Bitsight

Apresentação FCUL

Nuno Almeida

Consulting Engineer
nuno.almeida@bitsight.com

May 26, 2023

BITSIGHT

Agenda

- Sobre a Bitsight
- Security Ratings?
- Casos de Uso
- Riscos e alinhamento a áreas de Programas de Segurança
- Exemplo de Fonte de Dados - Sinkhole

Creating Trust in the Digital Economy

2800+
Customers worldwide

40 million+
Rated organizations

260 billion
Security findings to date

42
Global patents

42000
Active users

250 million
in funding from Moody's Corporation

Bitsight pioneered cybersecurity ratings in 2011

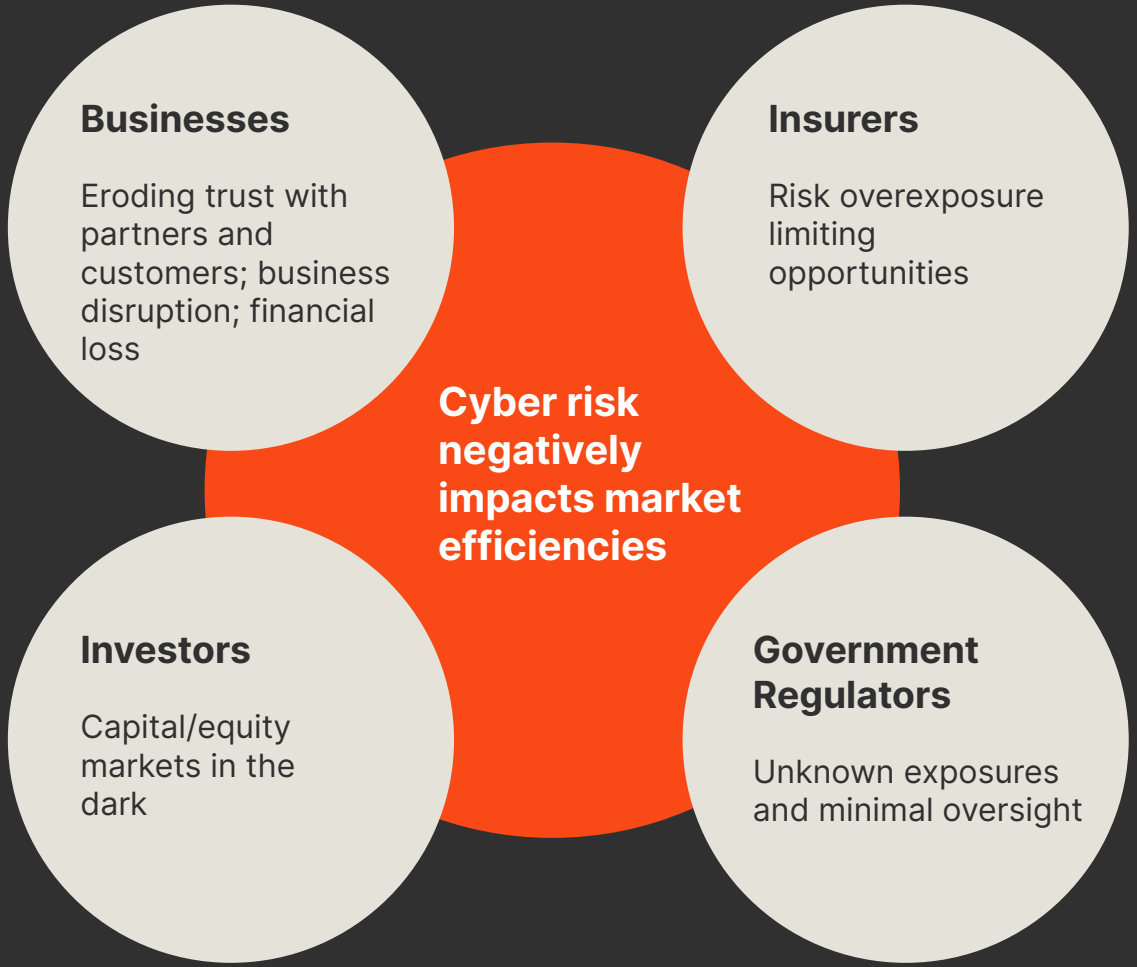
enabling global organizations to measure and manage cyber risk at scale. We have continued to evolve to provide the most accurate, meaningful cybersecurity data and analytics in the marketplace so our customers can engage confidently in the digital economy.

Bitsight is the only security rating in the market proven to correlate with ransomware attack risk and company stock performance.

- Security Performance Management
- Third-Party Risk Management
- Cyber Risk Quantification
- Cyber Insurance

Cyber risk is a global issue

Cyber risk is interconnected and erodes trust across global markets



Growing Cyber Risk Uncertainty

CISOs must answer today's tough cyber risk questions

Where are we most **exposed**?	Can we **quantify** the expected financial and material impact of our exposure?	Are we making the right **priorities** to reduce our cyber risks?	How do we **compare** to our peers?	How **much risk** do we want to take on, and do we **qualify** for cyber insurance?
Blind Spots	**Not Quantifiable**	**Siloed Efforts**	**No Objective Metric**	**Communication Breakdown**
Obscured exposure points, internal and across the digital partner ecosystem	Unable to quantify the potential impact of likely breaches	Disparate initiatives, mix of technologies and disconnected processes	No way to know what "good is" or measure progress or benchmark against others	No source of company truth on risk exposure

Impact of cyber risk uncertainty

Accelerating a step change in the role of the CISO

Protector		Risk leader
Protect everything	→	Fiduciary steward
Incident triage	→	Minimize loss
Business inhibitor	→	Growth enabler

Cyber Risk Management Solution

BITSIGHT

AUDIENCES

Risk Leader | Exec & Board | Insurers | Governments

ONE CENTRAL UNIFIED UX

Third-Party Risk Management

RISK
Vendor Risk Management

PERFORMANCE
Continuous Monitoring

EXPOSURE
Vulnerability Detection & Response, CNI App

Security Performance Management

RISK
Cyber Risk Quantification

PERFORMANCE
Governance and Analytics

EXPOSURE
External Attack Surface Management

Cyber Insurance

PERFORMANCE
Underwriting and Portfolio Management (incl questionnaire workflow)

EXPOSURE
Vulnerability Detection & Response

Data Analysis

RISK
Direct Access Enriched Data Sets for Analysis

PERFORMANCE
Analytical and Reporting Services

EXPOSURE
API for Third Party Developers

Cyber Risk Analytics Engine

Market-leading cyber risk data
Unique mapping and most extensive

Objective universal standard
Broadly adopted, trusted, transparent

Actionable risk insights
Verified correlation portfolio of capabilities

Translate Complex Cybersecurity Issues into Simple Business Context

Bitsight Rating

250 - 900

➔ *Unbiased common* metric to measure cybersecurity performance of organizations worldwide

How Bitsight Security Ratings are Calculated

Collect Data

World's largest sinkhole

400+ Billion events processed daily **(Externally observable)**

QUALIFIED DATA

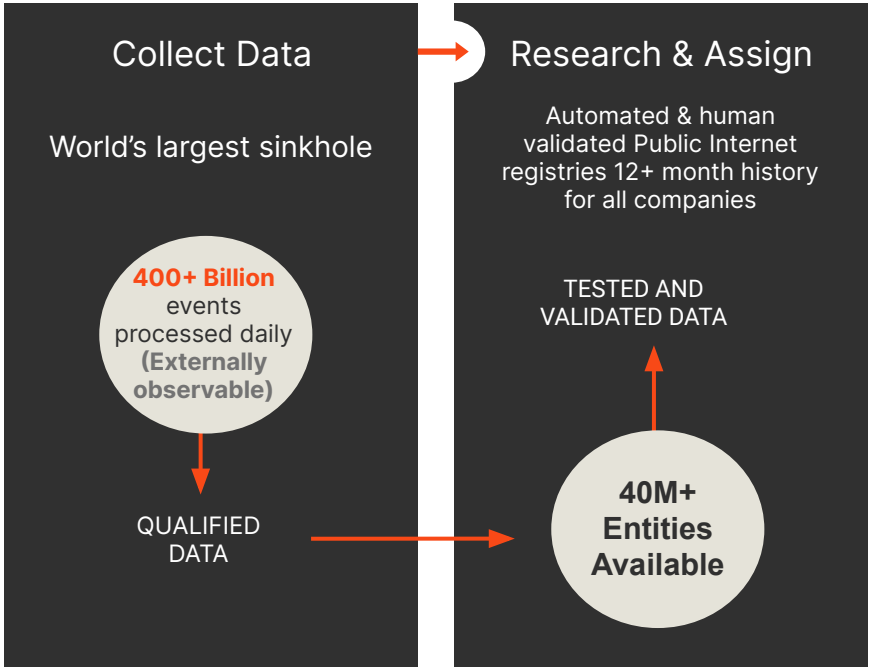
Bitsight Data Collection

The largest amount of proprietary data collection
Bitsight collects 400+ Billion Events on a daily basis across 23 unique risk vectors

Exclusive data partnerships giving unprecedented visibility unavailable elsewhere
Bitsight works with major ad networks, service providers and other unique data partners to provide visibility into organizational security posture unavailable elsewhere on the market.

Broadest Visibility into Emerging Areas of Cyber Risk
Bitsight has visibility into emerging areas of cyber risk including Mobile Applications, Mobile Software, Internet of Things (IoT), File Sharing and more.

How Bitsight Security Ratings are Calculated



Bitsight Digital Footprint Curation

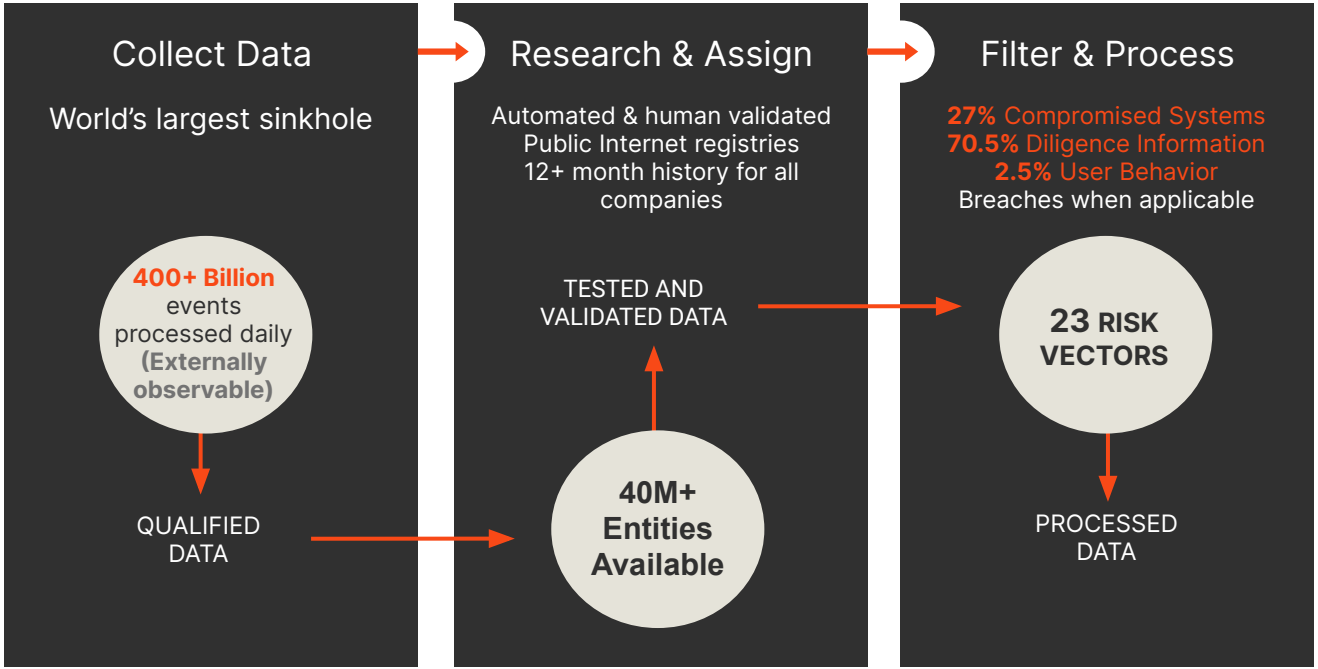
Advanced Automated Mapping
Team of over 60+ technical researchers worldwide curating organizational digital footprints

Broad Array of Sources
Bitsight uses public registries, corporate documents, and technical methods to determine the IP and domain footprint belonging to a company

Parent-Child Relationship Mapping
Bitsight is the only security ratings provider with extensive parent-child relationship mapping to ensure that corporate structure is properly identified

Customizable Mappings of Your Organization
Bitsight enables organizations to self-publish relevant ratings to the Bitsight platform for better risk visibility and communication. Examples include regional breakouts (e.g. "France Operations"), excluding irrelevant infrastructure like Guest Wifi (e.g. "Corporate Rating") and more.

How Bitsight Security Ratings are Calculated



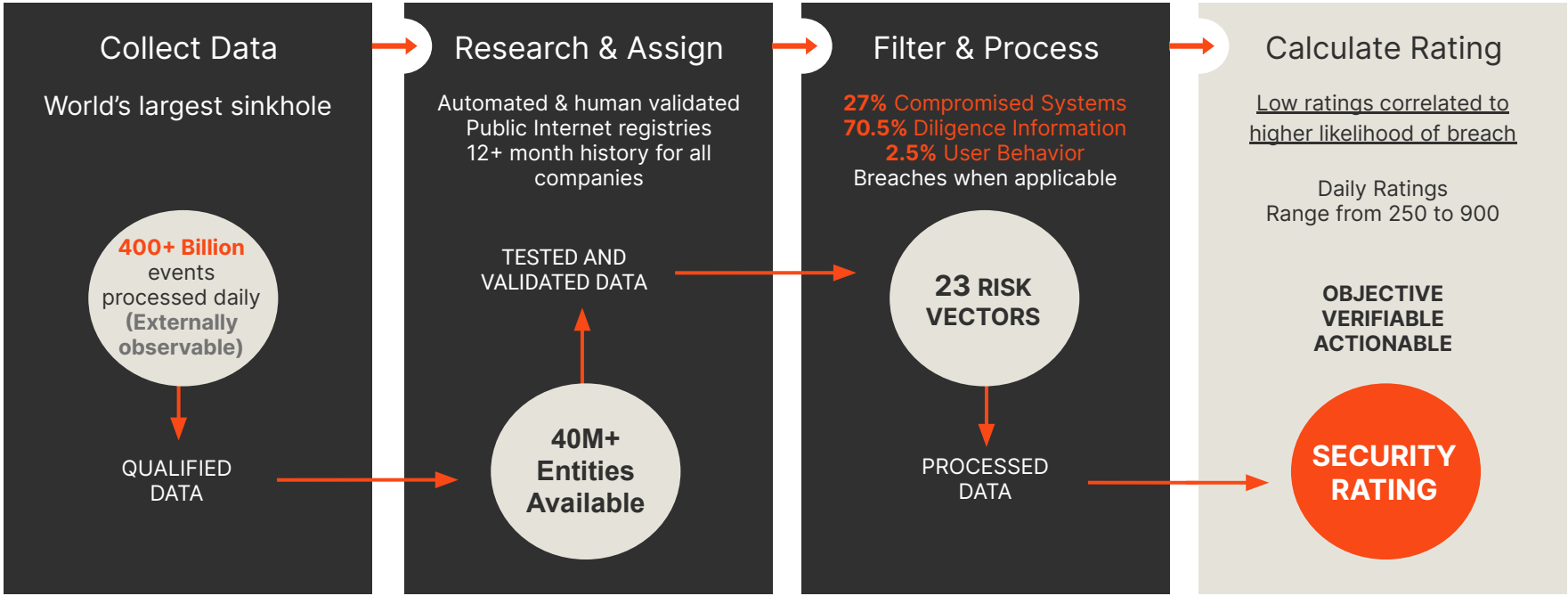
23 Risk Vectors

27% Compromised Systems
Botnet Infections
Spam Propagation
Malware Servers
Unsolicited Comms
Potentially Exploited

70.5% Diligence Information
SPF Domains
DKIM Records
SSL Certs/Config
Open Ports
Web Application Headers
Patching Cadence
Insecure Systems
Server Software
Desktop Software
Mobile Software
DNSSEC
Mobile Application Security
Domain Squatting

2.5% User Behavior
File Sharing
Breaches if Applicable

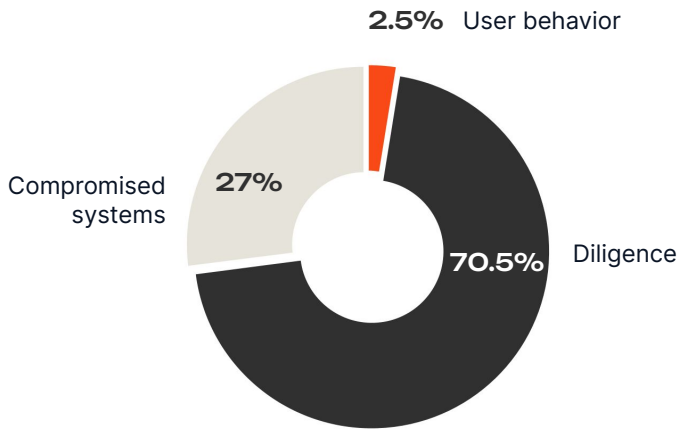
How Bitsight Security Ratings are Calculated



Risk Vector Weightings

Compromised Systems	Botnet Infections	27%	
	Spam Propagation		
	Malware Servers		
	Unsolicited Communications		
	Potentially Exploited		
Diligence	SPF Domains	1%	70.5%
	DKIM Records	1%	
	Mobile Software	1%	
	Server Software	2%	
	Insecure Systems	2.5%	
	Desktop Software	3%	
	Web Application Headers	5%	
	Open Ports	10%	
	TLS/SSL Certificates	10%	
	TLS/SSL Configurations	15%	
	Patching Cadence	20%	
User Behavior	File Sharing	2.5%	

What makes a Security Rating?



Breaches have a negative impact on Security Ratings only if they occur

Strong Validated Correlation to Data Breach

IHS Markit · AIR · Advisen Transforming • Insurance

Likelihood of Data Breach

5x If the security rating drops below 400 as compared to an organization with a 700 or higher

BITSIGHT

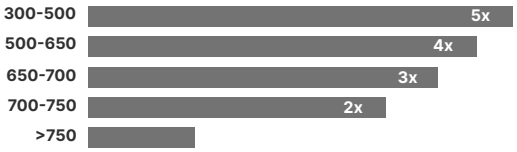
Likelihood of Ransomware

6.4x If the security rating drops below 600 as compared to an organization with a 750 or higher

MarshMcLennan

Likelihood of Security Incident

14 14 risk vectors, including the rating itself, showed “statistically significant” correlations to the likelihood of a cybersecurity incident



2x **Botnet Grade** is B or lower
File Sharing grade is B or lower
Open Ports grade is F

7x Patching Cadence Grade is **C or lower**
4x TLS/SSL Configurations Grade is **C or lower**
3x TLS/SSL Certifications Grade is **C or lower**

1 Patching Cadence
2 Desktop Software
3 Potentially Exploited

Levels of Information - Tailored for stakeholder needs

1. Security Rating - Overall Cyber Risk posture rating

Dashboard, Management reports
'view from the bridge', trending

2. Risk Vectors – Rating for groupings of similar events

Compromised Systems		Diligence	
Botnet Infections	F	SPF Domains	F
Spam Propagation	D	DKIM Records	C
Malware Servers	A	TLS/SSL Certificates	F

Risk hunting, thematic reviews,
Audit selection + scoping
Operational reports

3. Events – specific incidents and risk indicators

Port	Total Hosts	Grade Distribution	Service
21	2		Detected service: FTP with AUTH TLS and 1 other service
22	10		Detected service: SSH and 1 other service
23	3		Detected service: Telnet

Remediation, preparation for on-site audits
Activity reports

Security Performance Management

Strengthening Enterprise Security

Confident Assurance

Customers, boards, investors

Provide objective evidence

Third-Party Risk Management

Strengthening Digital Supply Chain Risk Management

Vendor Risk Management

- Automated assessments
- Growing vendor network
- Evidence to validate

Continuous Monitoring

- Inspect vendor controls at any moment
- In-context vendor collaboration
- Automatic discovery of concentrated fourth-party risk

Powered by Managed Services

- Managed vendor assessments
- Continuous monitoring & risk hunting
- Surfaced insights and reporting

Exposure Management

- Accelerate vulnerability remediation
- Scale and track vendor outreach efforts
- Prioritize mitigation to exposure

Bitsight Third-Party Risk Management

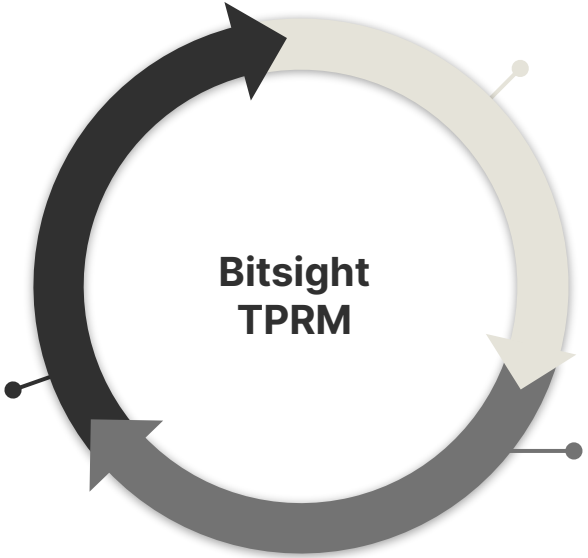
Strengthening Digital Supply Chain Risk Management

Powered by Managed Services

- Managed vendor assessments
- Continuous monitoring & risk hunting
- Surfaced insights and reporting

Exposure Management

- Accelerate vulnerability remediation
- Scale and track vendor outreach efforts
- Prioritize mitigation to exposure



Vendor Risk Management

- Automated assessments
- Growing vendor network
- Evidence to validate

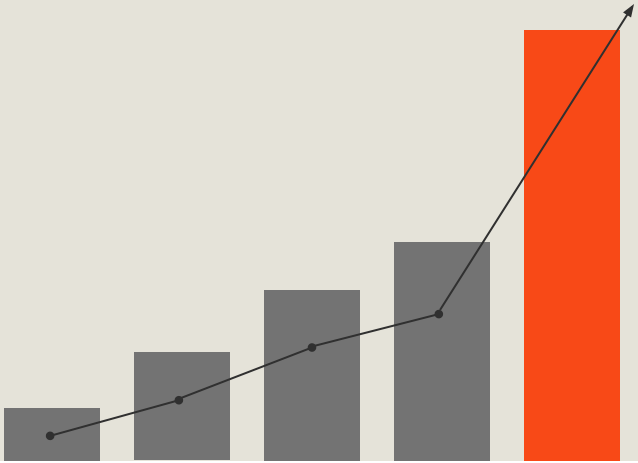
Continuous Monitoring

- Inspect vendor controls at any moment
- In-context vendor collaboration
- Automatic discovery of concentrated 4th-Party risk

Example of Impactful Results from Vendor Collaboration

Onboarded **496** suppliers and engaged with Bitsight Security Ratings as part of this process

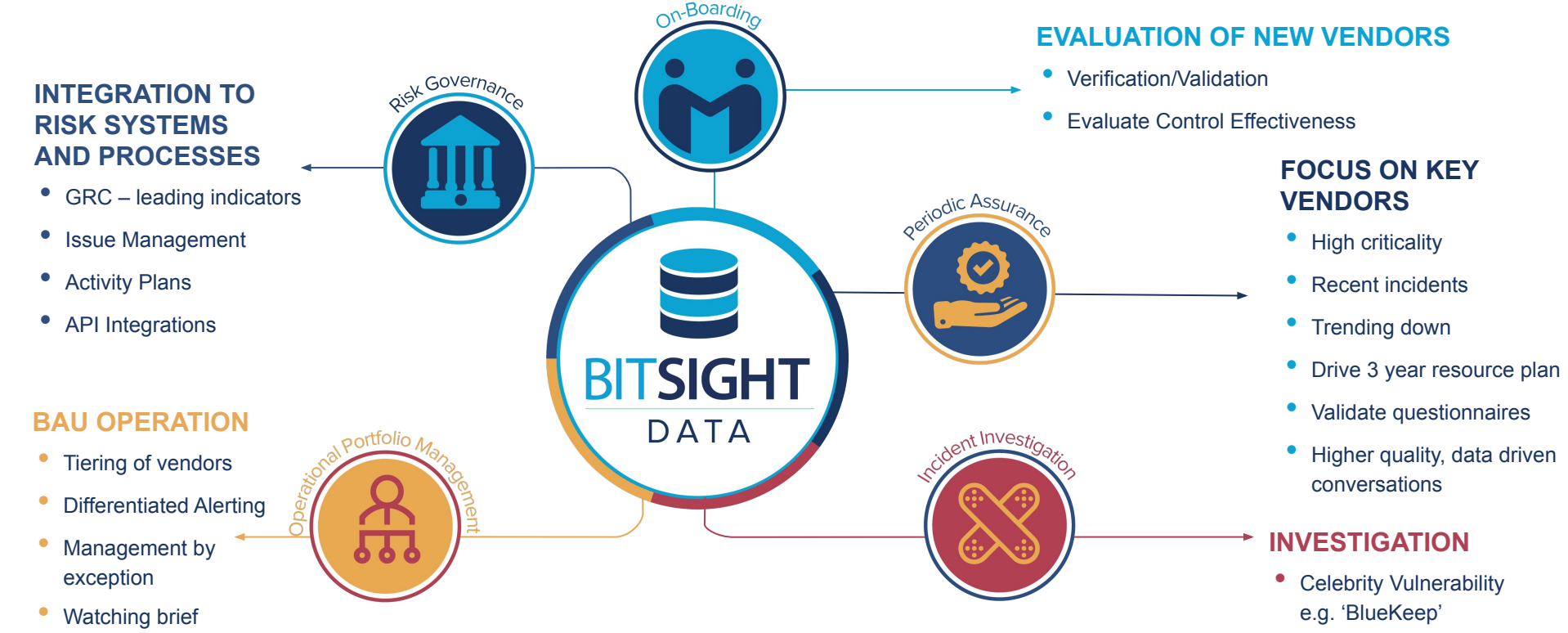
56%
Saw a Rating Increase
276



50
Average points increased across this group

*Suppliers on-boarded between May 1st and October 31.
Ratings compared between May 1st and Dec 4th

TPRM – High level Use Case Components



INTEGRATION TO RISK SYSTEMS AND PROCESSES

- GRC – leading indicators
- Issue Management
- Activity Plans
- API Integrations

EVALUATION OF NEW VENDORS

- Verification/Validation
- Evaluate Control Effectiveness

FOCUS ON KEY VENDORS

- High criticality
- Recent incidents
- Trending down
- Drive 3 year resource plan
- Validate questionnaires
- Higher quality, data driven conversations

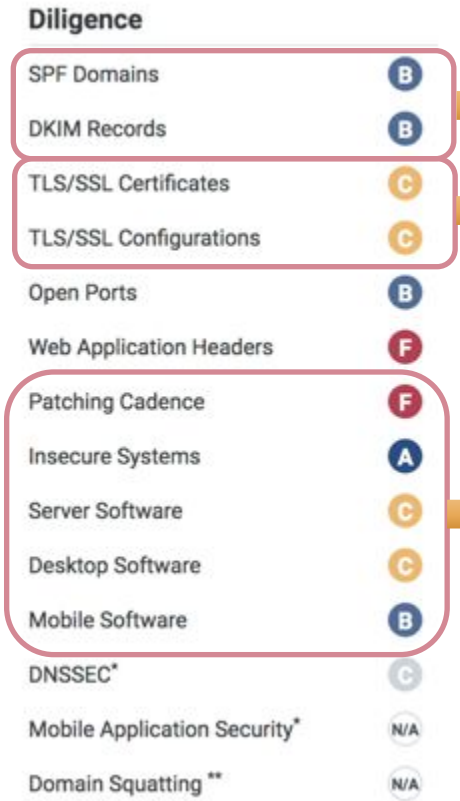
BAU OPERATION

- Tiering of vendors
- Differentiated Alerting
- Management by exception
- Watching brief

INVESTIGATION

- Celebrity Vulnerability e.g. 'BlueKeep'
- 3rd and 4th party investigations

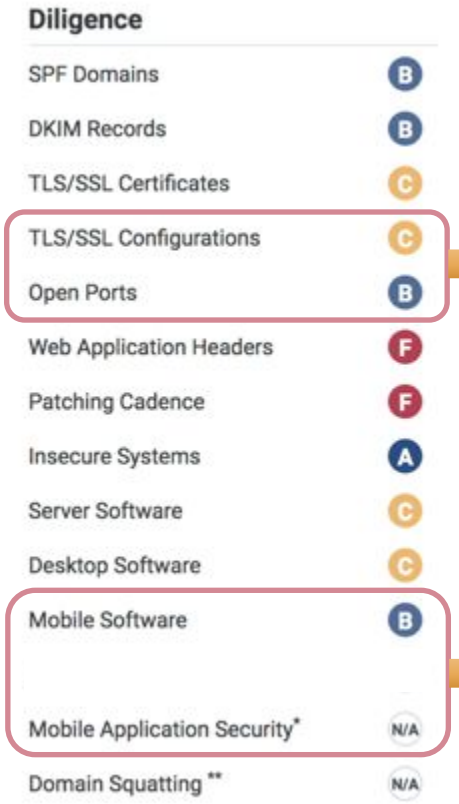
Evidence: Diligence (1 of 3)



- Email security
- Encryption
- Vulnerability management
- Patch management
- Asset inventory
- Hardening standards

- Who's responsible?
  Which teams do these areas map to in your organization?
- What is the root cause?
  Apply Toyota's "5 Whys" to avoid playing whack-a-mole
- Where is the problem?
  Is it an independent BU, still autonomous acquisition, or external partner?

Evidence: Diligence (2 of 3)

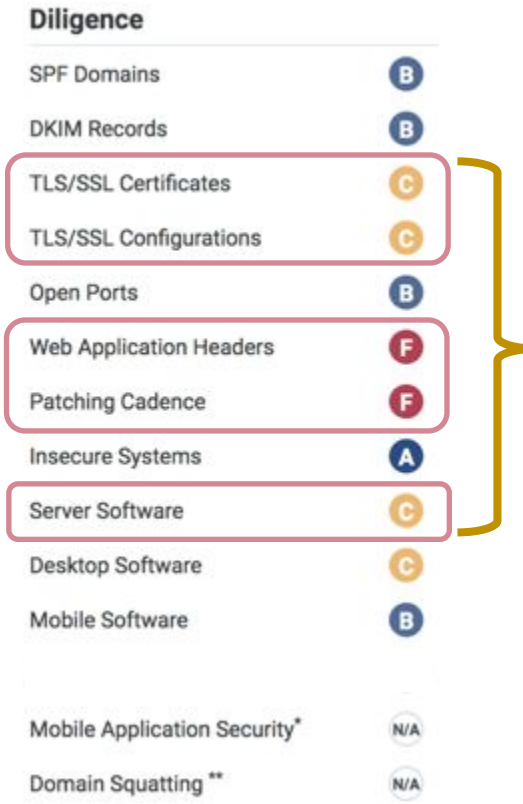


- Perimeter security
- Hardening standards
- Encryption
- Change management

- Mobile security
- Secure development

- Who's responsible?
  Which teams do these areas map to in your organization?
- What is the root cause?
  Apply Toyota's "5 Whys" to avoid playing whack-a-mole
- Where is the problem?
  Is it an independent BU, still autonomous acquisition, or external partner?

Evidence: Diligence (3 of 3)



- Secure development (SDLC)
- Web application security
- [Sec]DevOps

- Who's responsible?
  Which teams do these areas map to in your organization?
- What is the root cause?
  Apply Toyota's "5 Whys" to avoid playing whack-a-mole
- Where is the problem?
  Is it an independent BU, still autonomous acquisition, or external partner?

Evidence: Compromised Systems

- Endpoint protection
- Incident management / Detection and response
- Security awareness / training

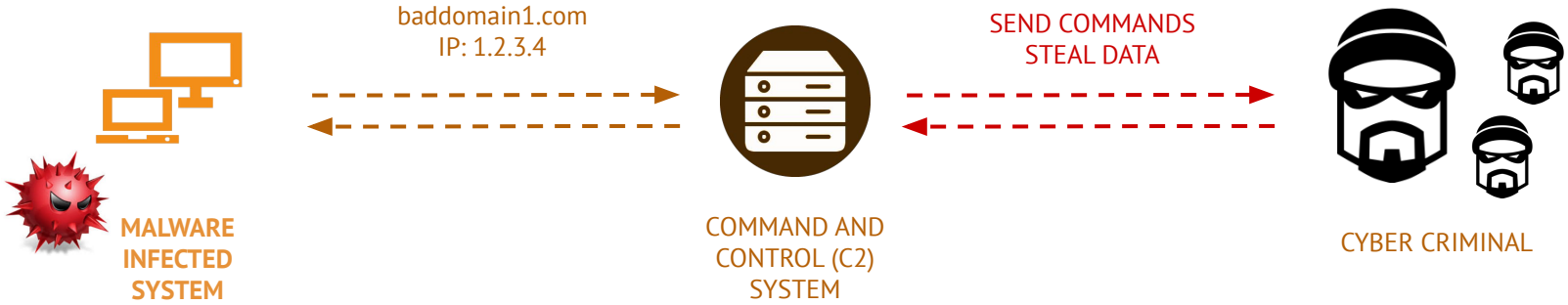
- Who's responsible? Which teams do these areas map to in your organization?
- What is the root cause?
- Where is the problem? Is it an independent BU, still autonomous acquisition, or external partner?

Evidence: Public Disclosures

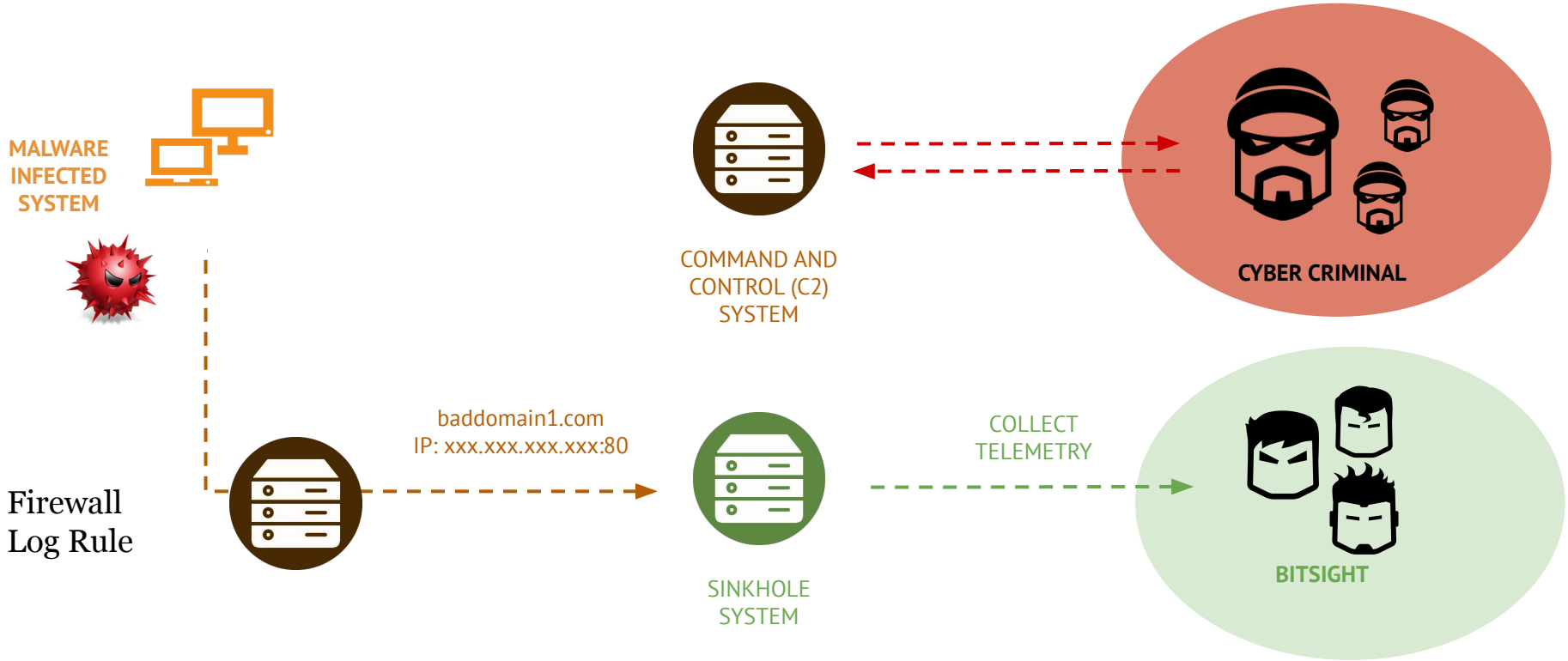
- Incident management
- Data loss prevention
- Secure disposal
- Capacity management / Business continuity

- Who's responsible? Which teams do these areas map to in your organization?
- What is the root cause? Apply Toyota's "5 Whys" to avoid playing whack-a-mole
- Where is the problem? Is it an independent BU, still autonomous acquisition, or external partner?

What is a Sinkhole



What is a Sinkhole



Obrigado!