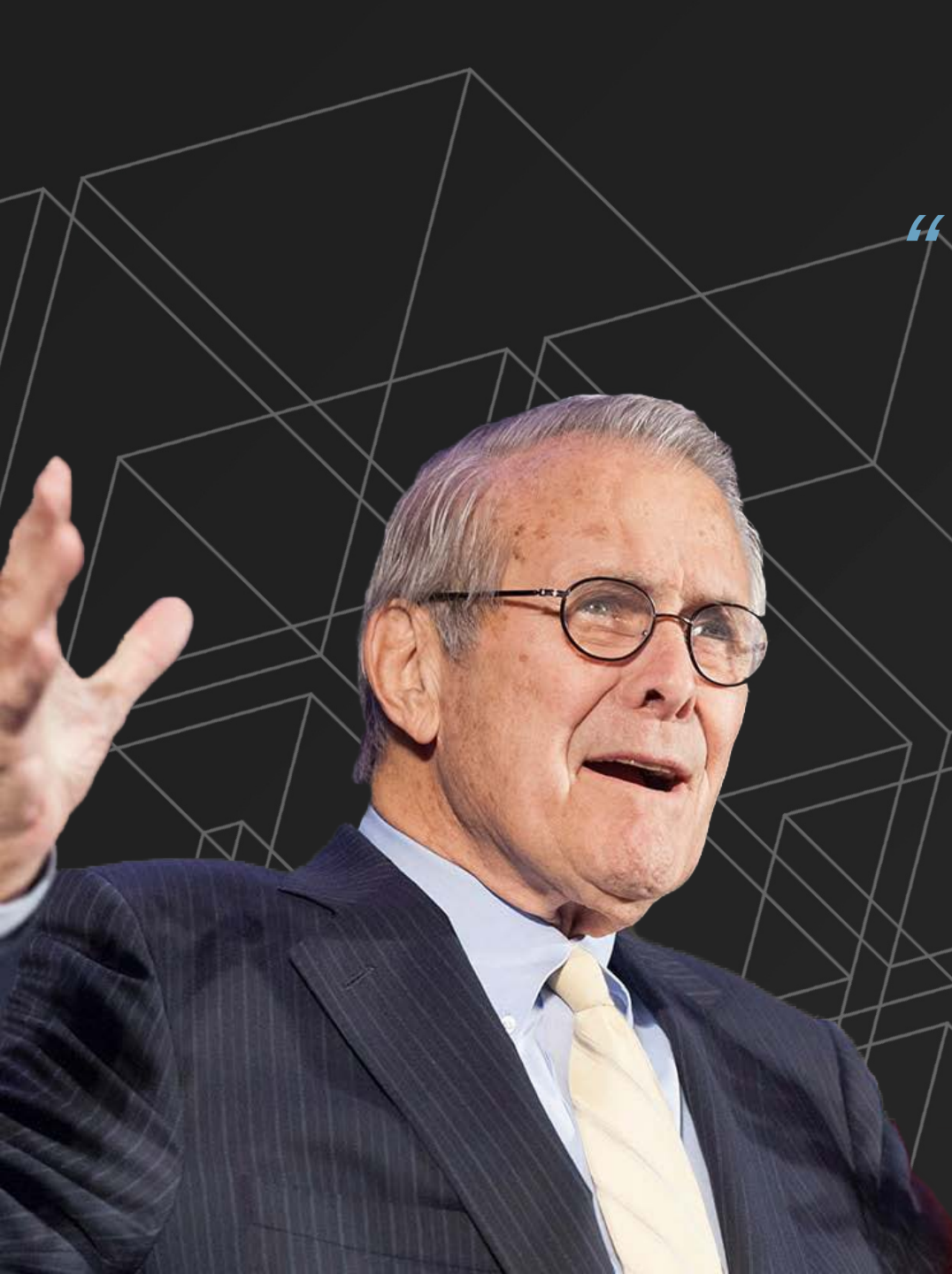


Praktické možnosti predchádzania bezpečnostným incidentom – techniky, technológie a stratégie

Zsolt Géczi, Fortinet, regional account manager

The logo consists of a stylized orange lowercase 'e' followed by the word 'FOCUS' in large, white, bold, sans-serif capital letters.

The logo features the word 'FORTINET' in bold, black, sans-serif capital letters. The letter 'O' is replaced by a red square icon composed of smaller squares. A registered trademark symbol (®) is located at the end of the word.



*“ WE DON’T KNOW
WHAT WE DON’T
KNOW. ”*

Donald Rumsfeld
Former US Secretary of Defense

What Are We Talking About

Data Protection vs. Cyber Security

Data Protection...



...is the process of protecting data and involves the relationship between the collection and dissemination of data...It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

Cyber Security...



...is the body of technologies, processes and practices designed to **protect** networks, computers, programs and **data from attack, damage or unauthorized access.**

The background is a solid orange color with a subtle pattern of hexagons and padlocks. The hexagons are outlined in a lighter orange, and some of them contain a small padlock icon. The padlocks are also in a lighter orange color. The overall effect is a textured, geometric background.

FORTINET AND GDPR.

WHERE, WHAT, WHY AND HOW.

Two Key Aspects of GDPR

1. Consequences for GDPR violations

- Empowers supervisory authorities to assess fines that are “effective, proportionate and dissuasive.”
- Two tiers of maximum fines depending upon severity of violation
 - » **2% or €10M, whichever is higher**
 - » **4% or €20M, whichever is higher**
- Allows data subjects to seek monetary damages in court from controllers who violate their rights and from processors as well.



LET'S PLAY
“WHAT IF”...

Tesco Bank (UK) Data Breach

The Numbers

EARLY
NOVEMBER
2016

£25M
STOLEN FROM
9,000
ACCOUNTS

4
POSSIBLE
EXPLANATIONS

- INSIDER THREAT
- MOBILE APP
- INSUFFICIENT INTERNAL PROCESSES
- REACHED THROUGH 3RD PARTIES

What We Could Expect in the Future...

**TESCO COULD FACE
FINES OF UP TO “£1.9B”
IF GDPR HAD BEEN
IN EFFECT AT THE TIME***

Two Key Aspects of GDPR

2. Data Breach notifications

- A personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
- Data controllers must notify the supervisory authority "competent under Article 55"
- Notice must be provided “without undue delay and, where feasible, **not later than 72 hours** after having become aware of it.”

- Notification to the authority must consist of at least:
 - » Describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected;
 - » Provide the data protection officer’s contact information;
 - » Describe the likely consequences of the personal data breach
 - » Describe how the controller proposes to address the breach, including any mitigation efforts
 - » If data processor experiences a breach, it must notify the controller
- Notice **is not** required if “the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons,”

Looking to the Future - What GDPR Requires



DATA BREACH
DETECTED!



DATA BREACH
REPORTED!

JANUARY 2019

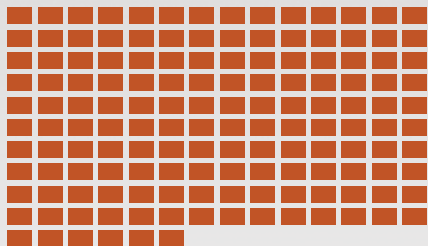
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1	2	3	4
5	6	7	8	9	10	11
12	13 	14	15	16 	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

What Your Network Requires



INITIAL
INTRUSION!

Average time between
intrusion and detection =



146 DAYS*

AUGUST 2018

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20 	21	22	23	24	25
26	27	28	29	30	31	

The Hacker's Advantage:

Window of Opportunity



INITIAL INTRUSION



"WINDOW OF OPPORTUNITY"



BREACH DETECTION

Deloitte Says 'Very Few' Clients Hit by Hack

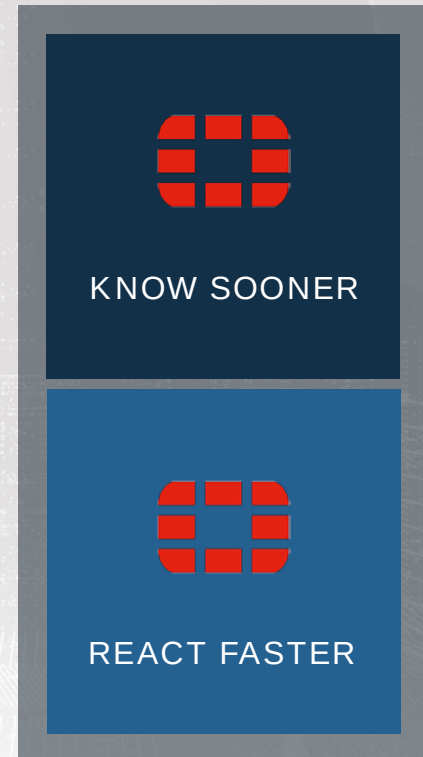


...Deloitte discovered the attack in March, but the hackers may have **had access to the information since October or November 2016**, the newspaper reported...

<http://www.securityweek.com/deloitte-says-very-few-clients-hit-hack>

The Fortinet Objective:

Close the Window of Opportunity



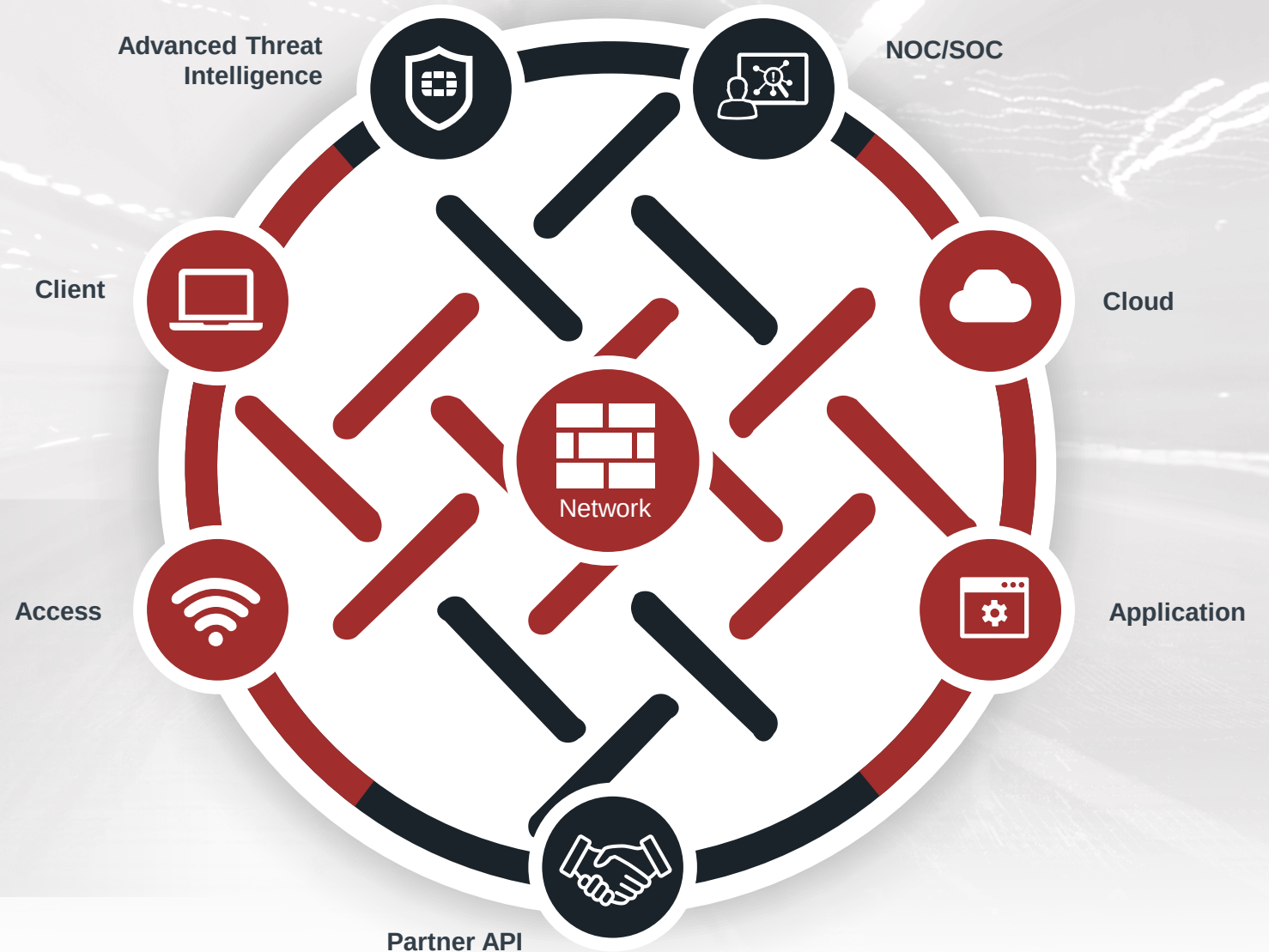
THE ROAD TO GDPR COMPLIANCE

The First Step...

...towards GDPR Compliance



 BROAD
 POWERFUL
 AUTOMATED



Technology Integration and Collaboration



APPLICATION SECURITY

- FortiMail
- FortiWeb
- FortiADC
- FortiDDoS
- FortiWAN
- FortiCache



SECURE ACCESS

- FortiAP
- FortiWiFi
- FortiSwitch
- FortiAuthenticator
- FortiToken
- FortiExtender



ENTERPRISE FIREWALL

- FortiGate
- FortiWiFi



CLOUD SECURITY

- FortiGate VM (Virtual FW)
- FortiGate VMX (SDN Virtual FW)
- FortiGate VM for Public Cloud
 - » AWS
 - » Microsoft Azure
 - » OpenStack



ADVANCED THREAT PROTECTION

- FortiSandbox
- FortiMail
- FortiWeb
- FortiClient



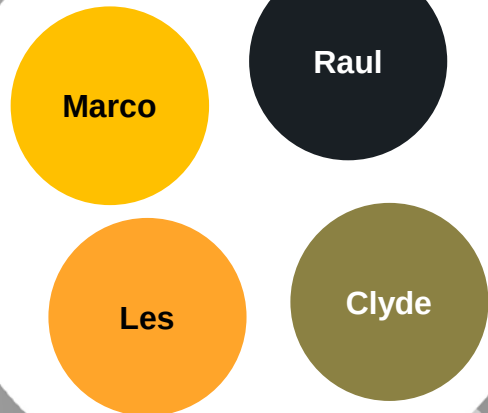
SECURITY OPERATIONS

- FortiManager
- FortiAnalyzer
- FortiSIEM

PSEUDONYMIZÁCIA A SEGMENTÁCIA

Pseudonymizácia vs. Anonymizácia

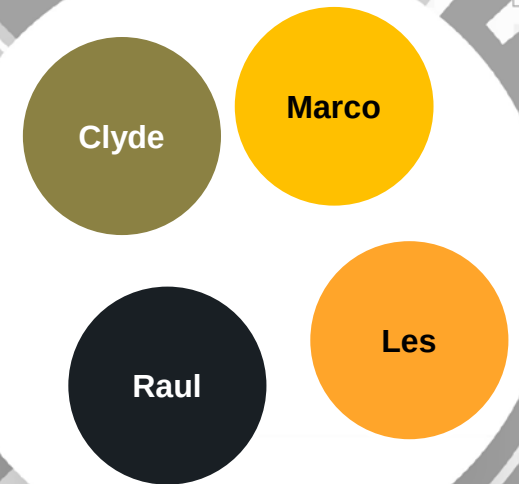
Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxxx
Marco	Loqfh	xxxxxx
Les	Mcv	xxxxxx
Les	Mcv	xxxxxx
Marco	Loqfh	xxxxxx
Raul	BhQl	xxxxxx
Clyde	qOerd	xxxxxx



Pseudonymized
Data Record

*“Pseudonymizácia je metóda
nahrádzania identifikovateľných
údajov s reverzibilnou, konzistentnou
hodnotou.*

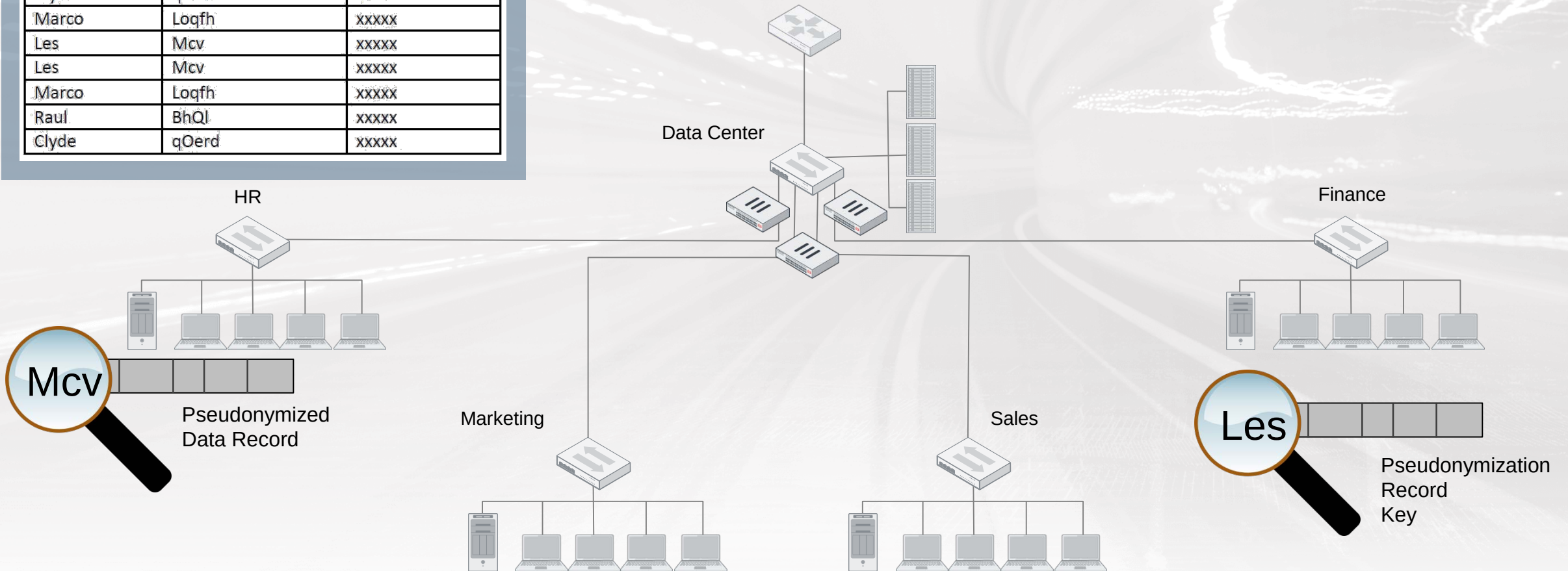
*Anonymizácia je zničenie
identifikovateľných údajov.”*



Anonymized Data
Record

Segmentation for Increased Data Protection

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	XXXXX
Marco	Loqfh	XXXXX
Les	Mcv	XXXXX
Les	Mcv	XXXXX
Marco	Loqfh	XXXXX
Raul	BhQl	XXXXX
Clyde	qOerd	XXXXX



The background of the slide features a light gray hexagonal grid pattern. Within this grid, several white padlock icons are scattered, some appearing slightly more prominent than others. The overall aesthetic is clean and technical, suggesting a focus on security or risk management.

CONTINUOUS RISK ASSESSMENT

FortiGuard

Since 2000, FortiGuard Labs has provided in-house, industry-leading security intelligence and research, powering the Fortinet Security Fabric and delivering a suite of advanced security services



FortiGuard Research

Zero-Day Research



82 found in 2016

36 still unpatched by vendors

IoT Research



Product vulnerabilities

Protocol weaknesses

Innovation



Finding new ways to solve problems

Dealing with increases in volume, sophistication and breadth of attacks

Collaborative Research



Working with research partners which include national CERTs and law enforcement organisations

FortiGuard Threat Intelligence Projects



The Road to GDPR Compliance

So Much More Than Just Technology

Complex



Potentially long,
complicated
and expensive

Impact



Potential impact across
the whole of the
organization

Product/Service
Process
People

Threat



Think ahead of the
Threat – Close the
“Window of Opportunity”

“Harden” the Network

FORTINET®



Ďakujeme za pozornosť

