INFOTEC

Preparing and Executing A Successful IT Risk Management Audit for Insurance Industry

สุวิทย์ ศิรสิทธิวรภัทร
Senior Consultant Manager

บรรณกิจ ศรีสวย
Senior Consultant Manager

23 กันยายน 2564

10:00 - 12:30 น.

WEBINAR

Speakers Panel

- Let’s start

© 2021 ACinfotec. All rights reserved.

คุณสุวิทย์ ศิรสิทธิวรภัทร

Senior Consultant Manager, ACinfotec

Mr. Suwit is a senior consultant manager who provide Framework to Audit Insurance Company for Office of Insurance Commission, as a project manager & consultant who has multi-discipline knowledge ranging and successfully led the implementation of the full information security management system (ISO/IEC 27001), service management system (ISO/IEC 20000), business continuity management based on ISO 22301.

His expertise is to implement the effective process from modernize framework to match with organization business needs and operating environment for real business benefits.

© 2021 ACinfotec. All rights reserved.

คุณบรรณกิจ ศรีสวย

Senior Consultant Manager, ACinfotec

Mr. Bannakit is a senior consultant who has multi-discipline knowledge ranging from security management based on ISO 27001:2005 and ISO 27001:2013 more than 13+ years, service management based on ISO 20000, business continuity management based on ISO 22301 and privacy information management system based on ISO 27701.

With this fact he is a high-profile consultant who can assist client in establishing and sustaining best practice processes base on well-known international standards.

© 2021 ACinfotec. All rights reserved.

Topic

ภาพรวม เหตุผล และความท้าทาย IT Risk Management ของอุตสาหกรรมประกันภัย

สาระสำคัญ กรอบเวลา และวัตถุประสงค์ตามประกาศของ คปภ.

การเตรียมความพร้อมสำหรับ IT Risk Management Audit และการตรวจแบบ Modern Optimized Audit

เคล็ดลับ และแนวทางการดำเนินการตรวจสอบให้มีประสิทธิภาพ

Security Rating by Security Scorecard ช่วยส่งเสริมด้าน IT Risk Management

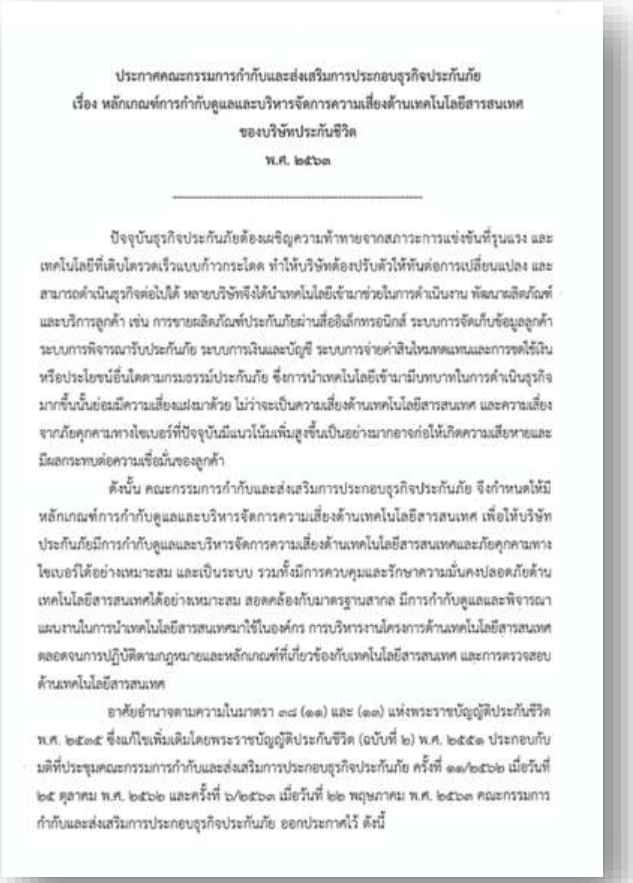
Q & A

© 2021 ACinfotec. All rights reserved.

PRESENTATION OF IT AUDIT FRAMEWORK & IT AUDIT PROGRAM

© 2021 ACinfotec. All rights reserved.

Introducing OIC IT Risk Management and IT Audit Manual

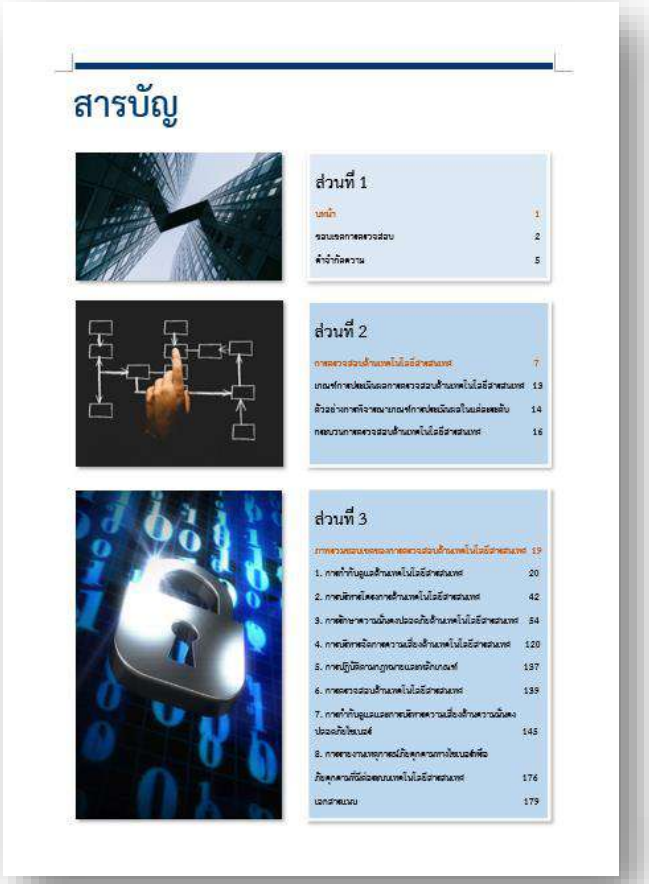


ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ของบริษัทประกันชีวิต
พ.ศ. ๒๕๖๓

ปัจจุบันธุรกิจประกันภัยต้องเผชิญความท้าทายจากสภาวะการแข่งขันที่รุนแรง และเทคโนโลยีที่เติบโตรวดเร็วแบบก้าวกระโดด ทำให้บริษัทต้องปรับตัวให้ทันต่อการเปลี่ยนแปลง และสามารถดำเนินธุรกิจต่อไปได้ หลายบริษัทจึงได้นำเทคโนโลยีเข้ามาช่วยในการดำเนินงาน พัฒนาผลิตภัณฑ์และบริการลูกค้า เช่น การขายผลิตภัณฑ์ประกันภัยผ่านสื่ออิเล็กทรอนิกส์ ระบบการจัดเก็บข้อมูลลูกค้า ระบบการพิจารณารับประกันภัย ระบบการเงินและบัญชี ระบบการจ่ายค่าสินไหมทดแทนและการชดใช้เงินหรือประโยชน์อื่นใดตามกรมธรรม์ประกันภัย ซึ่งการนำเทคโนโลยีเข้ามามีบทบาทในการดำเนินธุรกิจมากขึ้นนั้นย่อมมีความเสี่ยงแฝงมาด้วย ไม่ว่าจะเป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมากอาจก่อให้เกิดความเสียหายและมีผลกระทบต่อความเชื่อมั่นของลูกค้า

ดังนั้น คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย จึงกำหนดให้มีหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้บริษัทประกันภัยมีการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม และเป็นระบบ รวมทั้งมีการควบคุมและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม สอดคล้องกับมาตรฐานสากล มีการกำกับดูแลและพิจารณาแผนงานในการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร การบริหารงานโครงการด้านเทคโนโลยีสารสนเทศ ตลอดจนการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๓๘ (๑๑) และ (๑๓) แห่งพระราชบัญญัติประกันชีวิต พ.ศ. ๒๕๓๕ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติประกันชีวิต (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ ประกอบกับมติที่ประชุมคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ครั้งที่ ๑๑/๒๕๖๒ เมื่อวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๒ และครั้งที่ ๖/๒๕๖๓ เมื่อวันที่ ๒๒ พฤษภาคม พ.ศ. ๒๕๖๓ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ออกประกาศไว้ ดังนี้



© 2021 ACinfotec. All rights reserved.

ภาพรวมขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศ

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ

การบริหารโครงการด้านเทคโนโลยีสารสนเทศ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

© 2021 ACinfotec. All rights reserved.

IT Audit Framework

© 2021 ACinfotec. All rights reserved.

OIC's IT Audit Framework

1. IR

- Inherent risk ความเสี่ยงที่มีอยู่

2. QRM

- Quality of risk management คุณภาพการบริหารความเสี่ยง

NR

- Net Risk ความเสี่ยงสุทธิ

QRM \ IR	ต่ำ (1)	ค่อนข้างต่ำ (2)	ปานกลาง (3)
ค่อนข้างต่ำ (2)	ค่อนข้างต่ำ (2)	ปานกลาง (3)	ค่อนข้างสูง (4)
ปานกลาง (3)	ปานกลาง (3)	ค่อนข้างสูง (4)	สูง (5)

NetRisk

- Information Systems Audit and Control Association (ISACA): IT Audit Framework (ITAFTM): A Professional Practices Framework for IT Audit, 4th Edition
- The Institute of Internal Auditors of Thailand
- ISACA: COBIT 5 for Assurance

© 2021 ACinfotec. All rights reserved.

IT Risk Profile from Aggregated Net Risk (ANR)

แบบสำรวจฯ part 1 & part 2

IR

QRM

Onsite audit

QRM

IT Risk Profile

OIC's regulation domains	IR	QRM	NR
1. การกำกับดูแลด้านเทคโนโลยีสารสนเทศ	ปานกลาง	ดี	ค่อนข้างต่ำ (4)
2. การบริหารโครงการด้านเทคโนโลยีสารสนเทศ	ปานกลาง	พอใช้	ปานกลาง (3)
3. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	ปานกลาง	พอใช้	ปานกลาง (3)
4. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ปานกลาง	ดี	ค่อนข้างต่ำ (4)
5. การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	สูง	พอใช้	ค่อนข้างสูง (2)
6. การตรวจสอบด้านเทคโนโลยีสารสนเทศ	ต่ำ	ดี	ต่ำ (5)
7. การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	ปานกลาง	พอใช้	ปานกลาง (3)
8. การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ	สูง	พอใช้	สูง (1)
Aggregated Net Risk (ANR)			ปานกลาง

ANR

© 2021 ACinfotec. All rights reserved.

Quality of Risk Management (QRM) by On-site audit : result

การสรุปผลจากการตรวจ On-site จะสรุปออกมาเป็น 2 ส่วน คือ

1. ผ่านประกาศหรือไม่
2. ระดับคุณภาพของการดำเนินการใน Domain นั้น และระดับคุณภาพของการดำเนินการเรื่อง IT Governance & Risk ภาพรวมองค์กร

1. สรุปการผ่านประกาศ

การสรุปผลการตรวจราย Domain
ผ่านประกาศ : คะแนนรวมได้ 2.00 - 3 และทุกข้อต้องได้คะแนน 2 ขึ้นไป
ผ่านบางส่วน : เมื่อได้คะแนน 0 หรือ 1 ในบางข้อย่อย (Controls)
ไม่ผ่านประกาศ : ได้คะแนน 0 ทุกข้อย่อย (Controls)

การสรุปผลการตรวจภาพรวมทั้ง 8 Domains
ผ่านประกาศ : คะแนนทุก Domain ต้องได้ 2.00 - 3 และทุกข้อต้องได้คะแนน 2 ขึ้นไป
ผ่านบางส่วน : เมื่อได้คะแนน 0 หรือ 1 ในบางข้อย่อย (Controls)
ไม่ผ่านประกาศ : ได้คะแนน 0 ทุกข้อย่อย (Controls)

2. สรุประดับคุณภาพ

** OIC คาดหวังให้บริษัทประกันอยู่ในระดับ bronze ภายใน 3 ปี

OIC's audit timeline

T1-SAQ release

Release SAQ to
Insurance company
to update IR

Feb

T2-Update IR

Update IR by SAQ
information

T4-Submit QRM report

Insurance company submit
The audit report to OIC

Dec

Mar-Apr

T3-QRM audit

Perform Audit
by Qualified auditor

T3-QRM audit

Perform Audit
by Qualified auditor

Jan

Next round

** กำหนดให้บริษัทประกันนำส่งเอกสารผลการตรวจสอบ Audit report (QRM)
ภายใน 1 เดือนหลังจากตรวจแล้วเสร็จหรือภายในวันที่ 31 มกราคม ของปีถัดไป

© 2021 ACinfotec. All rights reserved.

IT Audit Program

ภาพรวมขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศ

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ

การบริหารโครงการด้านเทคโนโลยีสารสนเทศ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

© 2021 ACinfotec. All rights reserved.

หัวข้อการตรวจสอบใน IT Audit Program ทั้ง 8

1. การกำกับดูแลด้านเทคโนโลยีสารสนเทศ

- การกำกับดูแลด้านเทคโนโลยีสารสนเทศ
- องค์ประกอบของคณะกรรมการบริษัท
- หน้าที่ความรับผิดชอบของคณะกรรมการบริษัท
- นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. การบริหารโครงการด้านเทคโนโลยีสารสนเทศ

- การบริหารโครงการด้านเทคโนโลยีสารสนเทศ
- การประเมินความเสี่ยงและการจัดลำดับความสำคัญของโครงการ
- กรอบการบริหารจัดการโครงการด้าน IT
- การกำกับดูแลโครงการด้าน IT

4. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

- การระบุบริบท ขอบเขต และเกณฑ์ความเสี่ยง
- การประเมินความเสี่ยง
- การจัดการความเสี่ยง
- การติดตามและทบทวนความเสี่ยง
- การรายงานความเสี่ยง

3. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- มีการบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล และทรัพย์สินสารสนเทศ
- มีการควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ
- มีแนวปฏิบัติด้านการเข้ารหัสข้อมูล
- มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
- มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท
- มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
- มีหลักเกณฑ์และกระบวนการในการจัดหาและการพัฒนาระบบ
- มีการบริหารจัดการผู้ให้บริการภายนอก
- มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา

5. การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

- การปฏิบัติตามกฎหมายและหลักเกณฑ์

6. การตรวจสอบด้านเทคโนโลยีสารสนเทศ

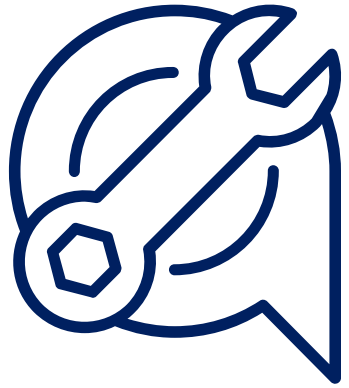
- บทบาทหน้าที่และแผนงานในการตรวจสอบ
- การปฏิบัติงานตรวจสอบ
- การรายงานผลและติดตามผลการตรวจสอบ

7. การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

- มีแนวทางการกำกับดูแลการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์
- การประเมินระดับความเสี่ยงตั้งต้น
- การกำกับดูแลการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์

8. การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

- การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ



Preparation and Optimization for IT Audit

Preparation and Optimization for IT Audit

Preparing

- จัดเตรียมทีมงานตรวจสอบด้านเทคโนโลยีสารสนเทศ
- กำหนดผู้รับตรวจที่เกี่ยวข้องทั้ง 8 หมวด

Document Assessment

- ร้องขอเอกสารที่มีอยู่ ณ ปัจจุบัน
- ตรวจสอบความสอดคล้องในระดับเอกสารที่ได้ร้องขอมา เพื่อสรุปประเด็นในเบื้องต้น

Finalize

- จัดทำร่างผลการตรวจสอบและแนวทางการแก้ไขจากผู้รับตรวจ
- จัดทำรายงานผลการตรวจสอบ และนำเสนอให้ผู้บริหารระดับสูง และคณะกรรมการตรวจสอบพิจารณา

Planning

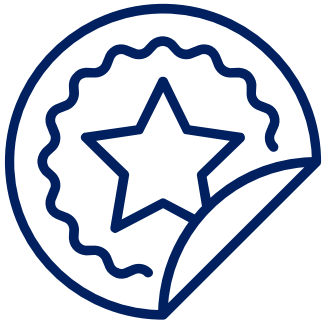
- วางแผนการตรวจสอบโดยแบ่งผู้รับตรวจตาม 8 เรื่องตามประกาศฯ ของสำนักงาน คปภ.

Interview

- นัดหมายและสัมภาษณ์ผู้ที่เกี่ยวข้องทั้ง 8 เรื่องตามประกาศฯ ของสำนักงาน คปภ.
- สรุปประเด็นจากการตรวจสอบเอกสารและสัมภาษณ์ลงใน IT audit program

บริษัทนำเสนอผลการตรวจสอบพร้อมเล่มรายงานผลการตรวจสอบแก่นำส่งรายงานผลการตรวจสอบให้กับสำนักงาน คปภ. ภายในวันที่ 31 มกราคม 2565

© 2021 ACinfotec. All rights reserved.

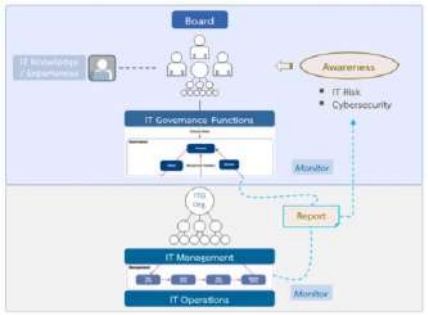


Tips for conducting effective IT Audit

© 2021 ACinfotec. All rights reserved.

Tips for conducting effective IT Audit

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ



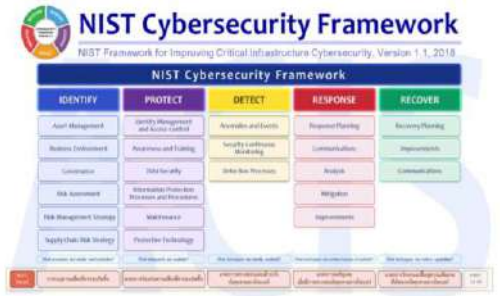
การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

การบริหารโครงการด้านเทคโนโลยีสารสนเทศ

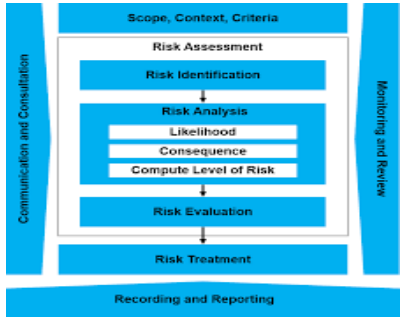
การตรวจสอบด้านเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี

การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์



การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ



การรายงานเหตุการณ์การโจมตีหรือภัยคุกคามทางไซเบอร์

Cybersecurity & Beyond in Insurance Industry

© 2021 ACinfotec. All rights reserved.

Preparing and Executing A Successful IT Risk Management Audit for Insurance Industry

SecurityScorecard

INFOTEC

Adam Denyer-Hampton

Adam Denyer-Hampton is the International Lead for the Pre-Sales Engineering team, heading up the development and expansion of Security Ratings, with a focus on Ratings within Insurance. Adam has 15 years of experience in successfully delivering large and complex IT security solutions for major global companies, across Europe and APAC, including the defense and government agencies. Prior to joining SecurityScorecard, Adam held key technical roles at companies such as SafeNet, SourceFire (part of Cisco Systems) and IT Security Experts, where he managed solution deployments and technical consultations/trainings to meet customer requirements and successfully onboard them to new solutions.

SecurityScorecard

Cybersecurity & Beyond in Insurance Industry

Adam Denyer-Hampton - International Pre-Sales Lead

23/09/2021

© 2021 ACinfotec. All rights reserved.

Our Journey

2013

SEED

bōldstart ventures · evo/ution EQUITY PARTNERS

Founded by Dr. Aleksandr Yampolskiy and Sam Kassoumeh; both are cybersecurity practitioners and leaders

2015

SERIES A

SEQUOIA

Collaboration Tools Launch

2016

SERIES B

G/

Instant SecurityScorecard, Automatic Vendor Detection, and ThreatMarket Launch

100K Companies Continuously Monitored

2017

SERIES C

NGP · Nokia Growth Partners · intel Capital · AXA Strategic Ventures · Moody's

Malware Grader Launches

Partnership with the London Digital Security Centre

200K Companies Continuously Monitored

2018

MILESTONE

1,000,000 SCORED

Milestone achievement provides unmatched amount of historical data to contextualize cybersecurity risk

Atlas Launches

2019

SERIES D

RIVERWOOD CAPITAL

SecurityScorecard closes **$50 million Series D** financing round led by Riverwood Capital, bringing the company's total funding to $110 million, to continue expanding its platform

2021

SERIES E

SILVERLAKE WATERMAN

$180 million Series E financing round led by Silver Lake Waterman bringing total investment to $300 million to expand globally and enhance solutions

MILESTONE

10,000,000 SCORED

Raising the bar for unmatched historical data to contextualize risk with 10 Million companies scored

Marketplace launched with 40 technology and alliance partners

© 2021 ACinfotec. All rights reserved.

Challenges of *Cyber Insurance*

Measuring and modeling security risk for cyber insurance underwriting

Underwriting cyber policies is time consuming

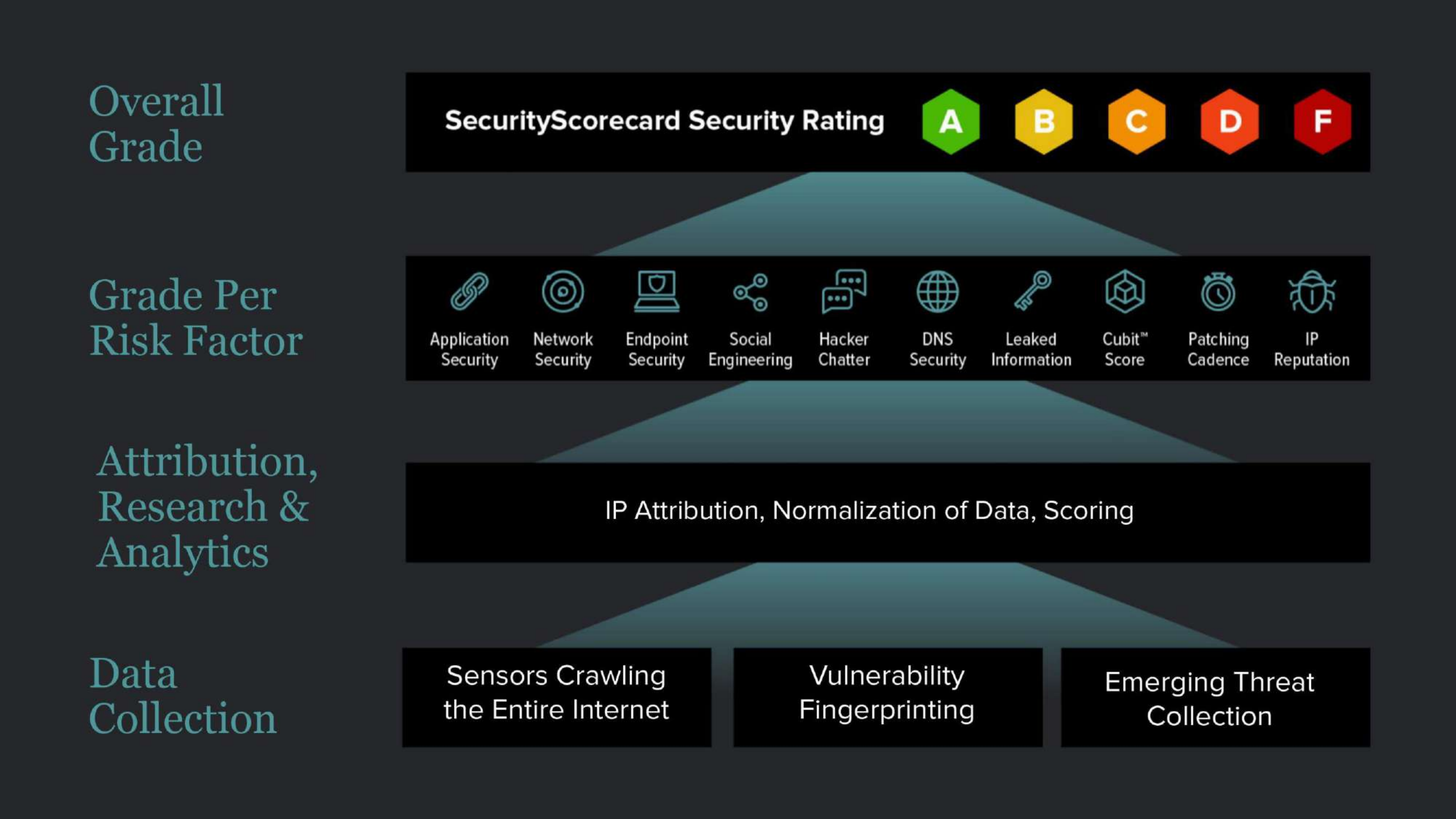
Due to lack of comprehensive historical loss data and no comprehensive centralized source of data

Identifying risk-aggregation across portfolios is difficult

Due to limited visibility and dynamic nature of cyber risk

We **instantly** and **non-intrusively** measure security of **any company in the world**, and help them **become more resilient?**

© 2021 ACinfotec. All rights reserved.


Overall Grade
SecurityScorecard Security Rating
A
B
C
D
F
Grade Per Risk Factor
Application Security
Network Security
Endpoint Security
Social Engineering
Hacker Chatter
DNS Security
Leaked Information
Cubit™ Score
Patching Cadence
IP Reputation
Attribution, Research & Analytics
IP Attribution, Normalization of Data, Scoring
Data Collection
Sensors Crawling the Entire Internet
Vulnerability Fingerprinting
Emerging Threat Collection

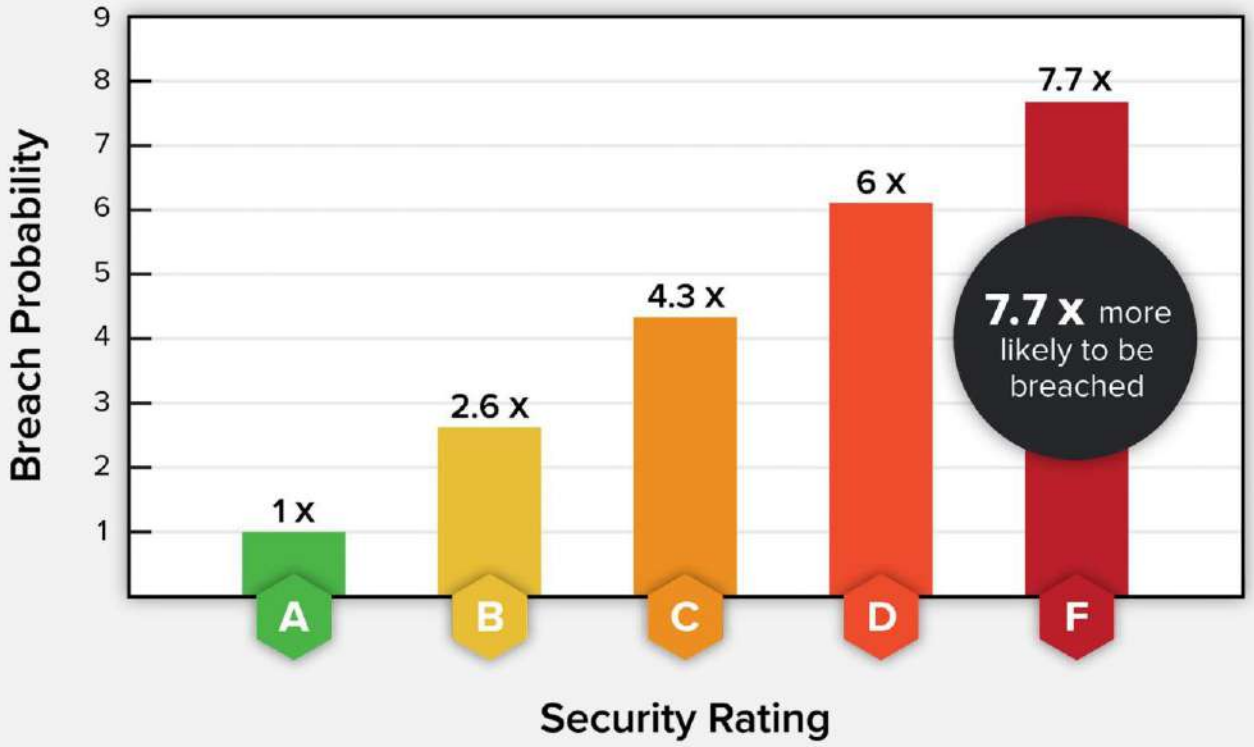
Companies With A Better SecurityScorecard Rating Are More Resilient

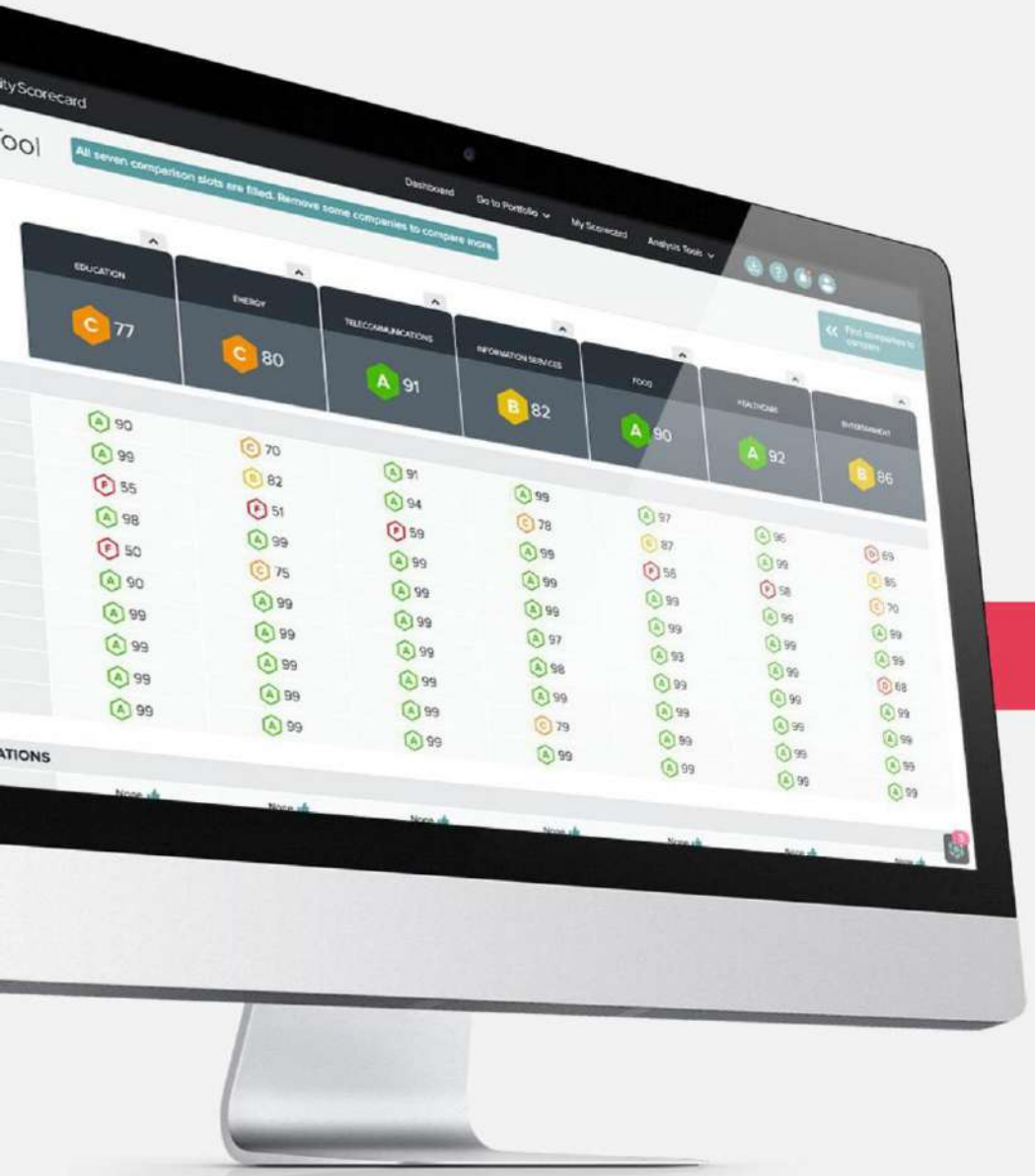
Study Parameters

Evaluation Period	3 Years
No. Data Breaches	2,228
No. Organizations	99,076

Organizations with an F have **7.7x higher likelihood** of breach compared to organizations with a grade of A.

Companies with a better SecurityScorecard rating are more resilient

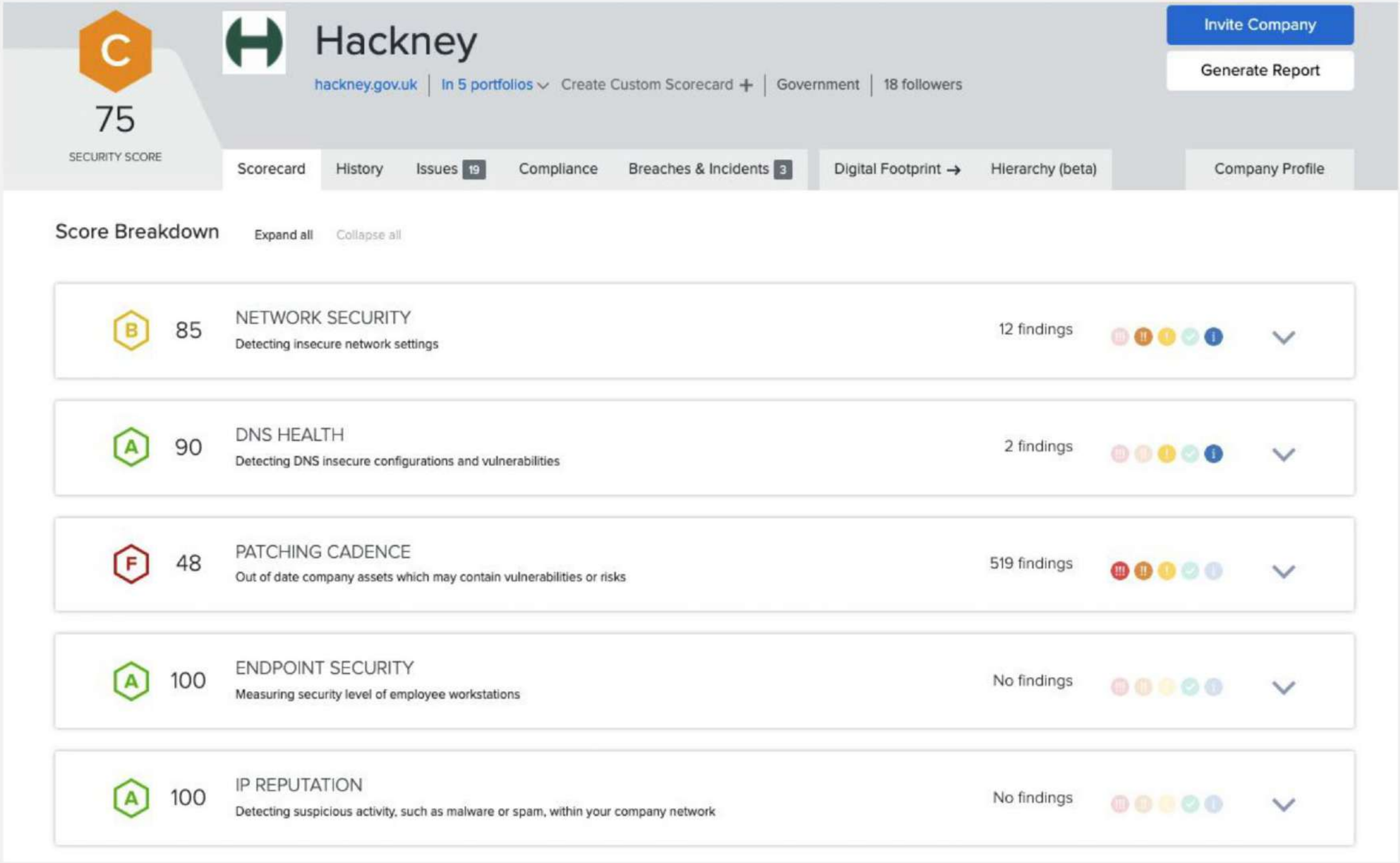




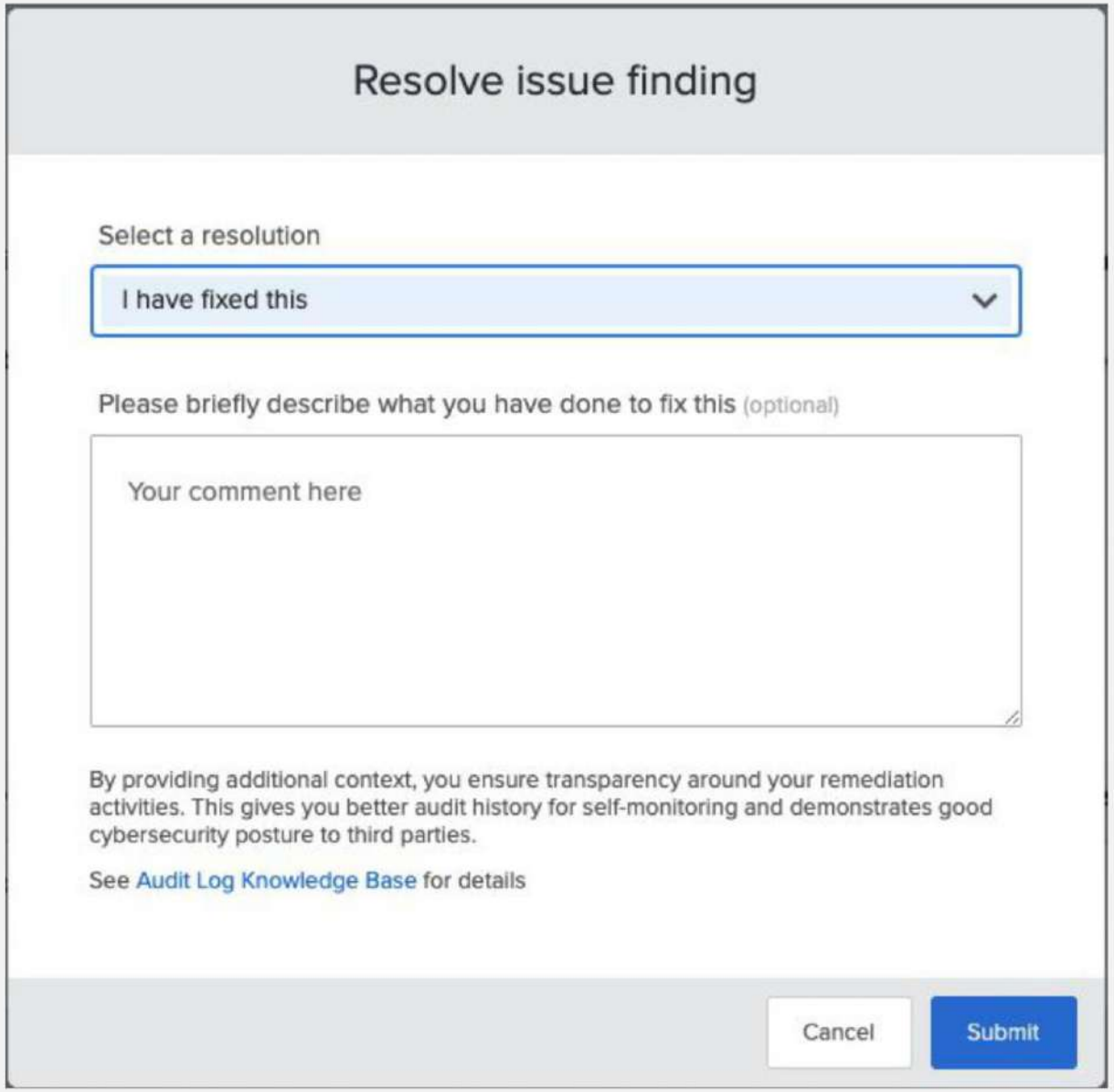
Demo

With New Capabilities

Self Monitoring


C
75
SECURITY SCORE
Hackney
hackney.gov.uk | In 5 portfolios | Create Custom Scorecard + | Government | 18 followers
Invite Company
Generate Report
Scorecard
History
Issues 19
Compliance
Breaches & Incidents 3
Digital Footprint →
Hierarchy (beta)
Company Profile
Score Breakdown
Expand all
Collapse all
B 85 NETWORK SECURITY
Detecting insecure network settings
12 findings
A 90 DNS HEALTH
Detecting DNS insecure configurations and vulnerabilities
2 findings
F 48 PATCHING CADENCE
Out of date company assets which may contain vulnerabilities or risks
519 findings
A 100 ENDPOINT SECURITY
Measuring security level of employee workstations
No findings
A 100 IP REPUTATION
Detecting suspicious activity, such as malware or spam, within your company network
No findings


C
75
SECURITY SCORE
Hackney
hackney.gov.uk | In 5 portfolios | Create Custom Scorecard + | Government | 18 followers
Invite Company
Generate Report
Scorecard
History
Issues 19
Compliance
Breaches & Incidents 3
Digital Footprint →
Hierarchy (beta)
Company Profile
VIEW LAST
7 days
30 days
6 months
12 months
YTD
Δ
+13 pts
Export CSV
LEGEND
Overall Grade
Industry Average
Industry Min/Max
All Factors
Select all
Network Sec.
DNS Health
Patching Cadence
Endpoint Sec.
IP Reputation
Application Sec.
Cubit Score
Hacker Chatter
Information Leak
Social Engineering
100
A
90
B
80
C
70
D
60
F
0
Oct 1
Nov 1
Dec 1
Jan 1
Feb 1
Mar 1
Apr 1
May 1
Jun 1
Jul 1
Aug 1
Sep 1

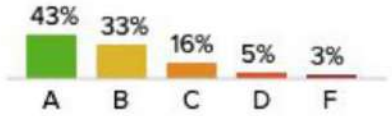

Resolve issue finding
Select a resolution
I have fixed this
Please briefly describe what you have done to fix this (optional)
Your comment here
By providing additional context, you ensure transparency around your remediation activities. This gives you better audit history for self-monitoring and demonstrates good cybersecurity posture to third parties.
See Audit Log Knowledge Base for details
Cancel
Submit

Insurance Model

Companies | Overview

Portfolio Average Rating B 85

Portfolio Rating Distribution



1255 companies
View list

276 active (22%)
979 inactive (78%)

Worst Performing Companies

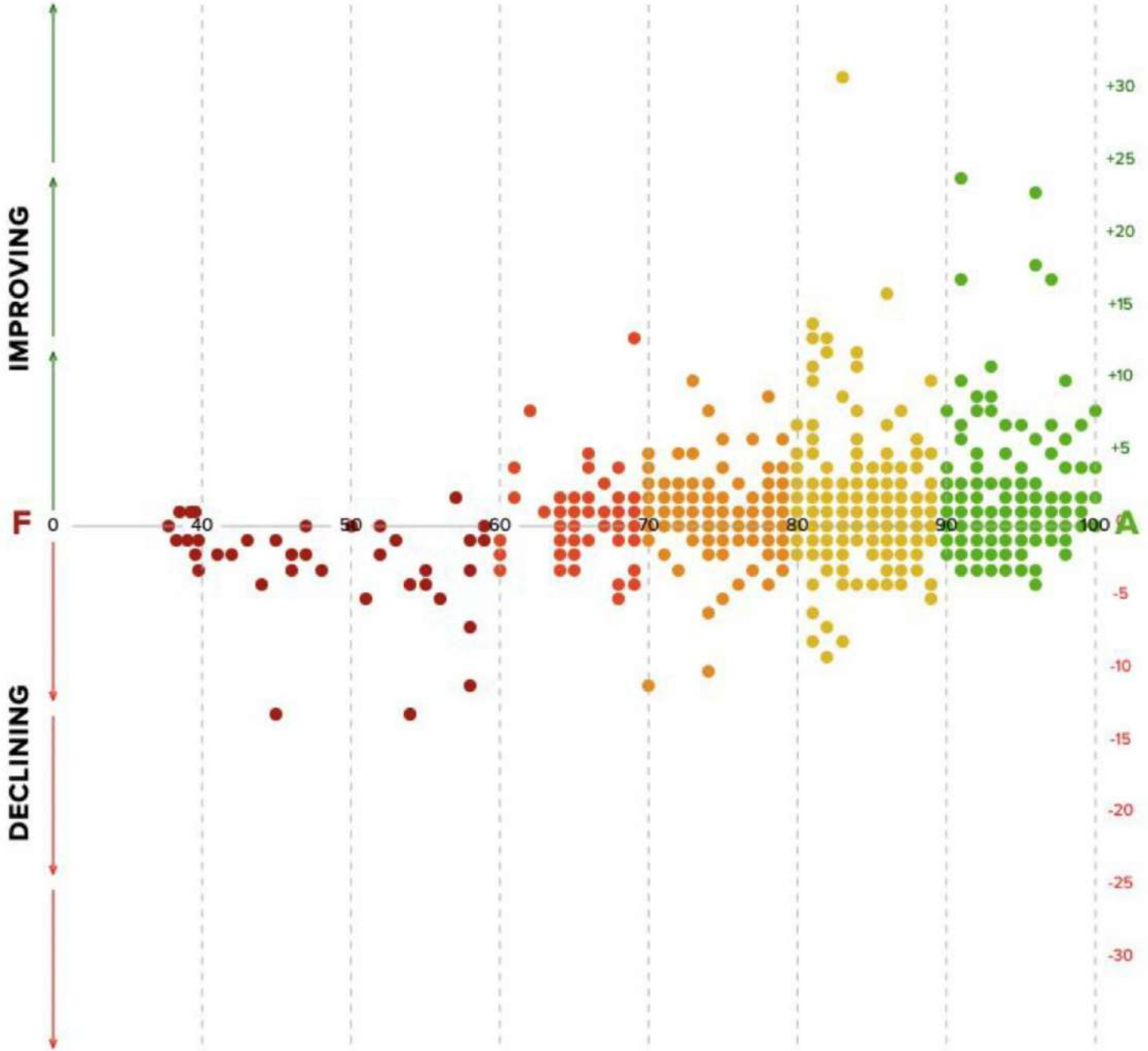
COMPANY	SCORE
Microsoft Corporation	31
Claro Brasil	33
Applied Concepts & Technologies Corp.	34
Telefonica Group	36
Excellbroadband	37

Most Critical Issues

ISSUES	COMPANY COUNT
Site does not enforce HTTPS	619
High Severity CVEs Patching Cadence	506
High-Severity Vulnerability in Last Observation	484
SSL/TLS Service Supports Weak Protocol	435
Certificate Is Revoked	125

Most Common Issues

% OF PORTFOLIO AFFECTED	ISSUE
84%	Website Does Not Implement HSTS Best Pr...
80%	Content Security Policy (CSP) Missing
78%	Website does not implement X-XSS-Protecti...
77%	Exposed Personal Information (Historical)
76%	Unsafe Implementation Of Subresource Inte...



TOP MOVERS	NEW RATING	CHANGE
Akamai Technologies	B 83	+31
Viswaroopa	A 91	+24
Chaucerplc	A 96	+23
Secure Trust Bank plc	A 96	+18
Ovofinance	A 97	+17
Harpenden Building Society	A 91	+17
Geomarkresearch	B 86	+16

BOTTOM MOVERS	NEW RATING	CHANGE
Amazon AWS	F 45	-13
Agiba	F 54	-13
Gladstonessolicitors	C 70	-11
Orange Business Services	F 58	-11
Lincare	C 74	-10
First Abu Dhabi Bank	B 82	-9
Cuddle	B 82	-9

Companies | Overview

38 companies | Compare | Copy To | Remove | Download list

	30-DAY	SECURITY SCORE	COMPANY	INDUSTRY	STATUS	INVITE	VENDOR ECOSYSTEM	ARTIFACTS
☐	-6	C 74	SAP	TECHNOLOGY	Active	✉	View 3rd Parties	
☐	-6	B 81	FireEye, Inc.	TECHNOLOGY	Active	✉	View 3rd Parties	
☐	-3	D 65	City of Brampton	GOVERNMENT	Inactive	✉	View 3rd Parties	
☐	-3	D 60	Apple	TECHNOLOGY	Inactive	✉	View 3rd Parties	
☐	-2	B 82	Direct Energy	ENERGY	Inactive	✉	View 3rd Parties	
☐	-2	B 88	Spotify	TECHNOLOGY	Active	✉	View 3rd Parties	2 artifacts
☐	-2	F 52	Fujitsu	INFORMATION SERVICES	Active	✉	View 3rd Parties	
☐	-1	B 82	Ford Motor Company	MANUFACTURING	Inactive	✉	View 3rd Parties	

COMPANY SEARCH

Search

FILTERS CLEAR ALL

Grade

A B C D F

Industry

Select...

Critical Vulnerabilities Select all

Select...

Issue Types

Select...

Status

Select...

Breaches Clear

Last week Last month **Last year**

Underwrite Policies with Precision and Agility

1. **Reduce time** to quote with instantly-available cyber performance analytics and historical data
2. **Find out the risk** of even the smallest supplier within minutes
3. **Group Based Risk Analytics** with any company anywhere in the world

Thank You

Let's follow us

www.acinfotec.com

ACinfotecthailand

ACinfotec Co., Ltd.

Tel. : +662 670 8980-3 ext. 406

Email : sales@acinfotec.com
training@acinfotec.com