G2M RESEARCH

Bug Bounties Gone Bad?

January 12, 2023

IBM YOUATTEST®

ESET®

G2M Webinar Ground Rules

G2M RESEARCH

- **G2M Research will record this webinar**
  ➔ We will send a link to the recording and a PDF of the slides for the webinar to all registrants approximately 2 days after webinar
- **You are strongly encouraged to ask questions**
  ➔ Please use the Zoom Q&A feature to submit your questions; we will go through all questions at the end of the session
- **We will conduct some audience surveys during the webinar**
  ➔ Please answer using the Zoom survey tool (and all answers are anonymous, so no one will know how you answered)

Thanks!

Webinar Agenda

10:00-10:03	Webinar Kickoff and Ground Rules (Mike)
10:04-10:08	Uber Case Highlights (Karen)
10:09-10:11	Matt Johnson Introduction (3 minutes)
10:12-10:14	Garret Grajek Introduction (3 minutes)
10:15-10:17	Tony Anscombe Introduction (3 minutes)
10:18-10:18	Audience Survey #1
10:19-10:28	Panel Question #1
10:29-10:29	Audience Survey #2
10:30-10:39	Panel Question #2
10:40-10:40	Audience Survey #3
10:41-10:50	Panel Question #3
10:51-10:58	Audience Q&A
10:59-11:00	Wrap-Up

Panelists

Matt Johnson
Principal Security Architect
www.ibm.com

Garret Grajek, CEH, CISSP
Chief Executive Officer
www.youattest.com

Tony Anscombe
Chief Security Evangelist
www.eset.com

Karen Heumann
Principal Cybersecurity Analyst
www.g2minc.com

Facts From the Uber Case

- In October 2016, hackers sought $100,000 in ransom from Uber in exchange for not disclosing the personal information for 50 million customers and 7 million drivers that they had hacked.
- After consulting with his team, Joe Sullivan (Uber CISO at the time) used “bug bounty” money to pay the ransom
  - Sullivan did not report the breach, even though Uber was under investigation for a 2014 breach at the time
- In its case, the government remarked that they had never seen a crime so well-documented.
  - The max payment from the bug bounty program was supposed to be $10,000
  - The payment of $100,000 was approved by then-CEO Travis Kalanick
  - The hackers signed an NDA
- When Dara Khosrowshahi took over as CEO in August 2017, he learned of the breach/coverup and fired Joe Sullivan, reported the breach, and worked with the government in its case against Joe Sullivan.
- Sullivan was convicted of obstruction and misprision (guilty knowledge of a felony) in Oct 2022.

Sources: Axios (Oct 7, 2022), Forbes (Oct 2022), New York Times (Oct 5, 2022), Washington Post (Oct 5, 2022), Security Week (Oct 5, 2022), Justice.gov (Oct 2022)

Why Is This Important Today?

- Ransomware attacks are on the rise
  - In 2017 there were 184M reported breaches compared to 623M attacks in 2021
  - The FBI does not support paying a ransom in response to a ransomware attack because paying a ransom incentivizes criminal activity and doesn't guarantee you will get any data back
- More jurisdictions require notifications when breaches occur (with even larger penalties for not notifying in a timely fashion)
- Many companies do not have a formal process for employees and vendors to report breaches
- Bug bounty programs (or using a 3rd party to run them) doesn't negate a company's responsibilities

IBM

Matt Johnson

Principal Security Architect

www.ibm.com

Matthew “MJ” Johnson

Principal Security Architect @ IBM

Years Maturing Organizations from ”Chaos to Organized Chaos”

- 15 Years as Security Operations practitioner/manager
- Built Large Security Operations Centers and CSIRT Teams for Federal (Military), State and Local Government and Large Scale Commercial Entities.
    - US Navy, State of Colorado Worlds Largest Medical Response Organization
    - Ran Security Operations and Incident Response for Fortune 100 Media Company and Financial Firms.
- Builds and Develops large scale security operations plans and Architectures for several Fortune 100 firms

Proactive Security is the only way to become successful in a modern security world

- Lead 100s of Incidents over the course of 15 years in Security
- Ran Large Scale Incident Response Efforts against multiple sophisticated Advanced Persistent Threats (APTs)
- Developed security operations teams, plans, and infrastructure on shoestring budgets to proactively defend environments
- Led efforts on several large Merger and Acquisitions to ensure secure unification of several large scale originations

YOUATTEST®

Garret Grajek

(CEH, CISSP)

Chief Executive Officer

www.youattest.com

YOUATTEST®

Cloud IGA
Automated and Simplified

www.youattest.com

FACT:

All organizations must know who is doing what with which systems (identity attestation).

REALITY:

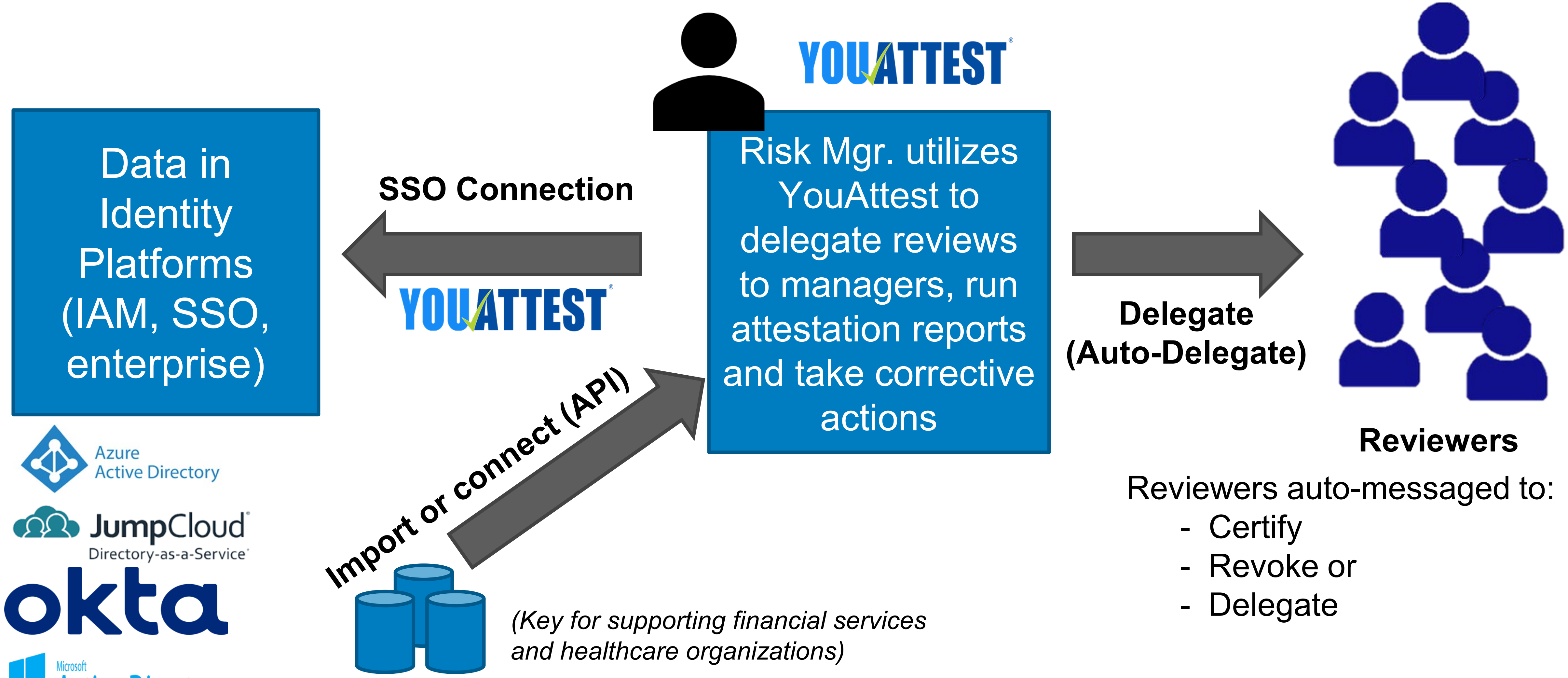
Outside of large corporations with armies of auditors, very few are doing this.

This is a problem.

YouAttest…

- An IGA focused product to automate:
  - Access Reviews
    - Applications
    - User / Groups
    - AD PAM and Service Accounts
  - Trigger/Attest on Access, ACL, Permission Changes
    - Users, Groups, Domain Admins, Service Accounts
  - Creates Identity Access review “evidence” (reports) for:
    - SOX, SOC 2 Type 2, ISO 27001, PCI-DSS, NIST, HIPAA/HITRUST, CMMC
- Big Differentiator:
  - Rapid Integration to all resources: Azure AD, Okta, JumpCloud & API, generic uploads

The Product - How YouAttest Works



Data in Identity Platforms (IAM, SSO, enterprise)

SSO Connection

YOUATTEST

Risk Mgr. utilizes YouAttest to delegate reviews to managers, run attestation reports and take corrective actions

Delegate (Auto-Delegate)

Reviewers

Import or connect (API)

Azure Active Directory

JumpCloud Directory-as-a-Service

okta

Microsoft Active Directory

Other Identity Stores

(Key for supporting financial services and healthcare organizations)

Siloed Resources

Reviewers auto-messaged to:

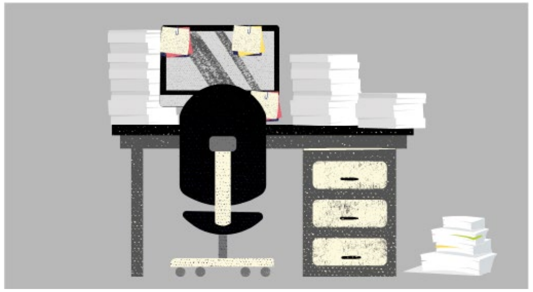
- Certify
- Revoke or
- Delegate

YouAttest auto-collates reviews and creates a report relevant to : SOX, SOC 2 Type 2, ISO 27001, PCI-DSS, NIST, HIPAA/HiTRUST, and CMMC type audits

YouAttest: Manual vs YouAttest for Access Reviews

YOUATTEST

YOUATTEST vs Manual



Access Review Action:	YouAttest:	Manual:
• Export to CVS or import from SSO tool	0.5 -1 hr.	1 hr.
• Identity Managers	Auto	2-4 hrs
• Create separate attestations per manager	Auto	4-12 hrs
• Send attestations to managers	Auto	2-4 hrs
• 1st line Managers delegate to 2nd line	30 mins	4-12 hrs
• Enable YouAttest Multiple Reviewers	Auto	4-12 hrs
• Mgr Conduct review verifying role info (per review)	0.5 – 2 hrs	4-12 hrs
• Nag e-mails/reminders	Auto	2-10 days
• Collate/Format Reports to single view	Auto	4-12 hrs
• Reports in centralized, cloud repository	Auto	4-12 hrs
• Repeatable	Yes	No
	4-12 hrs	5-14 days

Questions & Discussion

Garret F. Grajek

ceo@youattest.com

+1.714.658.0765

YouAttest

info@youattest.com

877.452.0496

Tony Anscombe

Chief Security Analyst

www.eset.com

Tony Anscombe

Chief Security Evangelist

@TonyAtESET
https://www.linkedin.com/in/tonyanscombe/
Tony.Anscombe@eset.com

Tony Anscombe is the Chief Security Evangelist for ESET. With over 20 years of security industry experience, Anscombe is an established author, blogger and speaker on the current threat landscape, security technologies and products, data protection, privacy and trust, and Internet safety. His speaking portfolio includes industry conferences RSA, Black Hat, VB, CTIA, MEF, Gartner Risk and Security Summit and the Child Internet Safety Summit (CIS). Anscombe is a current board member of the NCSA.

About ESET

- **Number One** EU Cybersecurity Company for Business
- **1Bn+** Internet users protected by our technology
- **400K+** Business customers
- **110M** Users

Trusted by Enterprise customers worldwide:

MITSUBISHI MOTORS
Drive your Ambition

Allianz
Suisse

Canon
Canon Marketing Japan Group

● HEADQUARTERS

Bratislava

● REGIONAL CENTERS

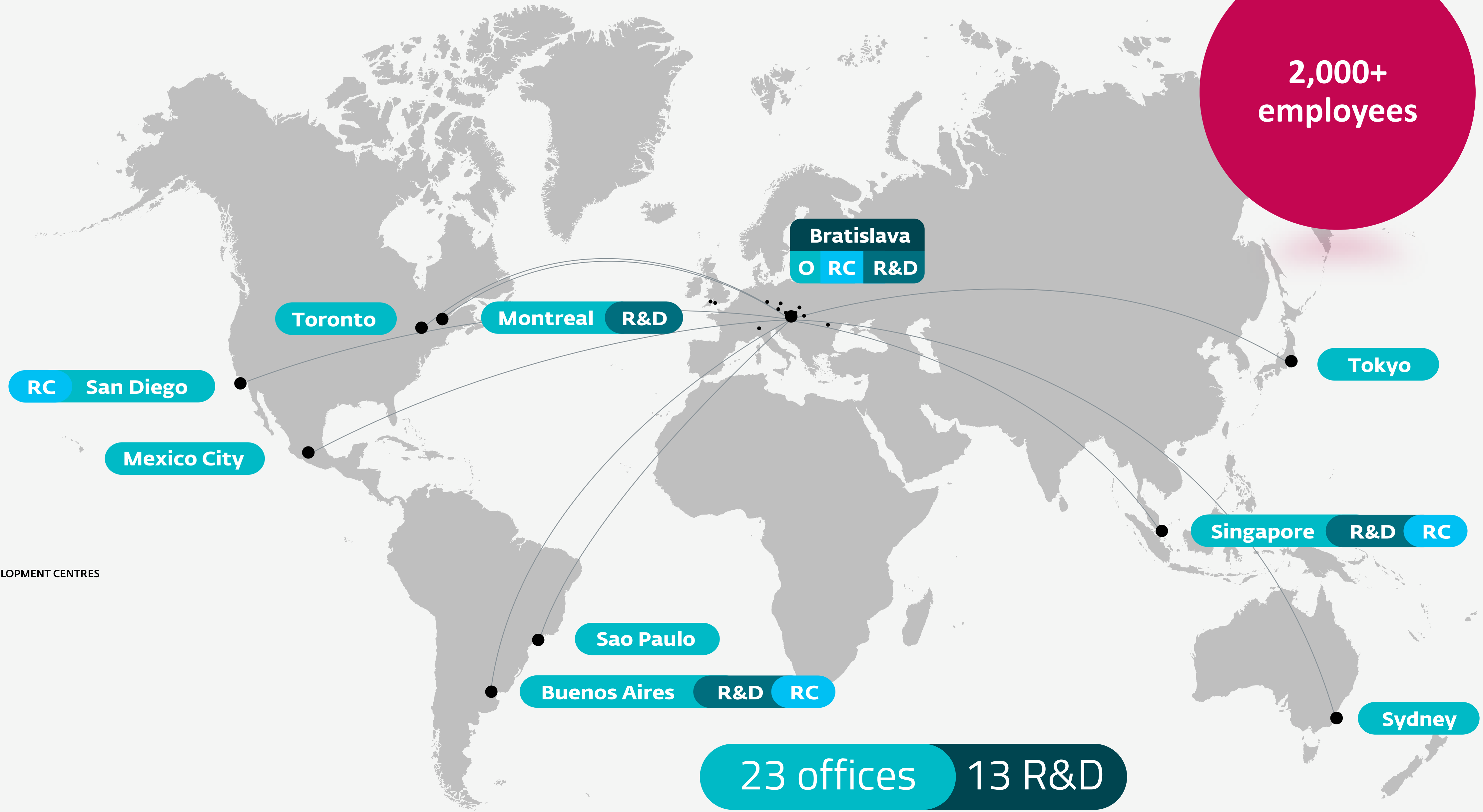
San Diego
Buenos Aires
Singapore

● OFFICES

Prague
Jablonec nad Nisou
Sao Paulo
Jena
Krakow
Sydney
Taunton
Bournemouth
Toronto
Montreal
Iași
Mexico City
Zilina
Brno
Tokyo
Milan

● RESEARCH AND DEVELOPMENT CENTRES

Bratislava
San Diego
Buenos Aires
Singapore
Prague
Košice
Krakow
Montreal
Zilina
Iași
Brno
Taunton



2,000+ employees

23 offices 13 R&D

Panel Questions and Audience Surveys

Audience Survey #1

Does your company have an active bug bounty program? (select one)

• Yes, we currently have a bug bounty program:	27%
• We do not today, but are starting one in the next 3 months:	0%
• We used to have one, but we did not continue it:	0%
• We have never had a bug bounty program:	40%
• Don’t know:	33%

Panel Question #1

The Joe Sullivan case illustrated risks and responsibilities that many in our industry did not previously consider as issues before. How much of these are specific to the Uber situation versus being a new part of the “CISO landscape”?

- Matt Johnson (IBM)
- Garret Grajek (YouAttest)
- Tony Anscombe (ESET)

Audience Survey #2

G2M RESEARCH

Does your company have an internal process to report data breaches by your company or vendors? (select all that apply)

- We have a process to report company data breaches: 33%
- We provide regular training for employees on how to report data breaches: 13%
- We have a process for vendors to report data breaches: 40%
- We work with our vendors' security organizations to ensure that they train their people on their process: 7%
- We require vendors to report data breaches, but we do not manage their processes or training: 13%
- We do not have a process to report company data breaches: 20%
- Don't know/no opinion: 27%

Panel Question #2

To what extent do bug bounty programs operated by third parties reduce liabilities for companies?

- Garret Grajek (YouAttest)
- Tony Anscombe (ESET)
- Matt Johnson (IBM)

Audience Survey #3

G2M RESEARCH

At what point does the company's legal staff (either inside or outside) get involved with potential breaches? (select all that apply)

• As soon as we suspect that a breach has occurred.	38%
• As soon as we confirm that a breach has occurred.	25%
• As a part of informing the company's executives and BoD.	0%
• We only get the company's legal staff involved when directed by the company CISO.	0%
• We only get the company's legal staff involved when directed by the company CEO.	13%
• Don't know/no opinion:	38%

Panel Question #3

What are the top 2-3 lessons that CISOs and other cybersecurity experts can learn from the Uber case?

- Tony Anscombe (ESET)
- Matt Johnson (IBM)
- Garret Grajek (YouAttest)

Audience Q&A

Panelists

Matt Johnson
Principal Security Architect
www.ibm.com

Garret Grajek, CEH, CISSP
Chief Executive Officer
www.youattest.com

Tony Anscombe
Chief Security Evangelist
www.eset.com

Karen Heumann
Principal Cybersecurity Analyst
www.g2minc.com

G2M RESEARCH

Effective Marketing & Communications with Quantifiable Results