Contención con Inteligencia

Jean Carlos Bardot

Qué entendemos por “Inteligencia” ?

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

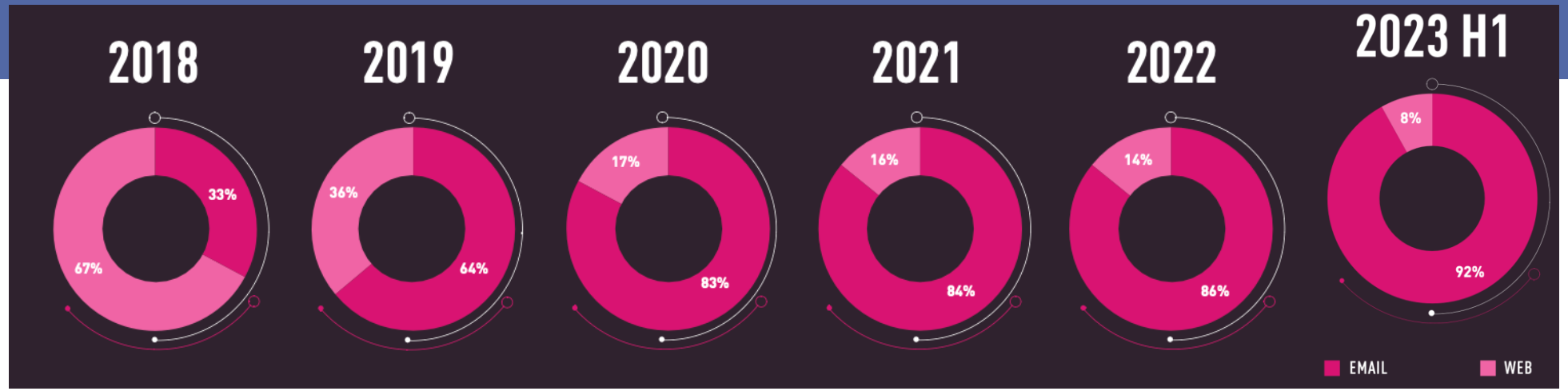
- Capacidad para pensar de manera abstracta.
- Capacidad para actuar con un propósito concreto, pensar racionalmente y relacionarse eficazmente con el ambiente.
- Capacidad para adaptarse al ambiente.

Inteligencia (RAE)

1. f. Capacidad de entender o comprender.
2. f. Capacidad de resolver problemas.
3. f. Conocimiento, comprensión, acto de entender.
4. f. Sentido en que se puede tomar una proposición, un dicho o una expresión
5. f. Habilidad, destreza y experiencia.

Algo de Contexto…

Vectores de ataque dirigidos a usuarios/clientes



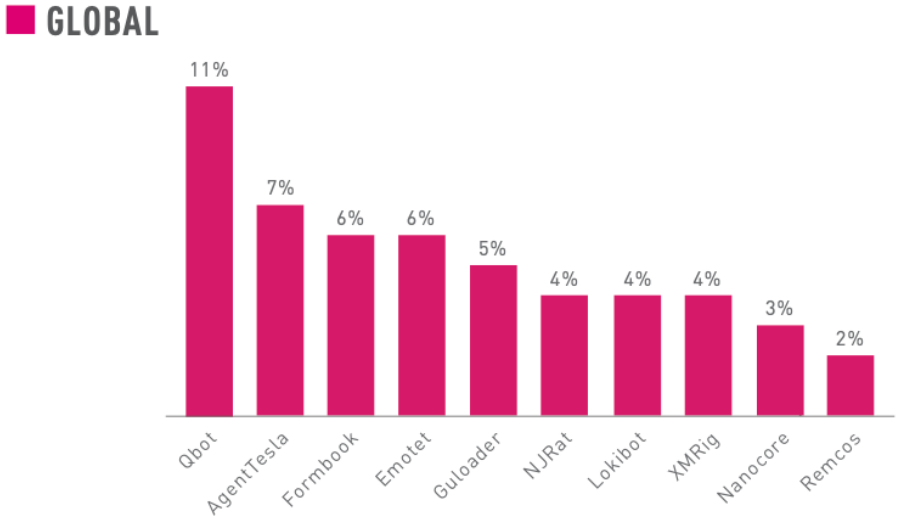


Figure 7. Most prevalent malware globally—H1 2023

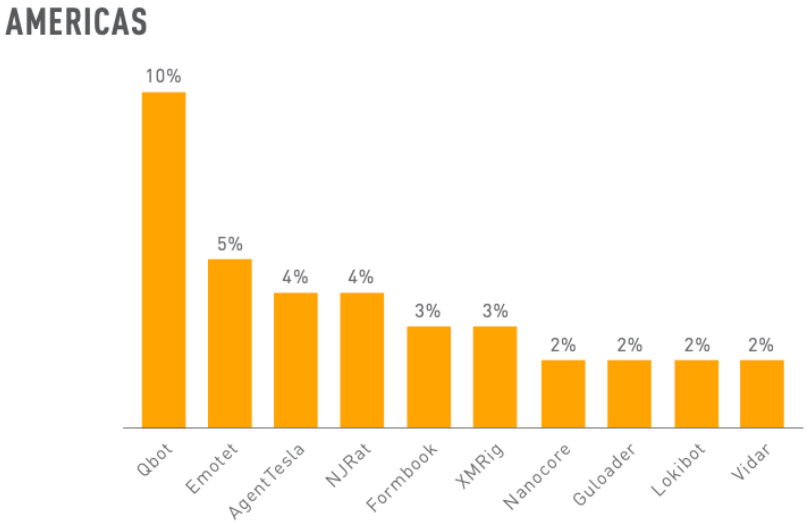


Figure 8. Most prevalent malware in the Americas—H1 2023

Fuentes:
- Checkpoint: Mid-Year Cyber Security Report 2023
- Sophos: The State of Cybersecurity 2023

Algo de Contexto…

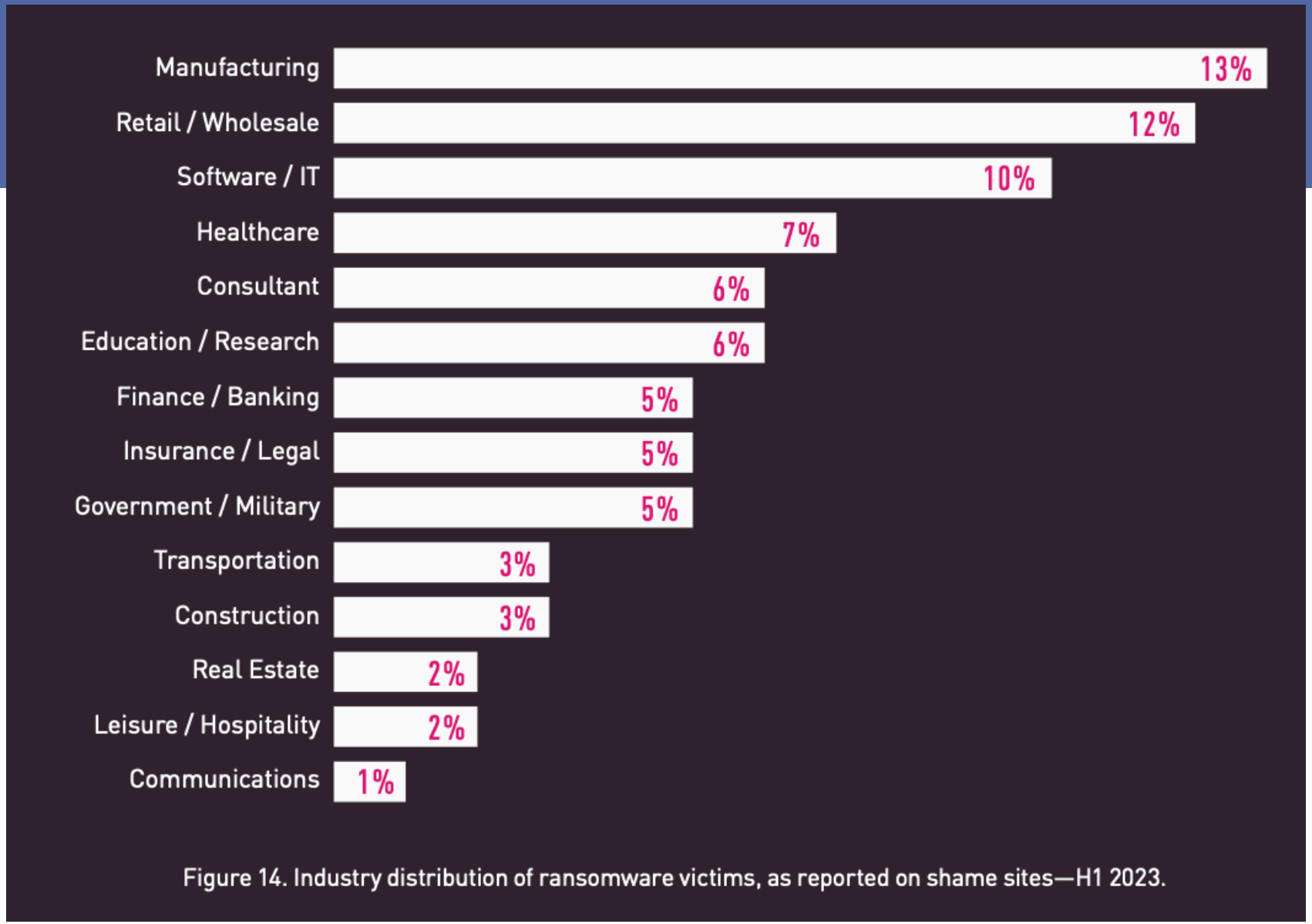


Figure 14. Industry distribution of ransomware victims, as reported on shame sites—H1 2023.

Los ataques van hacia donde sean más productivos

Fuentes:
- Checkpoint: Mid-Year Cyber Security Report 2023
- Sophos: The State of Cybersecurity 2023

Algo de Contexto…

Cuál es su mayor preocupación??

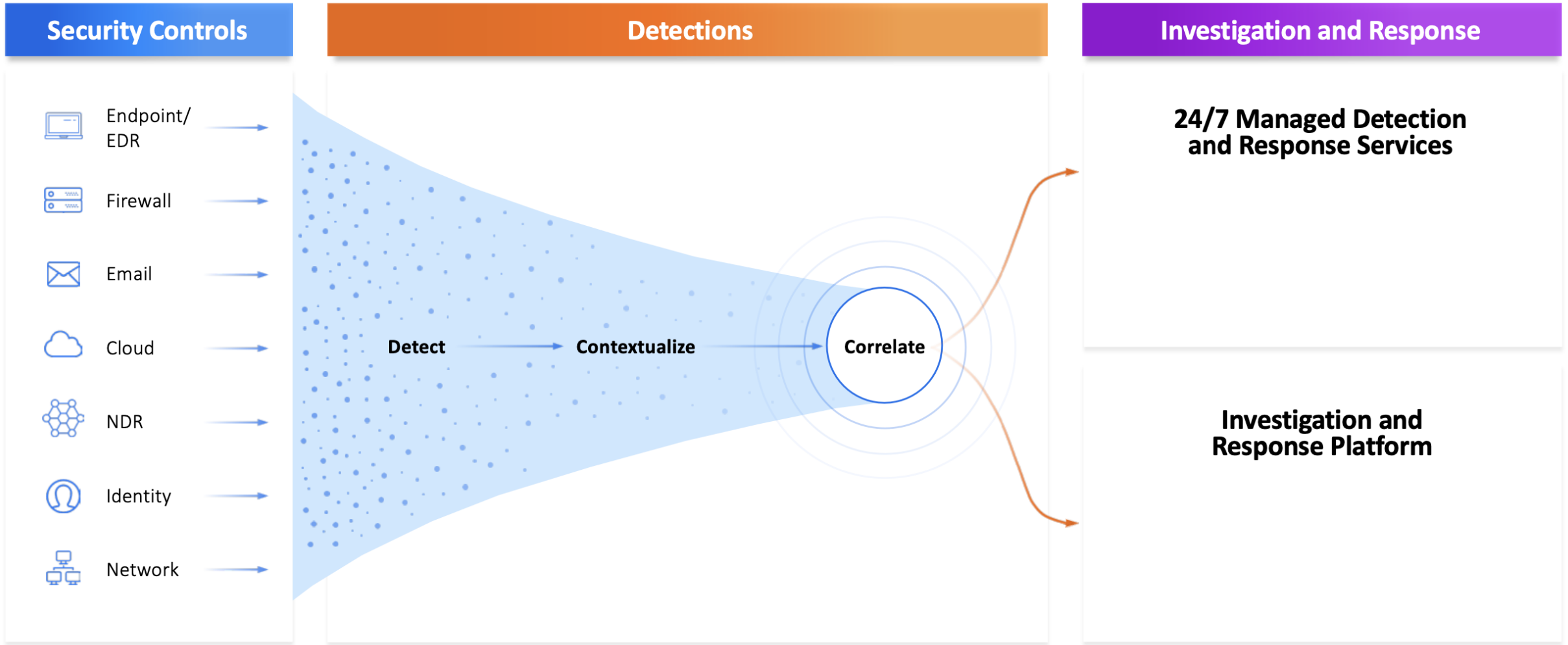
AMENAZA	% de Encuestados

Thinking about 2023, which cyberthreats are you most concerned about affecting your organization? (n=3,000)

Fuentes:
- Checkpoint: Mid-Year Cyber Security Report 2023
- Sophos: The State of Cybersecurity 2023

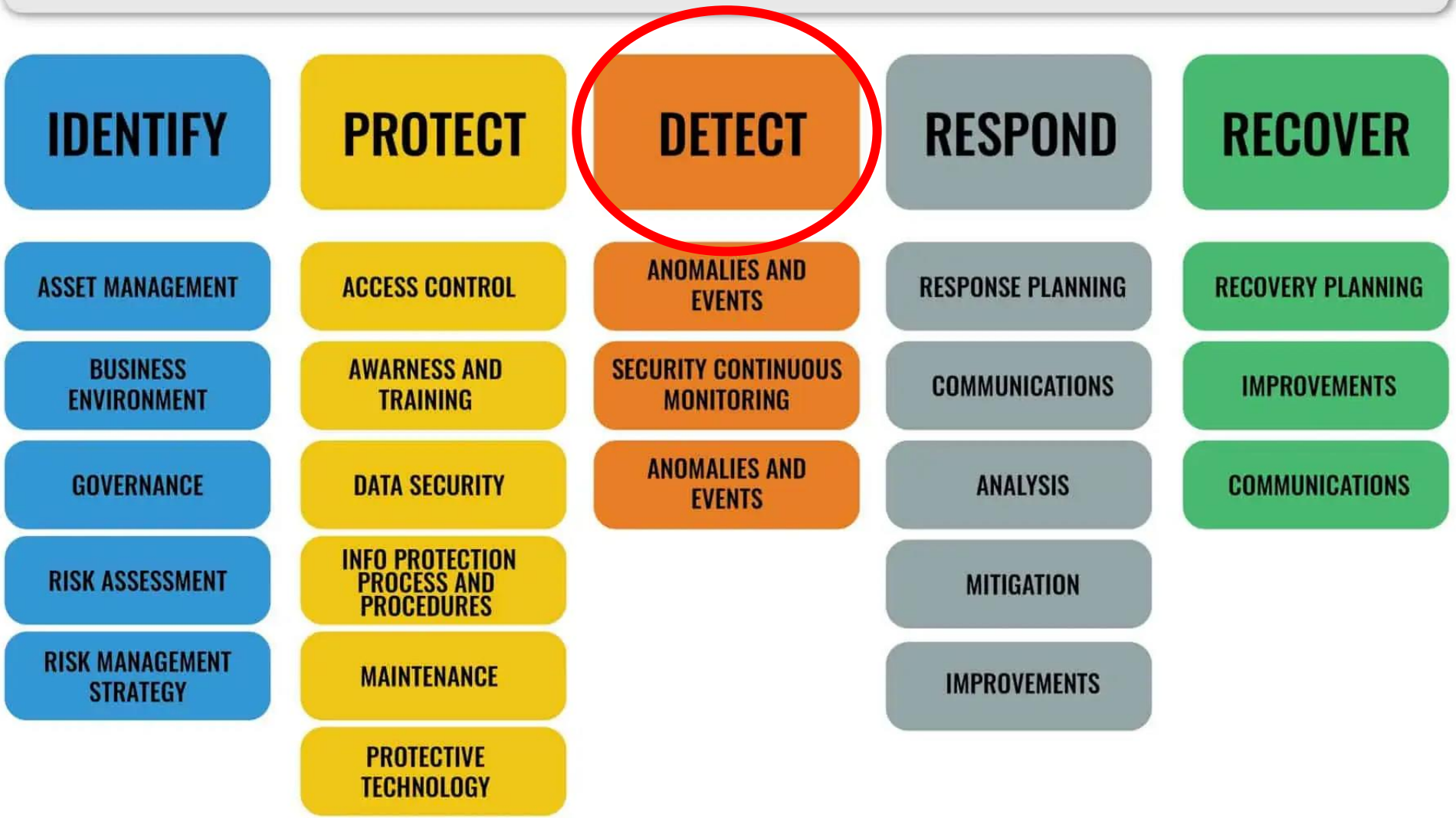
Algo de Contexto…

Cuál es el reto?



- Checkpoint: Mid-Year Cyber Security Report 2023
- Sophos: The State of Cybersecurity 2023

NIST CYBER SECURITY FRAMEWORK CORE



Algo de Contexto…

Cuál es el reto?

Median time to detect, investigate, and respond to an alert

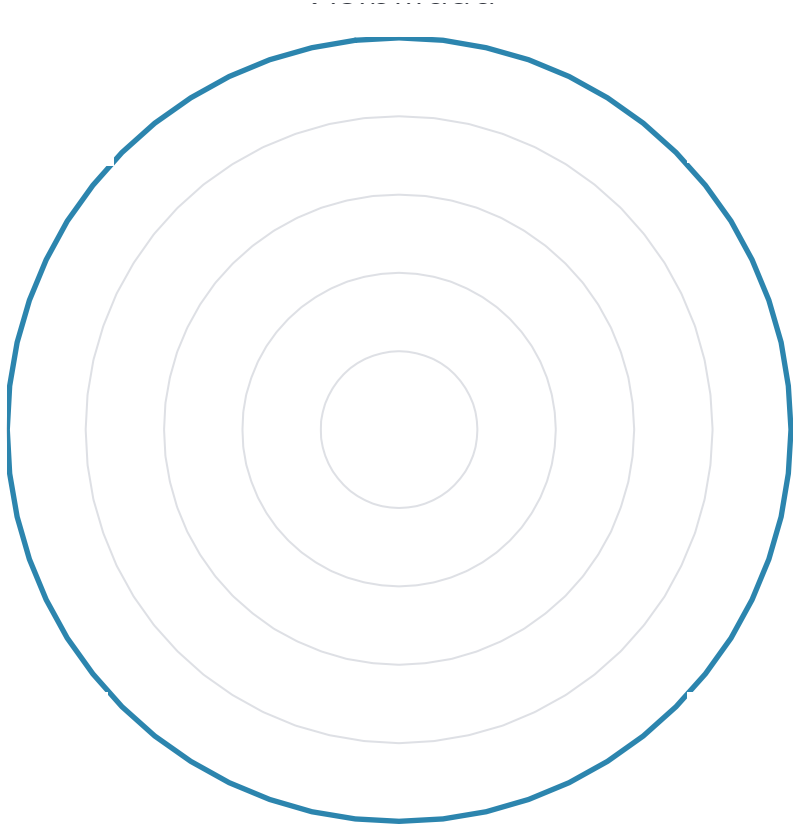
ACTIVITY	100-3,000 EMPLOYEES (n=2,460)	3,001-5,000 EMPLOYEES (n=350)	IT, TECHNOLOGY AND TELECOMS (n=98)	MANUFACTURING AND PRODUCTION (n=331)	ENERGY, OIL/GAS AND UTILITIES (n=66)
Detection					
Investigation					
Response					
Total					

How long does it take for your organization to detect, investigate and, when necessary, remediate a potential incident?
(n=2,812 respondents that investigate alerts in-house)

Fuentes:
- Checkpoint: Mid-Year Cyber Security Report 2023
- Sophos: The State of Cybersecurity 2023

Vectores de Contención

1. Visibilidad
2. Calidad del dato
3. Oportunidad / Latencia
4. Procesamiento / Análisis
5. Correlación / Priorización
6. Reacción / Decisión
7. Contención
8. Automatización



Contención Inteligente

- Madurez (Vectores)
- Responsabilidad
- Autoridad
- Confianza
- Inversión
- Capacitación
- Automatización

Contención con Inteligencia