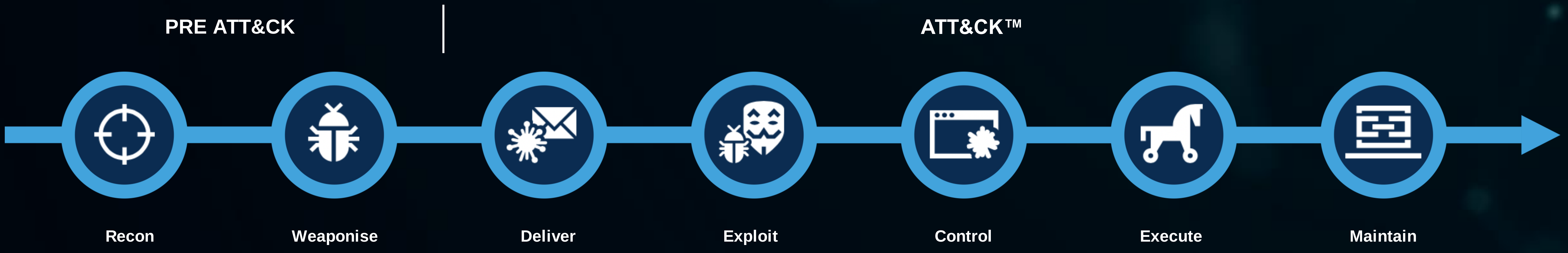
On the 2nd of January 2019 Cobalt Strike version 3.13 was released, which contained a fix for an "extraneous space". This uncommon whitespace in its server responses represents one of the characteristics Fox-IT has been leveraging to identify Cobalt Strike Servers, with high confidence, for the past one and a half year. In this blog we will publish a full list of servers for readers to check against the logging and security controls of their infrastructure.

Cobalt Strike is a framework designed for adversary simulation. It is commonly used by penetration testers and red teamers to test an organization's resilience against targeted attacks, but has been adopted by an ever increasing number of malicious threat actors.

Subtle anomalies like these should not be underestimated by blue teams when it comes to combating malicious activity.

OUR SOLUTIONS

As a full service security company we can help in all stages of cyber risks.



PRE ATT&CK

ATT&CK™

Recon

Weaponise

Deliver

Exploit

Control

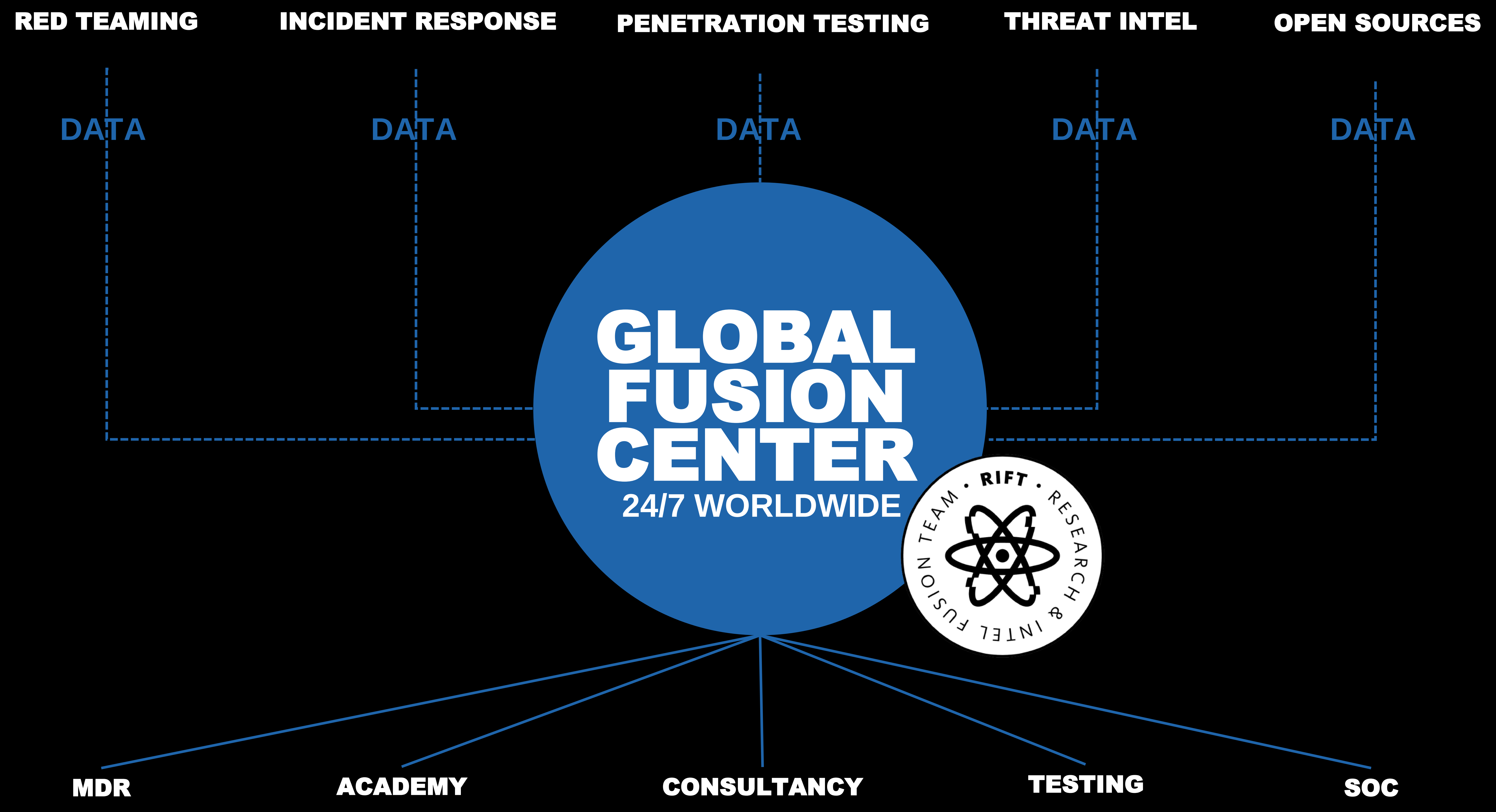
Execute

Maintain

THREAT INTELLIGENCE

	PREVENT		DETECT	RESPOND
PEOPLE	Consultancy & Academy		Managed Detection & Response	Digital Forensics Emergency Response (Retainers)
PROCESS				
TECHNOLOGY	Managed Intelligence Service	Penetration testing & security assessments		

GLOBAL FUSION CENTER & RIFT SIMPLIFIED


RED TEAMING

INCIDENT RESPONSE

PENETRATION TESTING

THREAT INTEL

OPEN SOURCES

DATA

DATA

DATA

DATA

DATA

GLOBAL FUSION CENTER

24/7 WORLDWIDE

MDR

ACADEMY

CONSULTANCY

TESTING

SOC

CALL US
BEFORE YOU NEED US

FOX IT
part of nccgroup