DVV solutions

BlueVoyant®

Third Party Risk Webinar:

Turning Cyber Risk Ratings Into Cyber Risk Reduction

20th May 2021

Your Expert Panel

Nick Trigg

Enterprise Risk Management Consultant

BlueVoyant

Sean O'Brien CTPRP, CTPRA

Managing Director

DVV Solutions

Growing Interconnected Ecosystems

Diagram from Deloitte Supply Chain & Digital Analytics Survey 2019

Key Drivers, Growing Threats & Regulatory Compliance

How the SolarWinds hack and COVID-19 are changing cybersecurity spending

5 MAR 2021 NEWS
SITA Supply Chain Breach Hits Multiple Airlines

71% of Employees Globally Admit to Sharing Sensitive and Business-Critical Data Using Instant Messaging and Business Collaboration Tools,

A Casino Gets Hacked Through a Fish-Tank Thermometer

6 MAY 2021 NEWS
Half of UK Manufacturers Suffered a Cyber-Attack Last Year

After refusing to pay ransom, US-based auto parts distributor has sensitive data leaked by cybercriminals

New type of supply-chain attack hit Apple, Microsoft and 33 other companies

Authority	Framework	Assessment Required	Monitoring Required
Regulations			
FCA	FG 16/5	✓	✓
EU	GDPR / UK Data Protection Act 2018	✓	✗
	Digital Operational Resilience Act (DORA)	✓	✓
	MiFID II	✓	✗
EBA	Guidelines on Outsourcing Arrangements	✓	✓
Guidelines			
PRA	Operational Resiliency	✓	✓
ESMA	ICT Technology Risk Management & Cybersecurity	✓	✓
MAS	Technology Risk Management	✓	✓
Industry Standards			
ISO	27001:2013	✓	✓
	27002:2013	✓	✓
	27018:2019(E)	✓	✓
NIST	SP 800-53R4	✓	✗
	CSF 1.1	✓	✓

Challenges in Cyber Risk & Continuous Monitoring

Cyber Threat Landscape Exponentially Growing

- Increasingly complex Cyber Supply Chains driven by digital transformation
- Supply Chain has now become a **Primary Route for attackers**
- COVID has forced us all to look more closely and **monitor more frequently**
- SolarWinds has forced us to reassess which suppliers to assess, **moving downstream from T1 & T2**
- PRA/FCA & EBA guidelines driving UK & EU financials to broaden TPRA into **4th, 5th & nth parties**
- Net result is a **extensive growth in how many suppliers we need to monitor**

Cyber Security Scorecards are a great method of identify potential risks, however

- They are **heavily reliant upon people** and
- Simply **do not scale**

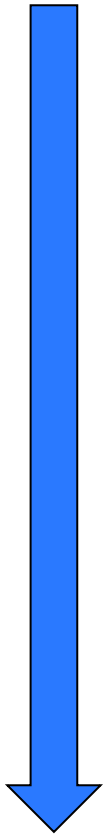
Desired Outcome

To manage the Cyber Risk Exposure within Third Parties

- ✓ To a required threshold
- ✓ In the most reliable, effective, and efficient manner
- ✓ On a continuous basis
- ✓ Move from 'Actionable Insights' to 'Insightful Action'

Third Party Cyber Risk | Key Fundamentals

Whether a program is managed in-house, outsourced, or managed in a hybrid model, an effective third party cyber risk management program incorporates the following core components



Visibility

- Coverage, Accuracy, Completeness
- Near Real Time
- Evidence-Based
- Objective / Data-Driven

Analysis (risk-based approach)

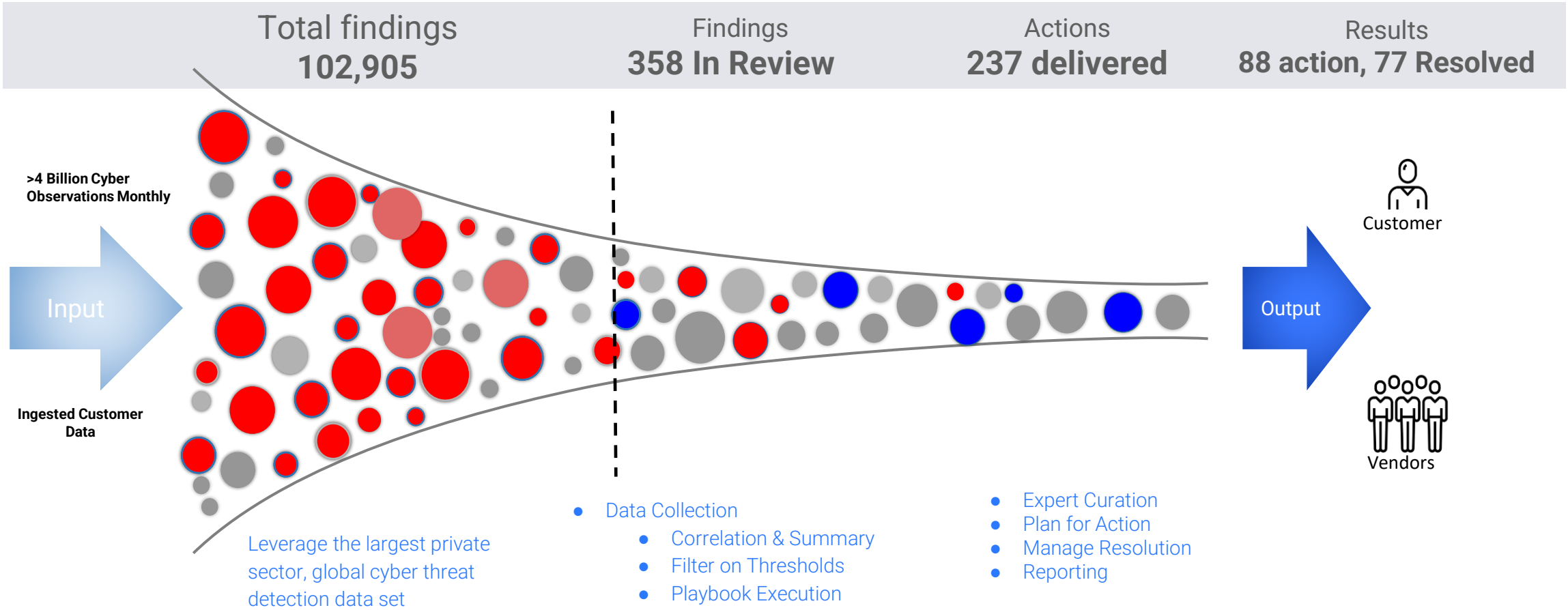
- Business-Relevance and Context
- Trend Analysis
- Significant Changes
- Risk Tolerance to Breach
- Noise Filtering

Resolution

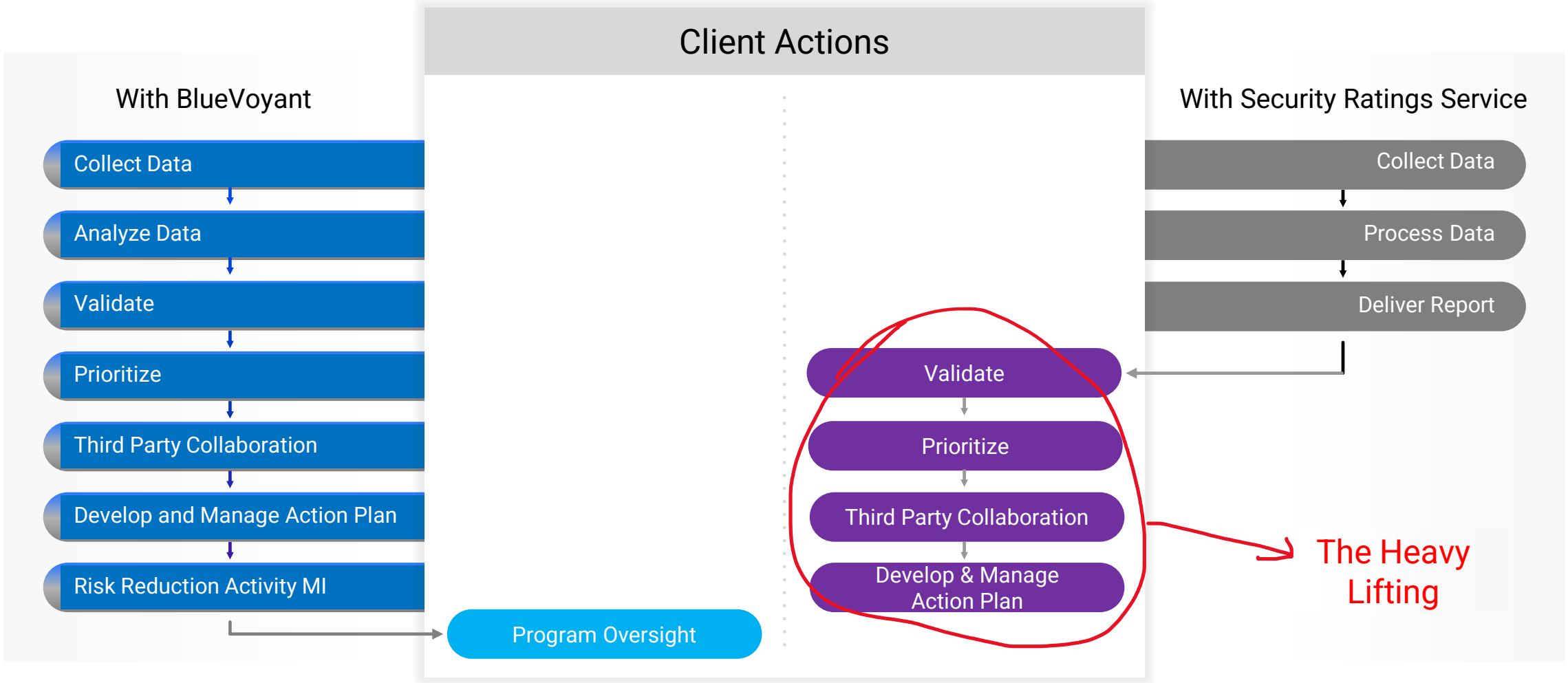
- Prioritization of Needs
- Remediation Plan for Internal and External
- Direct Engagement with Vendors on Client's Behalf
- Manage to Resolution - Confirmation of Completion

Data ---> Intelligence ---> Remediation (at scale)

Sample from 1 client over 1 quarter



Comparison of Activity to Security Ratings



Private and Confidential © DVV Solutions 2021

Inhibitors

Resource Constraints
Blind Spots Around Emerging Risks
Surfacing Issues with High Risk
Operational Factors
Unprioritized "Action Items"
Dealing with Unresponsive Suppliers
Scalability

Shift in Mindset | Entire Supply Chain Cyber Risk Reduction

SRS v BlueVoyant Managed Service

Security Rating Services – Risk Identification
Deliverable is a report, leaving the client to analyze
The Client must triage, prioritize, develop treatment action plan and collaborate with their vendors
Companies struggle to operationalize due to scale, high data volumes and potential false positives. This requires significant investment in terms of expertise/people.
Time to value – Programs typically take 18-24 months to scale
These operational challenges result in significant and material cyber risk 'blind spots' across the supply chain
Visibility and reporting of performance metrics can be ad hoc and manual activities

BlueVoyant – Risk Reduction

- Deliverables are two-fold – Cyber Risk measurement **PLUS** Cyber Risk reduction
- BV Risk Operations Centre does the triage, prioritization, treatment process and collaborates with the vendors (heavy lifting)
- BV service augments the Client's current TPRM approach and enables them to scale. BV ROC provides unparalleled expertise and tooling
- Time to value – Service can scale immediately (typically 2-3 weeks)
- Approach is consistent and robust across entire ecosystem, removing blind spots
- BV provides near real-time performance metrics on risk posture and remediation activity through the portal to measure/track cyber risk reduction

Fully Managed Service to reduce cyber risk across entire Third-Party supply chain ecosystems.

Delivered by our Risk Operations Centre (ROC), on a continuous daily basis.

DVV solutions

To discuss your third-party risk management challenges and how to generate scale and results in your TPRM program contact us via:

sobrien@dvvs.co.uk

+44 (0)161 476 8701
+44 (0)7973 295 997

dvv-solutions

dvvs.co.uk