



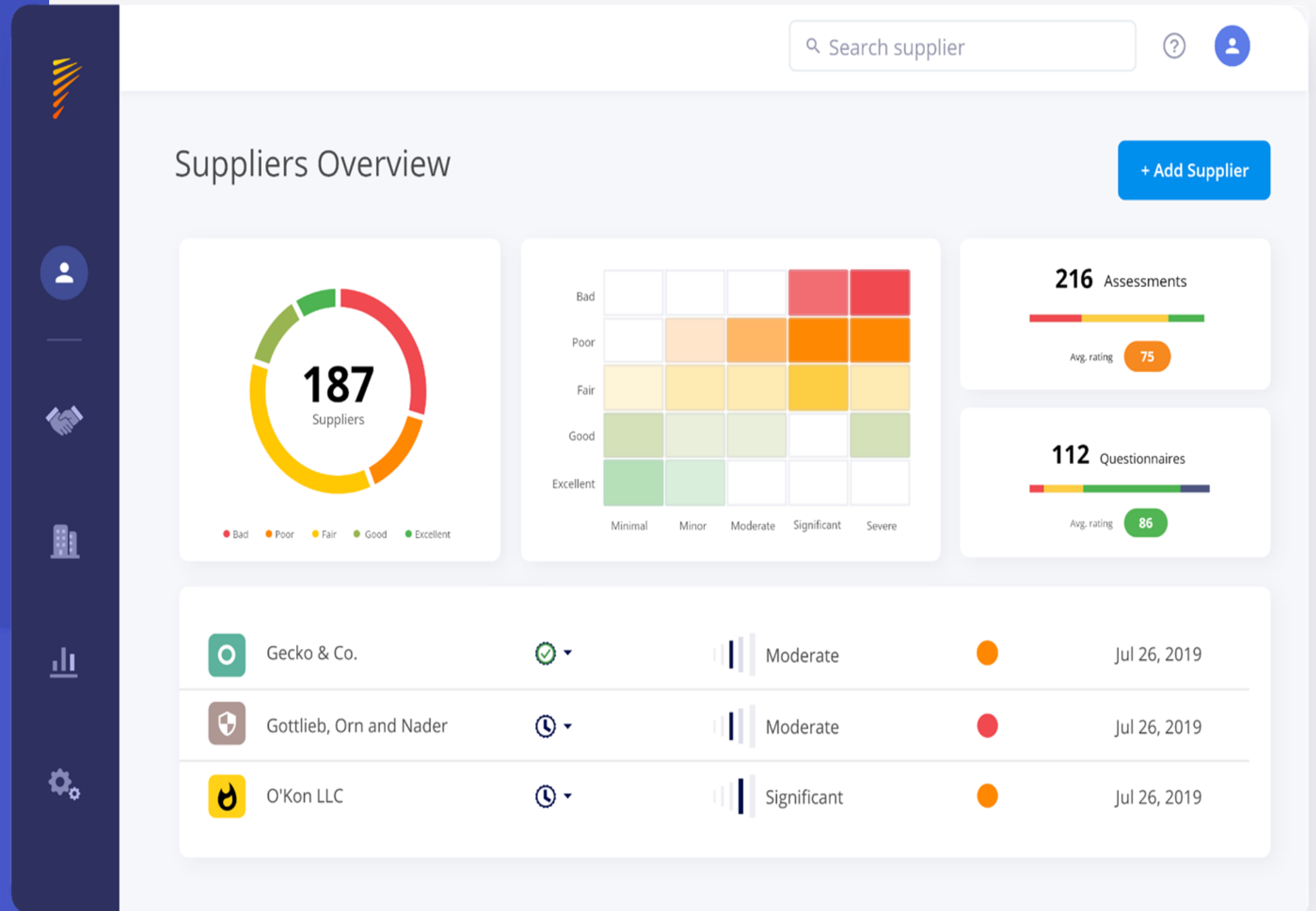
End-to-End Third-Party Cyber Risk Management

Matt Pearson

EMEA Channel Director

2024

Panorays provide a platform to manage the risk associated with sharing data with third parties



Third-Party Security Risk - **Why now?**



Reduce Risk

An average company shares data with

583 third parties*

54% of organizations
breached through third parties in
2022**



Comply With Regulation

Regulatory requirements around Third
Party Risk Management

**NIS2, DORA, HIPAA, GDPR,
PCI DSS, SBOM, etc.**



Save Costs

Third Party Risk Management will
free up your resources, both **Human
and Capital**

Third Party Cyber Risk Loss Events

Third Party
Availability

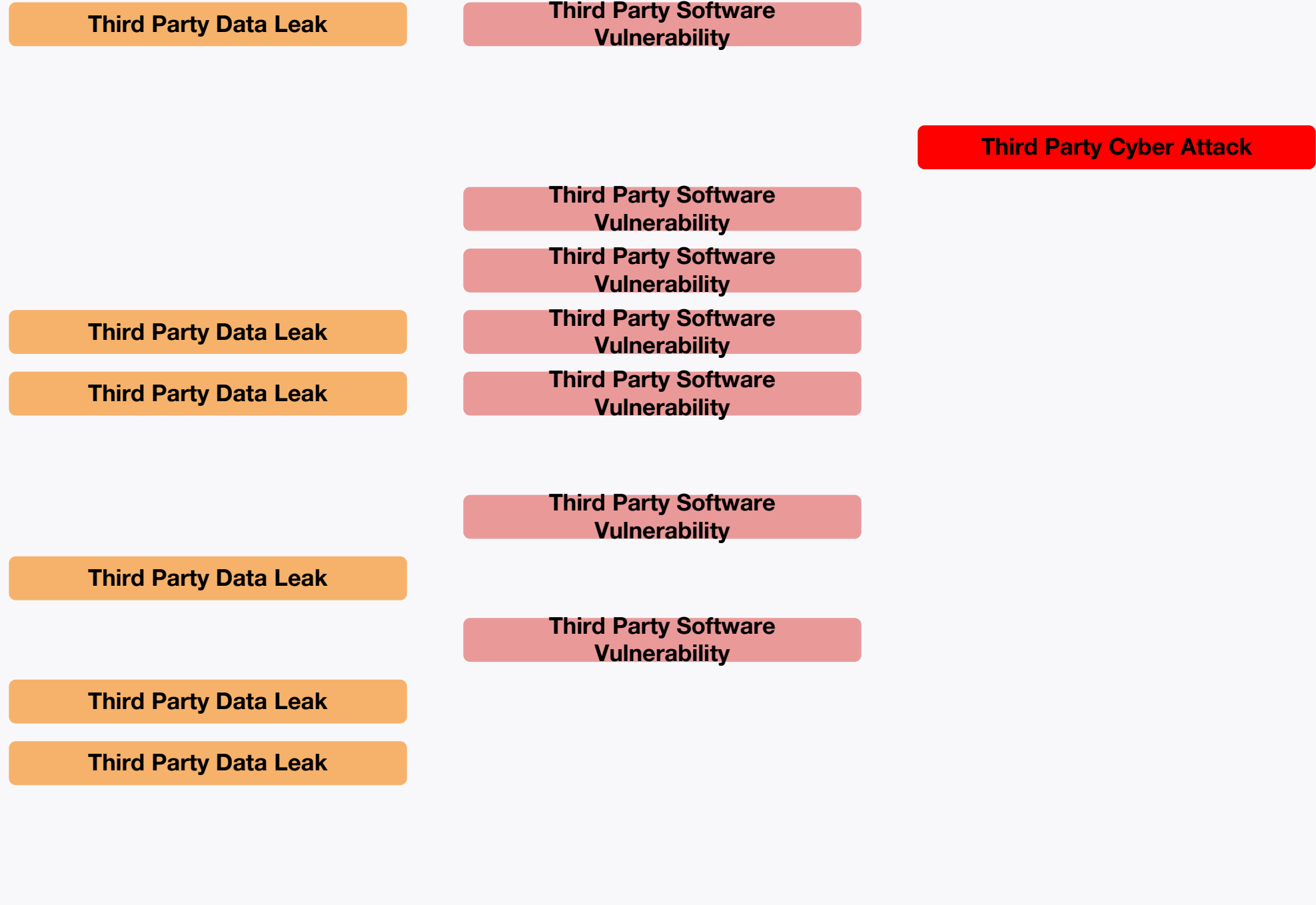
Third Party Data
Leak

Third Party Software
Vulnerability*

Third Party Cyber
Attack

Top Cyber Attacks of 2023

1. MOVEit Attacks
2. Casino Operator Attacks
3. 3CX Software
4. The UK Electoral Commission
5. ESXi Ransomware Attacks
6. GoAnywhere Attacks
7. PBI Research Services Breach
8. Royal Mail LockBit Attack
9. Barracuda Email Gateway
10. Microsoft Cloud Email Breach
11. Cisco IOS XE Attacks
12. Okta Support System Breach
13. DarkBeam
14. 23andMe Data Breach
15. ION Trading Technologies



Sources:
<https://www.crn.com/news/security/10-major-cyberattacks-and-data-breaches-in-2023?page=2>
<https://www.infosecurity-magazine.com/news-features/top-cyber-attacks-2023/>
<https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2023/>
<https://www.welivesecurity.com/en/cybersecurity/year-review-10-biggest-security-incidents-2023/>

Security Teams Are Overwhelmed

- Security Managers can't scale their programs
- Current systems are siloed, manual and unsuited to task
- Stakeholders lack visibility into critical business risk
- The organization has no way to respond to critical events

Acme Ltd New Vendor Profile Questionnaire			
Requestor Complete			
#	Question	Response Format	Response
1	Requestor Name		
2	Department		
3	Date Requested		
4	Vendor Name		
5	Vendor Function (in words)		
6	How critical will this relationship be to the business	1-5 1=not critical at all 5=very critical	
7	What kinds of data will be shared with the prospective vendor?		
	Sensitive Personal Data		
	Sensitive Corporate Data		
	Publicly-Available Data		
	No Data will be Shared		
8	What access will the vendor have to:		
	Network and/or Data Systems	Yes/No	
	Offices and Other Facilities	Yes/No	
9	Analyst Name		
10	Analyst General Comments		

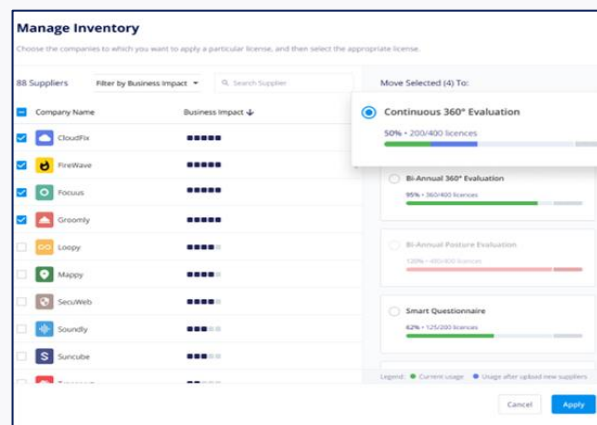
End to End Third Party Security Risk Management

01

Prioritization

Identify your third parties and tier them by inherent risk

Business Impact Classification
Third Party Inventory

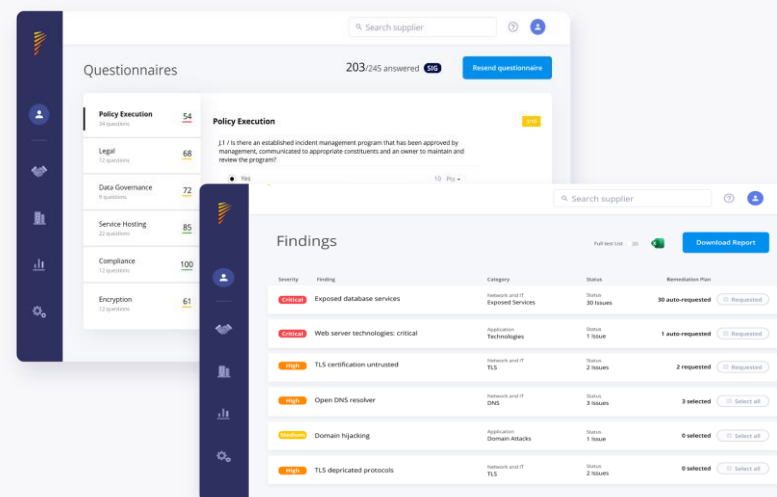


02

Evaluation

Choose the optimal evaluation process based on your risk appetite

Automated Questionnaires
Cyber Assessments (SRS)
Correlated Insights

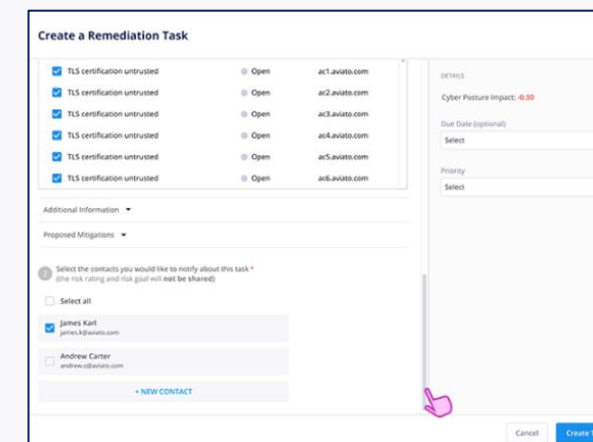


03

Mitigation

Help your third parties mitigate security gaps and reduce risk

Remediation Management

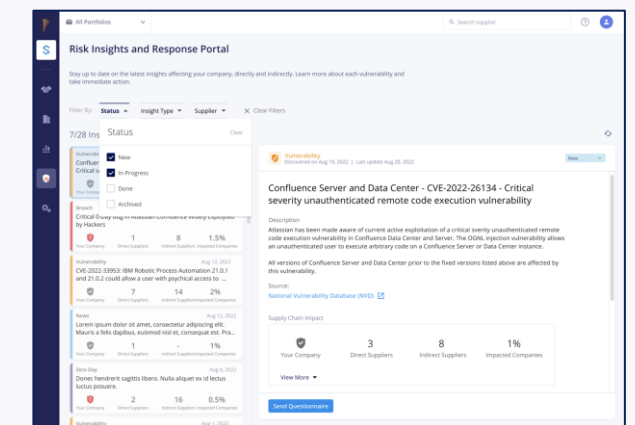


04

Continuous Monitoring

Monitor and re-evaluate third parties for changes in cyber posture and respond if needed

Real time alerts
Automated reevaluation
Risk Insights and Response



Accurate, thorough and actionable understanding of evolving Third Party Cyber Risk

DORA Compliance: Third Party ICT Risk

- Information Communication Technologies (ICT)-risk management framework
- Strategy for managing third-party ICT risk
- Register of information
- Exit strategy
- Contractual provisions
- Incident reporting

12/2023 Draft Regulatory Technical Standards

DORA Compliance: Third Party ICT Risk

How Panorays helps

- Information Communication Technologies (ICT)-risk management framework
- **Strategy for managing third-party ICT Risk**
- **Register of information**
- Exit strategy
- Contractual provisions
- **Incident reporting**

12/2023 Draft Regulatory Technical Standards





















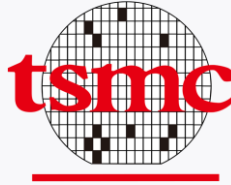







Digital Supply Chain Monitoring is Critical

Monitoring of the entire ICT subcontracting chain by the financial entity

“The financial entity must fully monitor the ICT subcontracting chain and must document it.”

JC 2023 67 27 November 2023 Consultation Paper on Draft Regulatory Technical Standards

Customers and Partners

Financial	Healthcare	Insurance	Media	Retail	IT & Services
   	   	   	  	  	  
Technology	Automotive	Utilities	Manufacturing	Software	Transportation
 	   Mercedes-Benz	  	   	  	  

Average Customer Size –

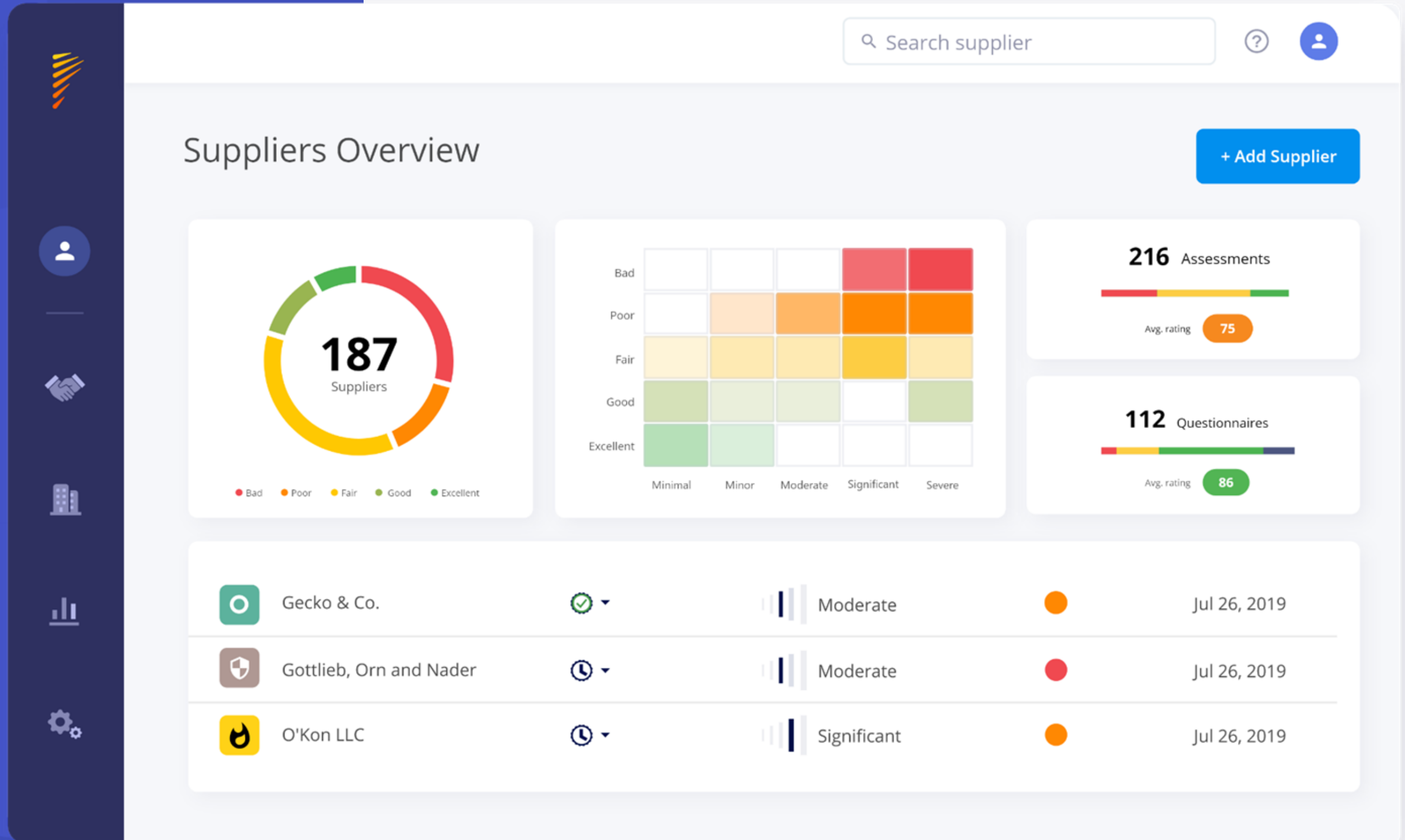
25 - Critical Vendors = £800 per vendor per year

25 – Semi critical vendors = £400 per vendor per year

25 – Non-critical vendors = £200 per vendor per year

Includes onboarding and customer success team access

Demo



Thank You.

Name

Title

xxxx@panorays.com

+972 xx xxxxxxxx