Driving operational resilience by securing your digital ecosystem with Mastercard

Cyber Security Forum – Sofia, Bulgaria

Samuel Ojeme
Director, Cyber Security & Resilience
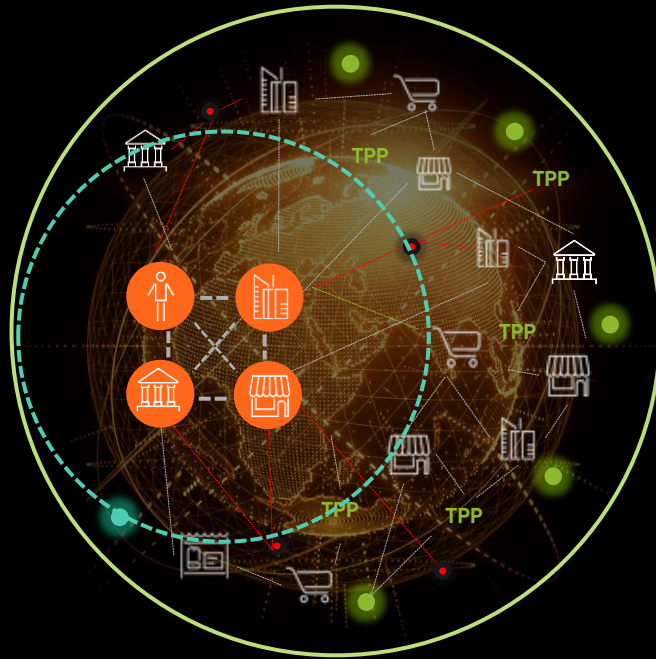Cyber & Intelligence Solutions, Europe

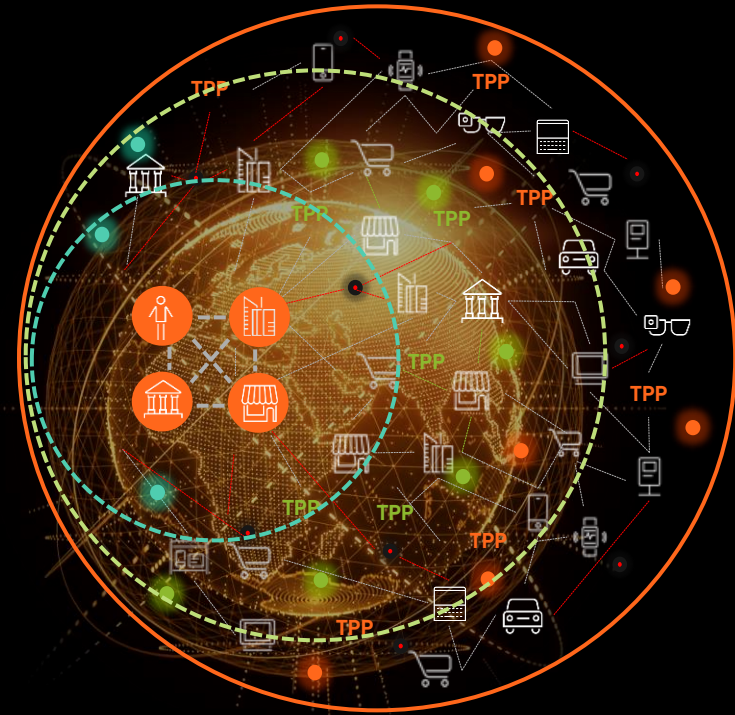# Safeguarding an evolving ecosystem goes beyond protecting transactions

Early Ecosystem

- Mainly physical interactions
- Protected connections
- Limited large-scale threat
- Lone Wolf Cyber Attacks

Expanding Ecosystem

- Growing digital interactions
- Unprotected connections
- Increased large-scale threat
- Organized Cyber Crime Groups

Evolving Ecosystem

- Infinite IoT interactions growth
- Countless unprotected connections
- Infinite large-scale threat
- Organized Crime / Nation State Attacks

We are evolving with the ecosystem...from securing transactions to protecting trust in every interaction

Enhance security in the consumer digital transaction journey

Expand security beyond transactions to cyber environments

DIGITAL **FINANCIAL** **CYBER** **SYSTEMIC**

Extend security to other types of transactions beyond cards

Extend security to mitigate systemic operational risk

One trusted source for protection

Mastercard's solutions enable businesses to protect the people, transactions and devices that power their business, from the outside and the inside
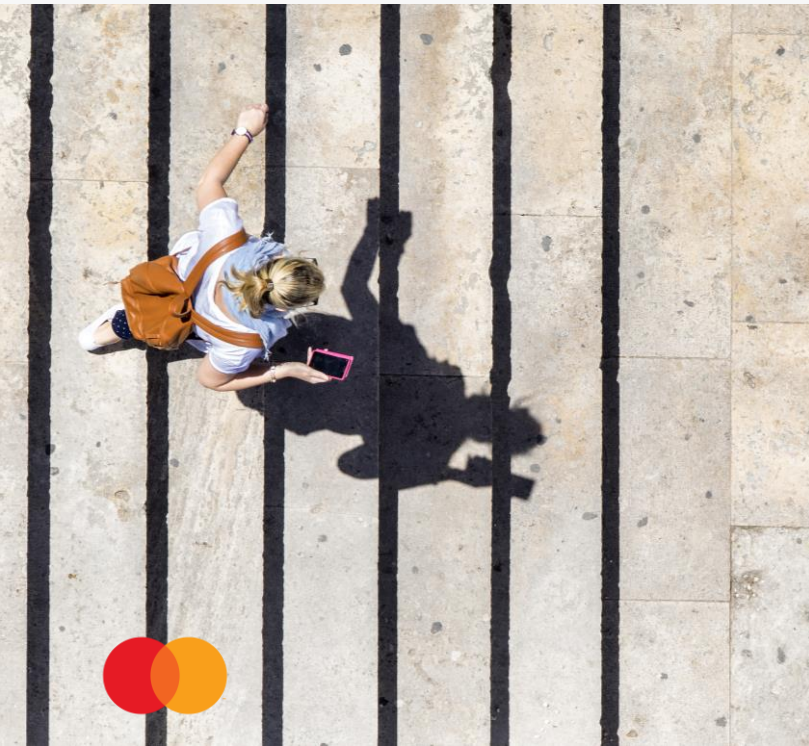
From the Outside-in:
Detect & Protect

From the Inside-out:
Assess, Advise & Simulate

Provide automated and objective assessments of your infrastructure

Identify, Prioritise & Mitigate vulnerabilities

Continuous and actionable understanding of Nth party risk

Tailor solutions to risk tolerance and regulatory / compliance frameworks

Measure cyber risk in business terms

Improve employee awareness & resilience

Leverage data, reporting and action plans to build cyber security culture

Receive expert advice, continuous support & technical advice

CYBER SECURE

ADC insights and cyber risk assessment

RISKRECON
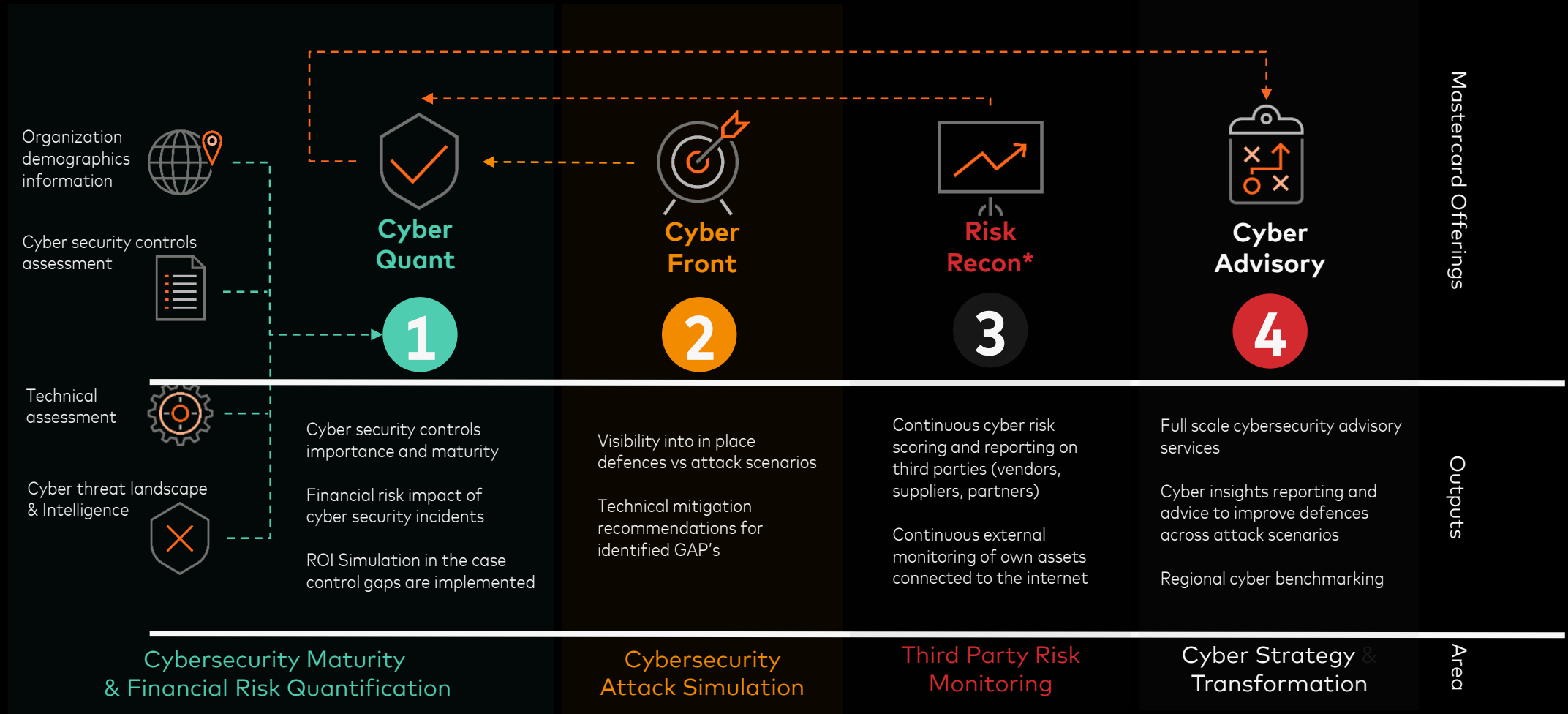
Cyber risk ratings of third-party relationships

ONBOARD RISK CHECK

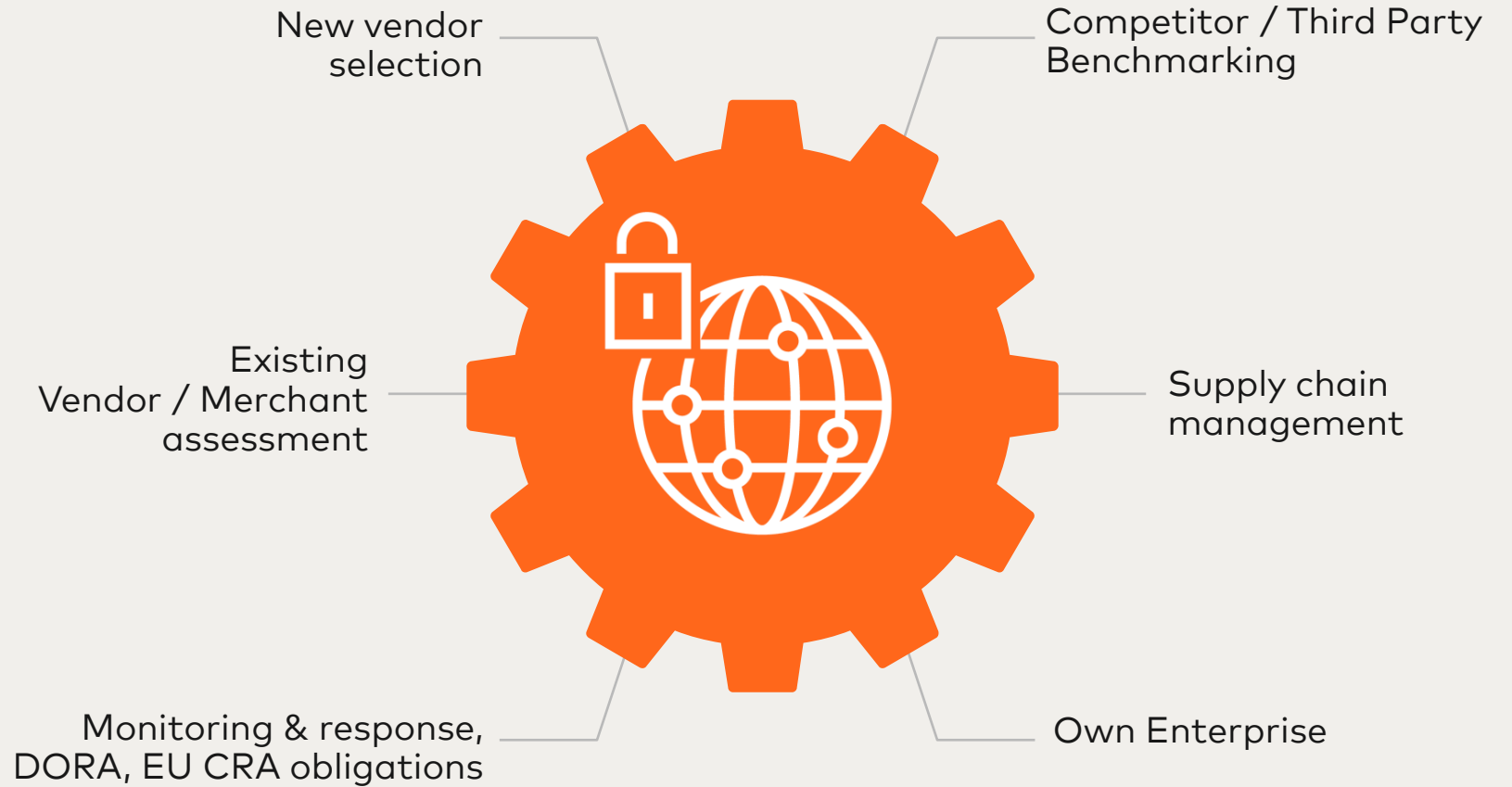Due diligence of Acquirer's prospective merchants

How we help our customers to improve their cybersecurity capabilities as a strong core of their digital resilience.

Mastercard Offerings

Organization demographics information

Cyber security controls assessment

Technical assessment

Cyber threat landscape & Intelligence

Cyber Quant — **1**

Cyber Front — **2**

Risk Recon* — **3**

Cyber Advisory — **4**

Outputs

Cyber Quant	Cyber Front	Risk Recon*	Cyber Advisory
Cyber security controls importance and maturity	Visibility into in place defences vs attack scenarios	Continuous cyber risk scoring and reporting on third parties (vendors, suppliers, partners)	Full scale cybersecurity advisory services
Financial risk impact of cyber security incidents	Technical mitigation recommendations for identified GAP's	Continuous external monitoring of own assets connected to the internet	Cyber insights reporting and advice to improve defences across attack scenarios
ROI Simulation in the case control gaps are implemented			Regional cyber benchmarking

Area

Cybersecurity Maturity & Financial Risk Quantification	Cybersecurity Attack Simulation	Third Party Risk Monitoring	Cyber Strategy & Transformation

Securing Business Outcomes

New vendor selection

Competitor / Third Party Benchmarking

Existing Vendor / Merchant assessment

Supply chain management

Monitoring & response, DORA, EU CRA obligations

Own Enterprise

*FUTURE CAPABILITY

The business value of Cyber Resilience

Increase cyber resilience and security across your entire digital ecosystem

Create a secure and resilient organization by continuously identifying and mitigating vulnerabilities and risks to your business from cyber criminals who will attack your organization and your supply chain .

Proactively reduce financial losses from cyber attacks

Advanced third-party assessments ensure your cyber environment is not in danger of compromise via vulnerable third-party suppliers, vendors or merchants.

Competitive advantage and reputation

Enable a more resilient and competitive organization by ensuring confidentiality, integrity and availability of data which appeals to customers, investors, shareholders and your Board.

Drive legislative and regulatory compliance across your portfolio

Ensure compliance with existing cyber security legislation and frameworks to suit your individual business requirements such as NIST, ISO, PCI DSS and GDPR. Align with the implementation of Digital Operational Resilience Act (DORA).

Accurate, automated and actionable assessments

Accurate and verifiable data of third-parties collected from public domains ensures cyber risk assessments are completely reliable. Automated third-party risk assessments reduce the time taken and identify risks quicker.