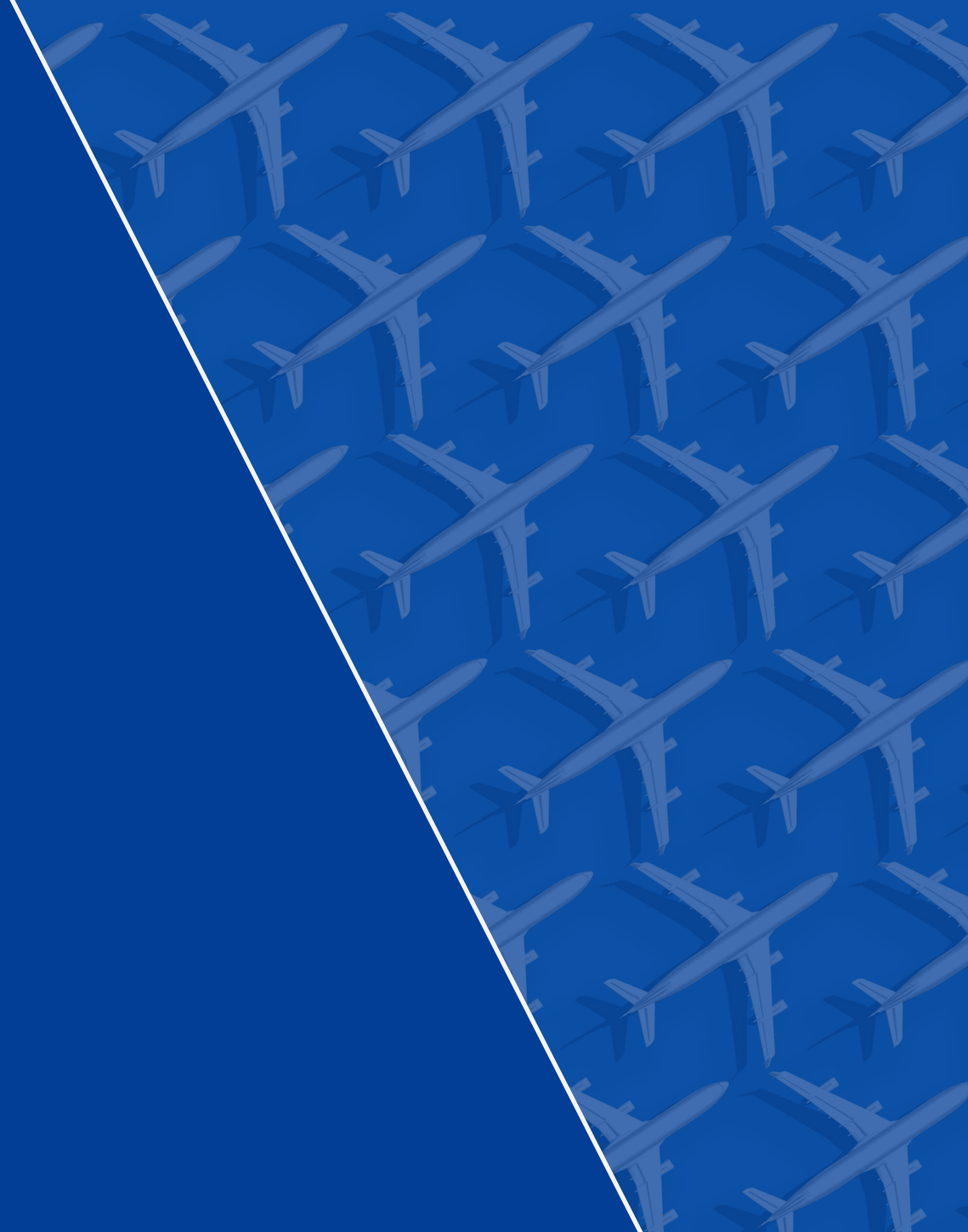
AVIATION **ISAC**

COMMUNITY MEETING

April 16, 2024



AGENDA

WELCOME

AVIATION ISAC UPDATES

THREAT BRIEFING

FEATURED PRESENTATION

- Data-Driven Third Party Risk Management: The Road to AI
  -Matthew Ancelin, Principal Solutions Architect, SecurityScorecard

QUESTIONS

MEETING REMINDERS

- Please remove last year’s community meeting invitation from your calendar
- New Meeting invite for next month’s call will go out at the conclusion of this call
- Meetings are recorded for those unable to attend
- Recordings are added to the website within 24 hours of meeting conclusion
- Link to Recordings: **a-isac.com/community-meetings**
- Access Password: CMeetings2023!!
- Unless otherwise indicated, all information shared in the monthly meetings is considered TLP: GREEN

AVIATION ISAC UPDATES

Summit

- Registration is live!
- September 17-19, 2024
- New Orleans, Louisiana
- Register early and lock in your room as the room block is limited
- Email events@a-isac.com with any questions

Q2 AvTech

- Registration is now open!
- Members will be emailed the information
- July 17-19, 2024
- Seeheim, Germany
- Thank you to Lufthansa for hosting!

AVIATION CYBER THREAT BRIEF

CYBER THREAT LANDSCAPE

RANSOMWARE

- Cloak ransomware
- Agenda ransomware
- RubyCarp (RO)

THREAT ACTORS

- JiaTan (CH?)
- UNC5221 (CH/APT)
- TA569 (SocGholish) (RU)

AREAS OF CONCERN

- NVD backlog
- China 3PLA officers found living in Canada

CYBER VULNERABILITIES

- XZ Utils
  (CVE-2024-3094, CVSS 10.0)
- Ivanti Connect Secure
  (CVE-2024-21894, CVSS 10.0)
  (CVE-2024-21893, CVSS 8.2)
  (CVE-2024-21894, CVSS 9.8)
- Windows Rust
  (CVE-2024-24576, CVSS 10.0)

GUEST PRESENTATION:

Data-Driven Third Party Risk Management: The Road to AI

Matthew Ancelin, Principal Solutions Architect, SecurityScorecard

SecurityScorecard

Data-Driven Third Party Risk Management: The Road to AI

AVIATION **ISAC**

Prepared for the Aviation ISAC
Matthew Ancelin, Principal Solutions Architect
April 2024

54%

of breaches in the last 12 months were **caused by third parties**

IBM Ponemon

solarwinds

A software update, SUNBURST, was weaponized to gain widespread persistent access to critical customer networks.
DECEMBER 2020, TECHTARGET

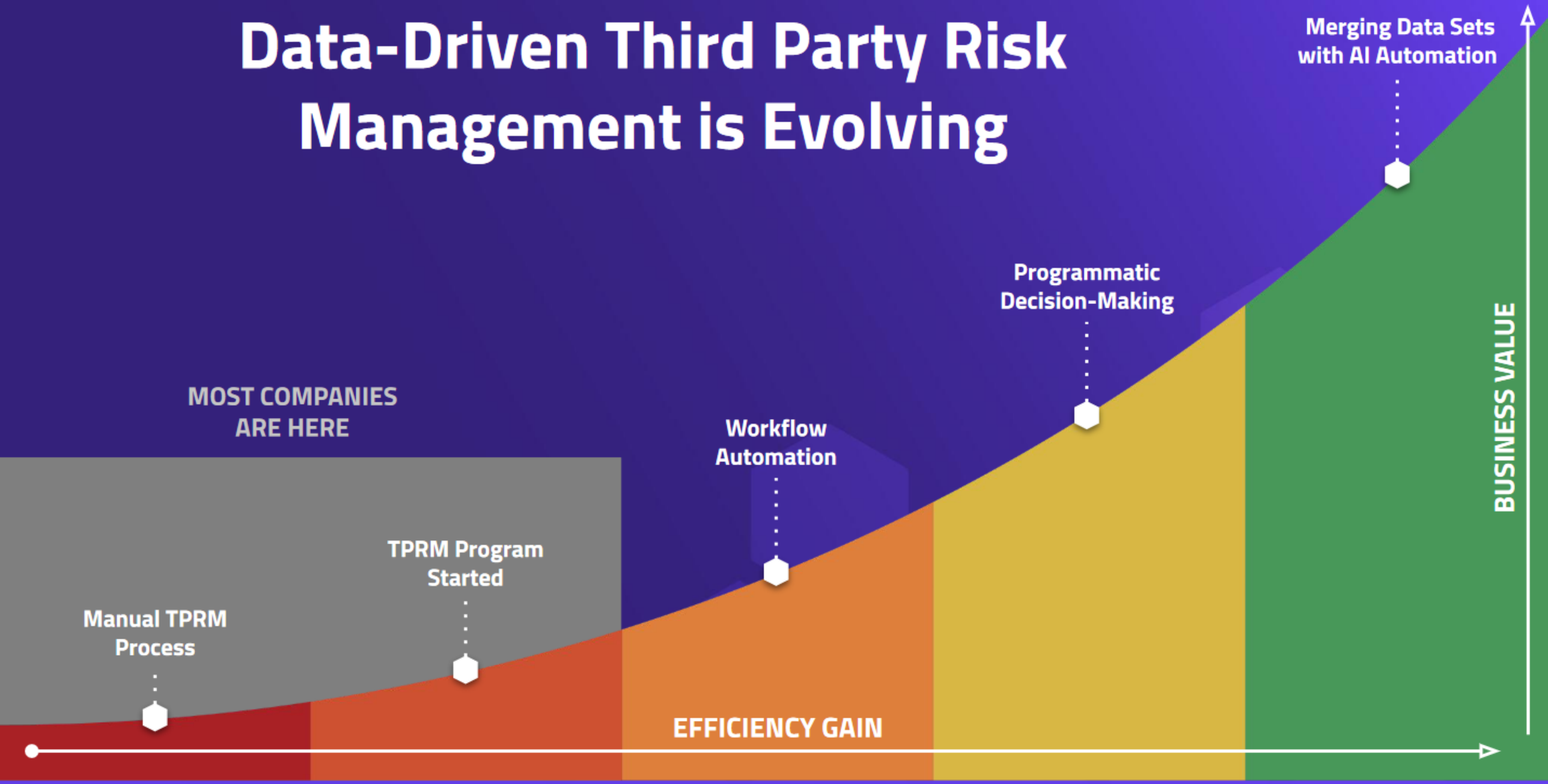
okta

LAPSUS$ gained control of an account belonging to a Costa Rica-based Sykes employee who provided services to Okta, gaining access to information on 2.5% of Okta's customer.
JANUARY 2022, FORBES

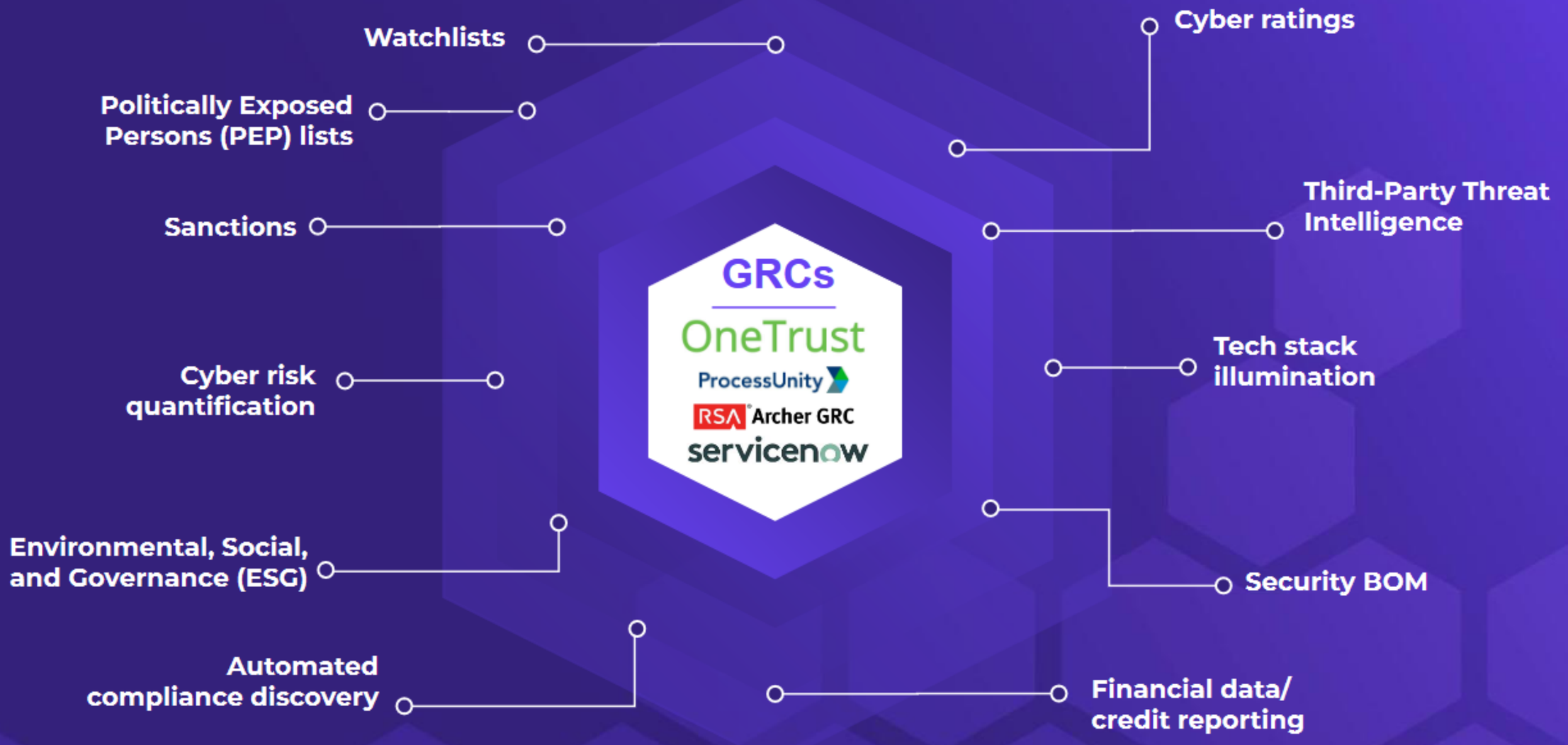
LastPass

LastPass attacked twice by threat actors gaining access through info available from third-party data breach and vulnerability in third-party media software, resulting in breach of encrypted password vaults.
FEBRUARY 2023, HACKERNEWS

Data-Driven Third Party Risk Management is Evolving



Programmatic TPRM decision-making requires continuous data



Merging data sets into AI-enabled GRC tools

- Watchlists
- Politically Exposed Persons (PEP) lists
- Sanctions
- Cyber risk quantification
- Environmental, Social, and Governance (ESG)
- Automated compliance discovery
- Cyber ratings
- Third-party threat intelligence
- Tech stack illumination
- Security BOM
- Financial data/ credit reporting

A primer on Artificial Intelligence and NLP

Types of Artificial Intelligence

From sources across the web

Machine learning

Natural language process...

Deep learning

Artificial general intellige...

Theory of mind

Computer vision

Expert system

Artificial neural network

Robotics

Automation

Unsupervised learning

Learning

SecurityScorecard

Natural Language Processing and Large Language Models

Types of Artificial Intelligence

From sources across the web

Machine learning

Artificial general intellige...

Expert system

Automation

Natural language process...

Theory of mind

Artificial neural network

Unsupervised learning

Deep learning

Computer vision

Robotics

Learning

SecurityScorecard

Natural Language Processing and Large Language Models

Types of Artificial Intelligence

From sources across the web

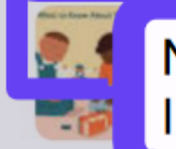

Machine learning


Artificial general intellige...


Expert system


Automation


Natural language process...


Narrow AI / Artificial Narrow Intelligence (ANI)


Large Language Models (LLM)


Unsupervised learning


Deep learning


Computer vision


Robotics


Learning

SecurityScorecard

Natural Language Processing and Large Language Models

General AI / Artificial General Intelligence (AGI)

Narrow AI / Artificial Narrow Intelligence (ANI)

Large Language Models (LLM)

Types of Artificial Intelligence

From sources across the web

Machine learning

Artificial general intellige...

Expert system

Automation

Natural language process...

Ar

Unsupervised learning

Deep learning

Computer vision

Robotics

Learning

SecurityScorecard

Natural Language Processing and Large Language Models

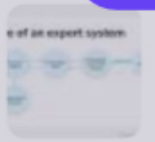
General AI / Artificial General Intelligence (AGI)

Types of Artificial Intelligence

From sources across the web

Machine learning

Deep Learning



Expert system

Automation

Natural language process...

Narrow AI / Artificial Narrow Intelligence (ANI)

Large Language Models (LLM)

Unsupervised learning

Deep learning

Computer vision

Robotics

Learning

SecurityScorecard

Examples of how AI is used today

- **Breach Collection:** to parse documents to determine 1st party, 3rd parties involved, who was affected, what type of attack or what data lost.

- **Co-Pilot Tool:** companion tool which produces summaries of scorecards highlighting decision making criteria.

- **Knowledge Base Chat Bot:** trained on our KB articles and help files to help our support organizations find answers using plain language.

Examples of how AI is used today

Framework Questionnaire auto-complete: leveraging an LLM solution on previously answered questionnaires to pre-fill contextually matched answers to new questionnaires.

Sample Questions & AI-Generated Responses

"What security frameworks are you compliant with?"	We are compliant with ISO 27001 and ISO 22307. Additionally, we follow a Secure SDLC that is aligned with OWASP security standards and includes Static and Dynamic code analysis, Manual Penetration testing, and Open Source Software assessments. We also have a Veracode certification that complies with OWASP security standards and includes white, grey, and black-box testing.
"what precautions are taken to protect data in transit?"	We take several precautions to protect data in transit. We use secure communication protocols such as HTTPS and SFTP to encrypt data during transmission. Additionally, we implement access controls and encryption on our communication channels to prevent unauthorized access. We also have policies and procedures in place to ensure that data is properly labeled and classified, and that appropriate security measures are applied based on the sensitivity of the data. Finally, we regularly monitor our communication channels for security breaches and vulnerabilities, and we have incident response plans in place to address any security incidents that may arise.
“What is the company’s address?”	The company's address is One Vanderbilt Avenue, 60th Floor, New York, NY 10017.
"How do you enforce endpoint security?	We enforce endpoint security through a centrally managed anti-malware solution, network IPS/IDS, host IDS/IPS, ACL, next-gen firewalls, and Microsoft Domain Controller, Microsoft Intune, and perimeter scanners. Additionally, we have a process that requires security approval to allow external networks to connect to the company network, and we enforce the least privilege necessary. Physical access to data processing equipment is also restricted, and our facilities are governed by a physical protection policy that is reviewed at least once annually.

Aspirational future uses of AI in 3rd party risk

- **Assessment documentation:** parsing documents such as questionnaires, SOC2 reports, Pen Test results, Insurance, and Compliance documentation
- **Vendor interactions:** conversational AI generated emails, requesting documents and working through assessment requirements with human or AI vendor counterparts.
- **Natural Language Search:** trained on all SSC data sources, the ability to analyze and synthesize results, action items, summaries, and relationship based recommendations.
- **Breach Prediction:** AI trained on both internal signals and external signals and intelligence to predict attack vectors, breach likelihood, and truly grade resilience.
- **Vendor management scaling:** Leveraging all of the above, 10X, 100X more vendors can be managed, more effectively, by the same staffing levels. ***Greater business outcomes*** from the TPRM/VRM program.

* These concepts are ideas only, no commitment to future product development

Problems to overcome on the road to AI

- **Underlying data flaws:** garbage in, garbage out still remains true.
- **Integration points:** No single source of data today truly covers all aspects of Risk or Vendor Risk Management. Credentials to multiple platforms given to AI presents its own security issue.
- **Labor force shifts/disruptions:** unlike gradual labor migrations of the past, this is happening fast and broad.

Analysis and Findings for the members of the Aviation ISAC

Matthew Ancelin, Principal Solutions Architect

Updated: 4/9/24

Aviation ISAC Findings Summary

Portfolio Average Rating

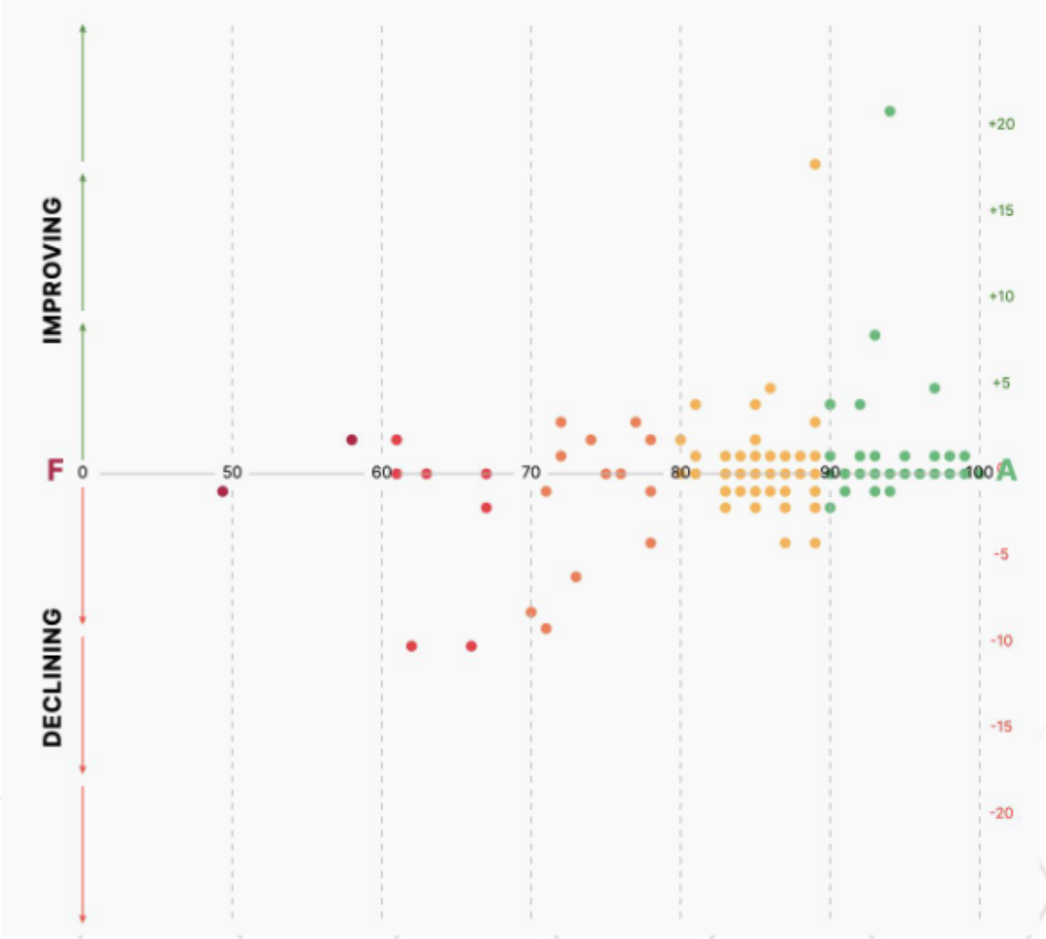
85

Portfolio Rating Distribution

135 companies

View List

31 active (23%)
104 inactive (77%)



- 19 members with exposed database(s)
- 5 members with exposed ICS
- 17 members with Ransomware susceptible related issues
- 6 members with darkweb Ransomware published data or mentions
- 32 members with mobile malware
- 11 members with active malware infection

SecurityScorecard

CVE's to watch: campaigned by major APT threat actors

43% of ISAC members show potential exposure of **CVE-2022-23943**

- Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Recent campaign activity by the following threat actors:
  - Gamaredon Group

10% of ISAC members show potential exposure to **CVE-2021-44142**

- The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
- Recent campaign activity by:

Tropic Trooper	Earth Berberoka
Gamaredon Group	Sandworm Team
Silence Hacker Group	The Shadow Brokers
APT41	Moses Staff APT
Pirate Panda	MuddyWater Group
Equation Group	Antlion APT
Cobalt Group	APT35

40% of ISAC members show potential exposure to **CVE-2018-15919**

- Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
- Recent campaign activity by:
  - APT35
  - Mustang Panda
  - APT37
  - APT28
  - Sandworm Team
  - APT39
  - Kimsuky
  - Cobalt Group

Vendors to Watch: 10%-33% concentration risk across ISAC Members

Securit

ecard

QUESTIONS