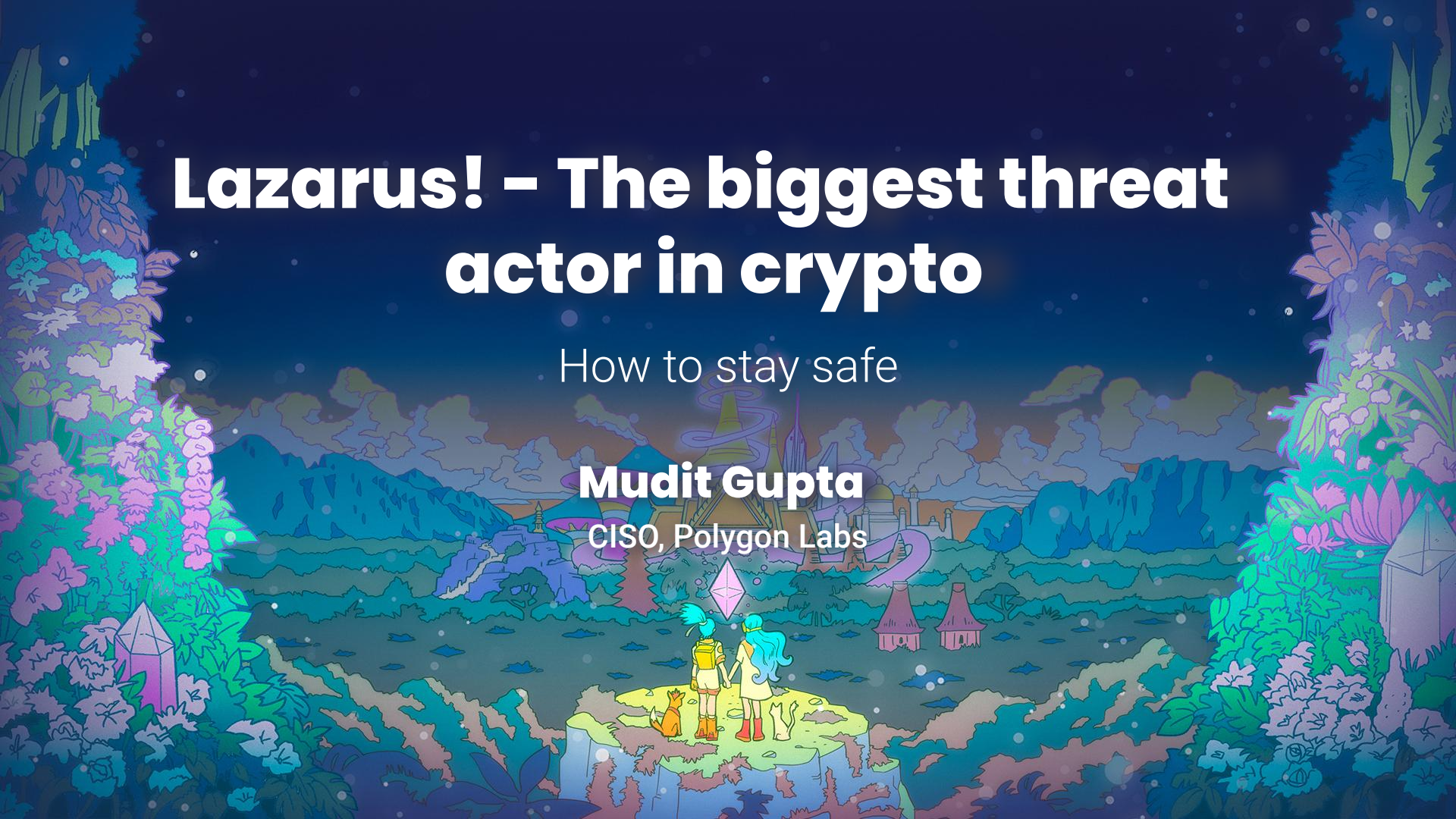
Lazarus! - The biggest threat actor in crypto

How to stay safe

Mudit Gupta

CISO, Polygon Labs



Lizard us who?

Who is Lazarus

- North korean hacker group
- Started out with simple DDoS against South Korea around 2009
- Started targeting banks in 2014, also hit Sony
- Focusing on crypto exchanges since 2017
- Hit DeFi jackpot in 2022 with 600m axie, 100m horizon hacks

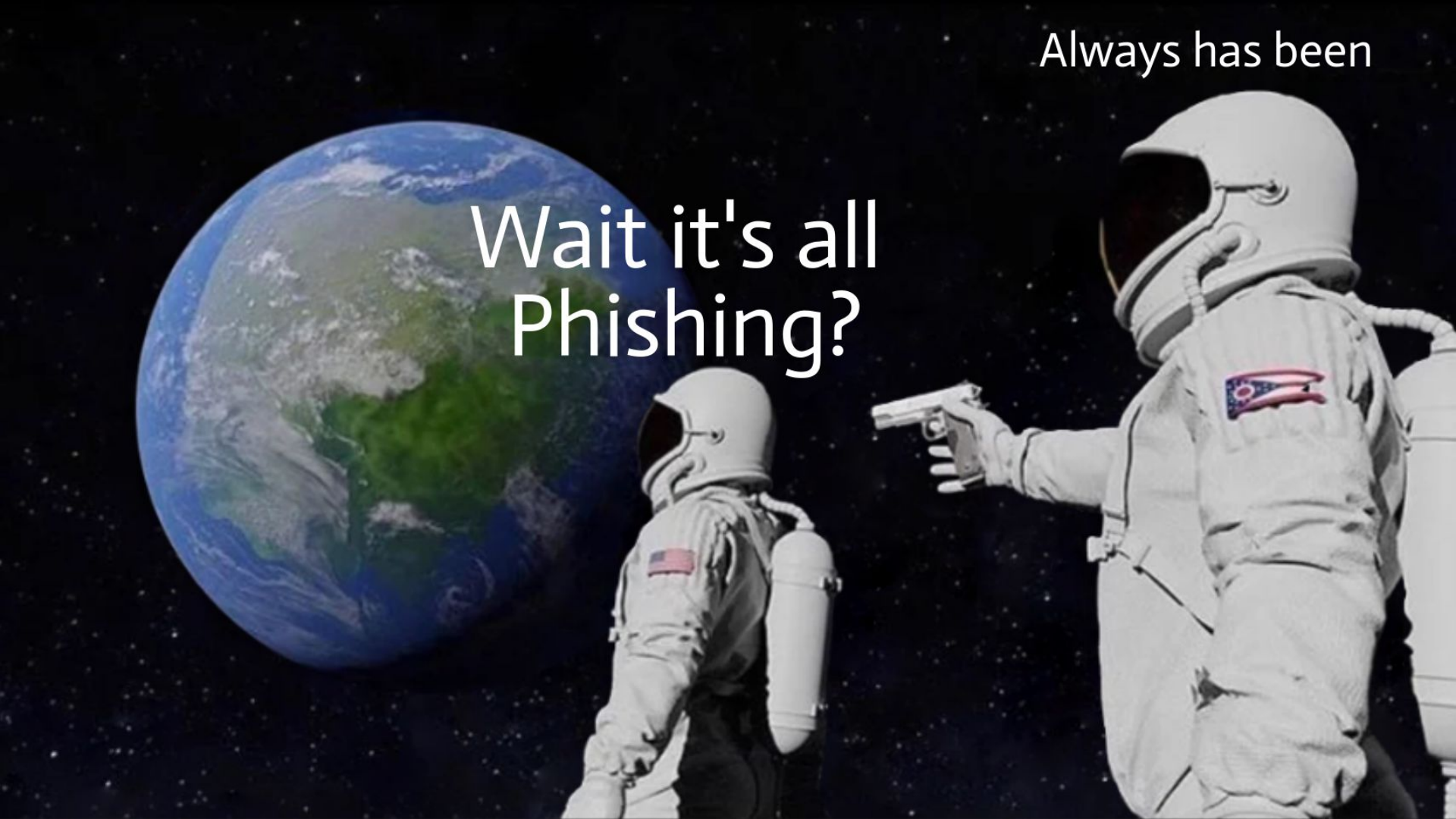
Year	Attack Name/Incident	Losses (Estimated)	Techniques Used
2017	Bithumb Exchange Hack	$7 million	Phishing, Social Engineering, Malware
2018	Coincheck Hack	$534 million	Spear Phishing, Exploitation of Poor Security Practices
2018	Youbit Exchange Hack	Unknown	Spear Phishing, Malware, Insider Compromise
2019	Upbit Exchange Hack	$49 million	Phishing, Unauthorized Access, API Exploitation
2020	KuCoin Exchange Hack	$275 million	Social Engineering, Unauthorized Access, Exploitation of Hot Wallets
2020	Eterbase Hack	$5.4 million	Phishing, Credential Stuffing, Exploitation of Hot Wallets
2021	Liquid Exchange Hack	$97 million	Phishing, Credential Theft, Social Engineering
2021	Ronin Network Hack	$600 million	Exploitation of Validator Nodes, Social Engineering
2022	Harmony Bridge Hack	$100 million	Exploitation of Multisig Wallet Vulnerabilities, Social Engineering
2023	Horizon Bridge Hack	$100 million	Exploitation of Smart Contract Vulnerabilities, Phishing
2024	WazirX Incident	$235 million	Phishing, Social Engineering, API Exploitation

Top Crypto hacks by Lazarus

How do they do it?

Do you see anything common?

Year	Attack Name/Incident	Losses (Estimated)	Techniques Used
2017	Bithumb Exchange Hack	$7 million	Phishing, Social Engineering, Malware
2018	Coincheck Hack	$534 million	Spear Phishing, Exploitation of Poor Security Practices
2018	Youbit Exchange Hack	Unknown	Spear Phishing, Malware, Insider Compromise
2019	Upbit Exchange Hack	$49 million	Phishing, Unauthorized Access, API Exploitation
2020	KuCoin Exchange Hack	$275 million	Social Engineering, Unauthorized Access, Exploitation of Hot Wallets
2020	Eterbase Hack	$5.4 million	Phishing, Credential Stuffing, Exploitation of Hot Wallets
2021	Liquid Exchange Hack	$97 million	Phishing, Credential Theft, Social Engineering
2021	Ronin Network Hack	$600 million	Exploitation of Validator Nodes, Social Engineering
2022	Harmony Bridge Hack	$100 million	Exploitation of Multisig Wallet Vulnerabilities, Social Engineering
2023	Horizon Bridge Hack	$100 million	Exploitation of Smart Contract Vulnerabilities, Phishing
2024	WazirX Incident	$235 million	Phishing, Social Engineering, API Exploitation


Always has been
Wait it's all Phishing?

Social Engineering

Social engineering techniques

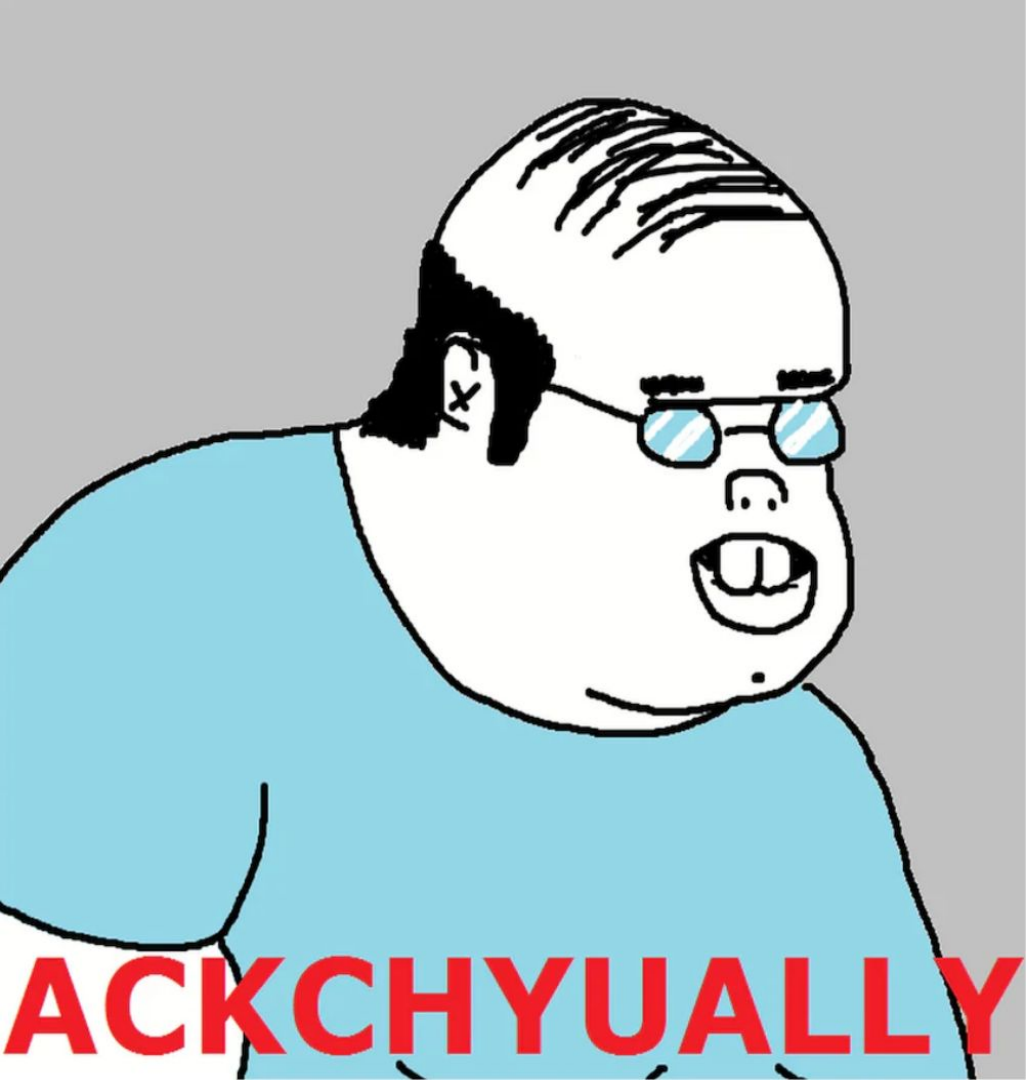
- Getting hired at your company
- VC Investment
- News interview
- Job listings
- Fake video call
- Malicious PDFs
- Malicious extensions
- Malicious feedback site
- Fake advertisements
- Fake airdrops
- Fake Docusign
- Fake order placed
- Fake discord verification
- Fake exchange listing
- Package delivery problem
- Quid-pro-quo
- Fake devcon side event ticket
- Tons more.....

How to stay safe from Social Engineering

- Phishing awareness trainings and phishing campaigns
- Be Skeptical of Unsolicited Communications
- Verify Identities Independently
- Avoid Clicking Suspicious Links or Attachments
- Use Strong, Unique Passwords
- Enable Two-Factor Authentication (2FA) and avoid SMS
- Keep Software Updated
- Educate Yourself and Others
- Limit Personal Information Sharing
- Report Suspicious Activity

YOU ARE GOING TO GET PHISHED

Layers of Security



Year	Attack Name/Incident	Losses (Estimated)	Techniques Used
2017	Bithumb Exchange Hack	$7 million	Phishing, Social Engineering, Malware
2018	Coincheck Hack	$534 million	Spear Phishing, Exploitation of Poor Security Practices
2018	Youbit Exchange Hack	Unknown	Spear Phishing, Malware, Insider Compromise
2019	Upbit Exchange Hack	$49 million	Phishing, Unauthorized Access, API Exploitation
2020	KuCoin Exchange Hack	$275 million	Social Engineering, Unauthorized Access, Exploitation of Hot Wallets
2020	Eterbase Hack	$5.4 million	Phishing, Credential Stuffing, Exploitation of Hot Wallets
2021	Liquid Exchange Hack	$97 million	Phishing, Credential Theft, Social Engineering
2021	Ronin Network Hack	$600 million	Exploitation of Validator Nodes, Social Engineering
2022	Harmony Bridge Hack	$100 million	Exploitation of Multisig Wallet Vulnerabilities, Social Engineering
2023	Horizon Bridge Hack	$100 million	Exploitation of Smart Contract Vulnerabilities, Phishing
2024	WazirX Incident	$235 million	Phishing, Social Engineering, API Exploitation

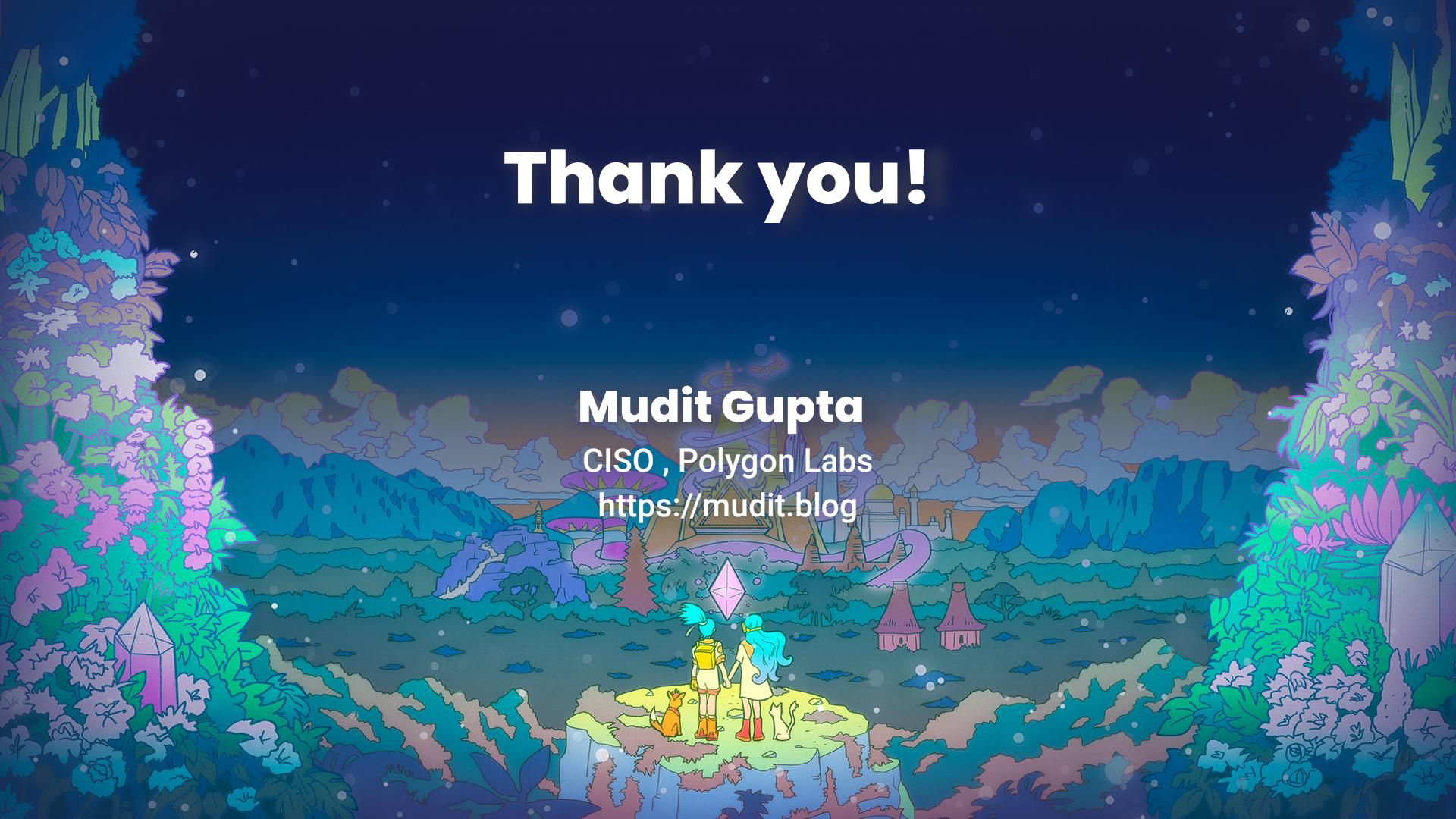
What layers?

- Principle of least privilege
- Multiple factors of authentication
- MDM/EDR
- Security monitoring and alerting
- No single point of failure
- Secure architecture
- Minimized trust
- Safe custody
- Spider sense

How to custody safely

Safe custody

- Consider using professional custodians
- Use hardware wallets
- Do not share your mnemonic/seed phrase/private key with anyone
- Connect hardware wallets via browser wallets
- Use a dedicated (semi-airgapped) device for signing
- Verify what you’re signing on the browser wallet
- USE MULTISIGS!
- Ensure secure threshold for multisigs
- Verify hash on hardware wallets (safe-tx-hashes-util from pcaversaccio)
- Use diverse set of hardware including mobile devices for signers
- Do not ignore failures


Thank you!
Mudit Gupta
CISO , Polygon Labs
https://mudit.blog

Enter your slide title here

Your slide subtitle here.

Your Name
Your title, your organization

Section 1

Section 1 title here.

Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
    - Condimentum
        - Magna
        - Ligula

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 2 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Section 3

Section 3 title here.

Enter your main point / statement here.

Section 3 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Enter your main point / statement here.

Here’s the timeline.

Event 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”
— Pythagoras

Thank you!

Your Name
Your title, your organization
your@email.address
@youraccount

Enter your slide title here

Your slide subtitle here.

Your Name

Your title, your organization

Section 1

Section 1 title here.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 2 details with an image.
Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Section 3

Section 3 title here.

Enter your main point / statement here.

Section 3 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Enter your main point / statement here.

Here's the timeline.

Event 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

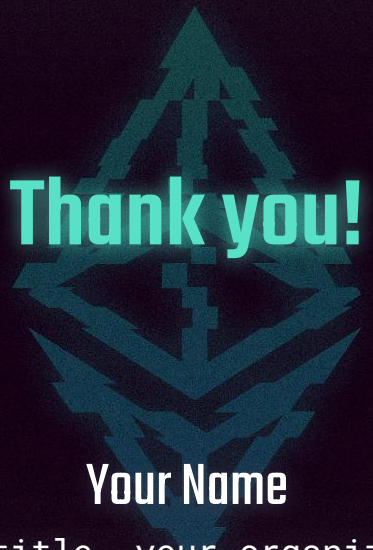
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”
— Pythagoras



Thank you!

Your Name

Your title, your organization

your@email.address

@youraccount