
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT012

SPONSORED BY JUPITERONE

Cyber hygiene strategies for security leaders

Shane Jones

Senior Director, Cloud Alliances
JupiterOne

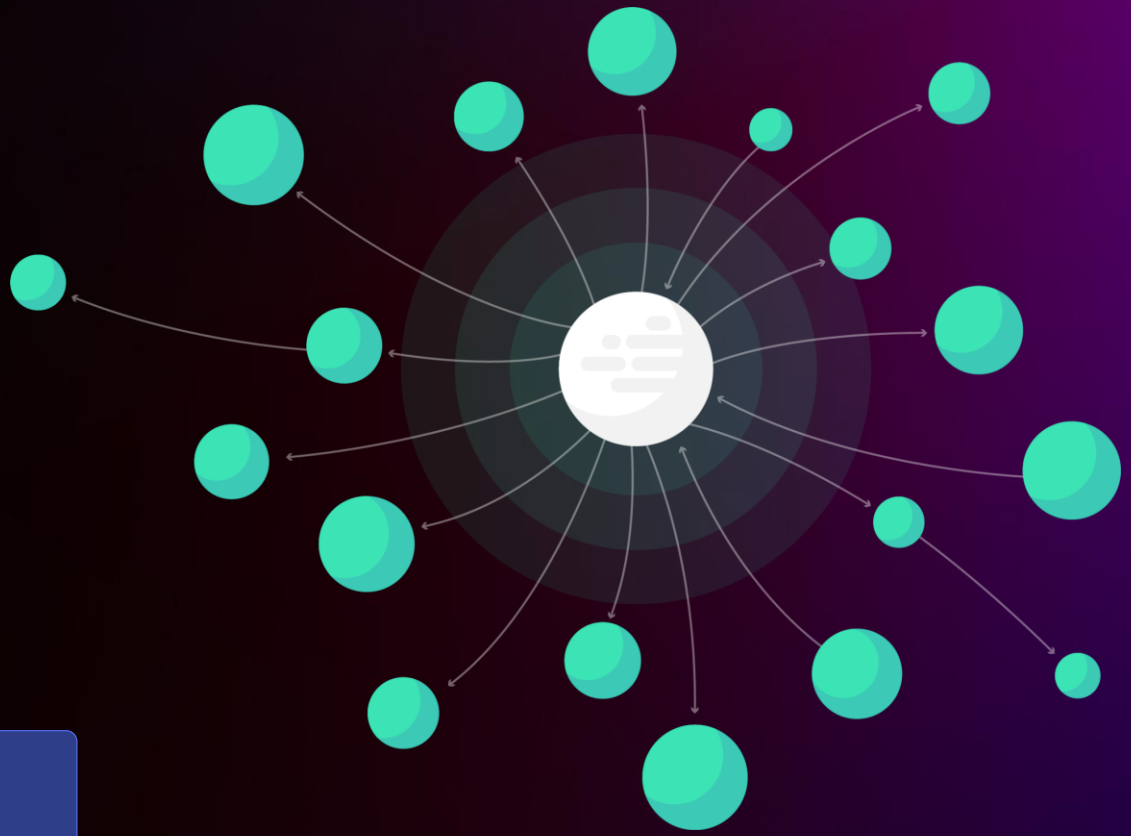
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The cloud revolution

The cloud revolution has led to new security challenges…

- Preventing the growth of security issues
- Controlling the attack surface and potential entry points
- Detecting when cybersecurity events happen, and preventing them



Security experts must think in graphs rather than lists to support security in the cloud

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud security trends

Security teams have many assets to secure . . .

27%
companies

are now using more than one public cloud

79%
companies

have experienced at least one cloud data event

165K+
cyber assets

in the average asset ecosystem that the security team is responsible for

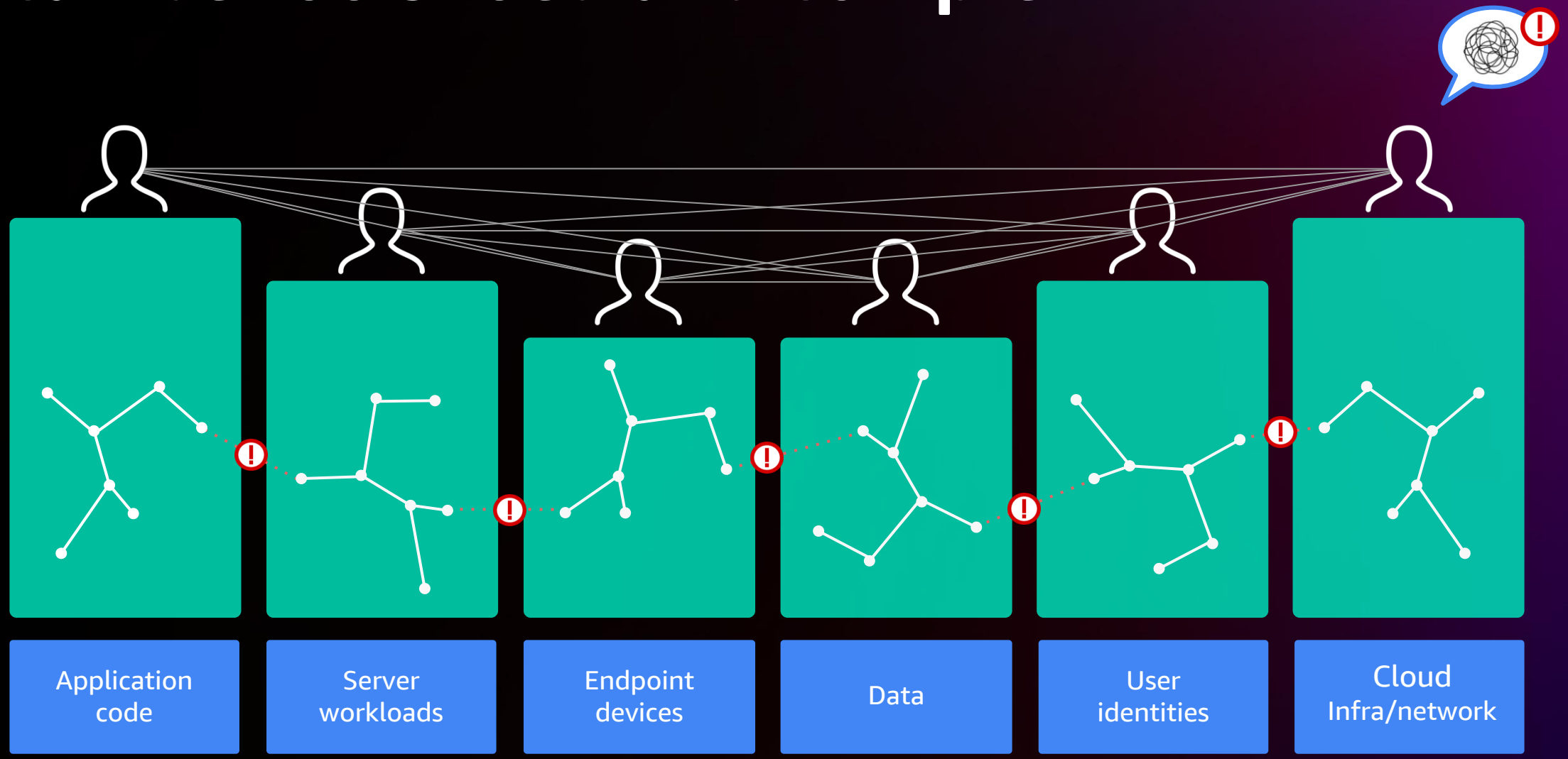
130+
security tools

that the average enterprise uses –
A lot of point-solution security tools

aws

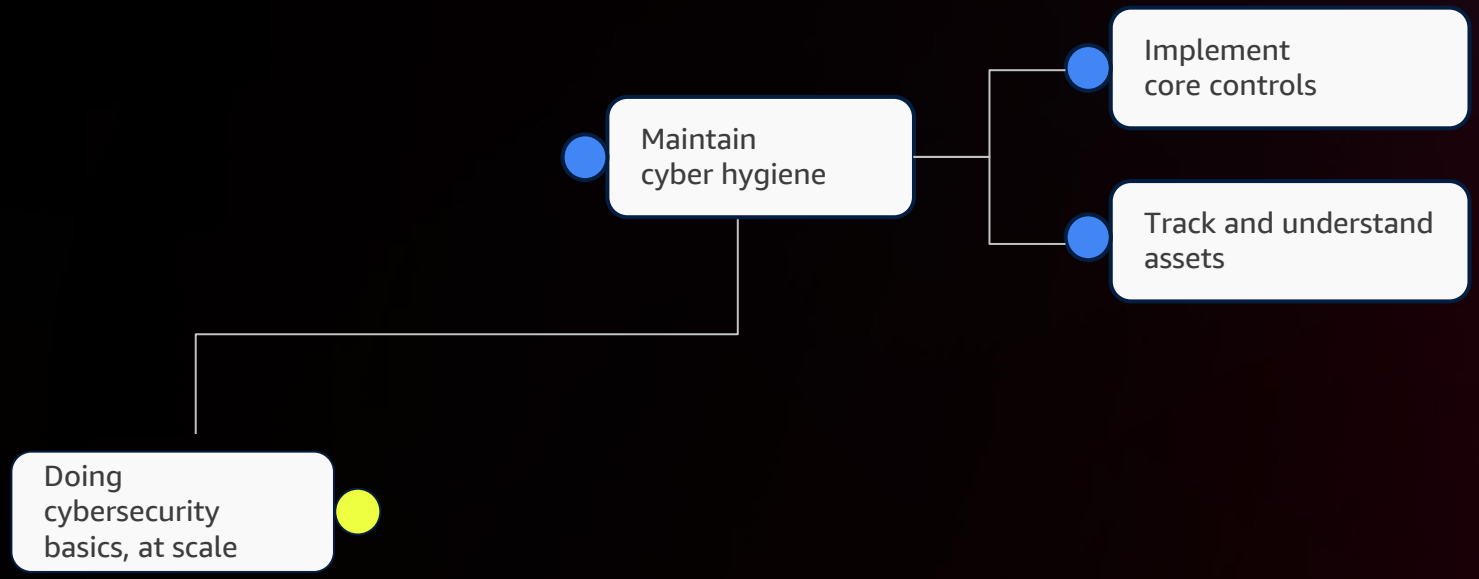
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

It can be too siloed and complex



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Doing security basics well, at scale



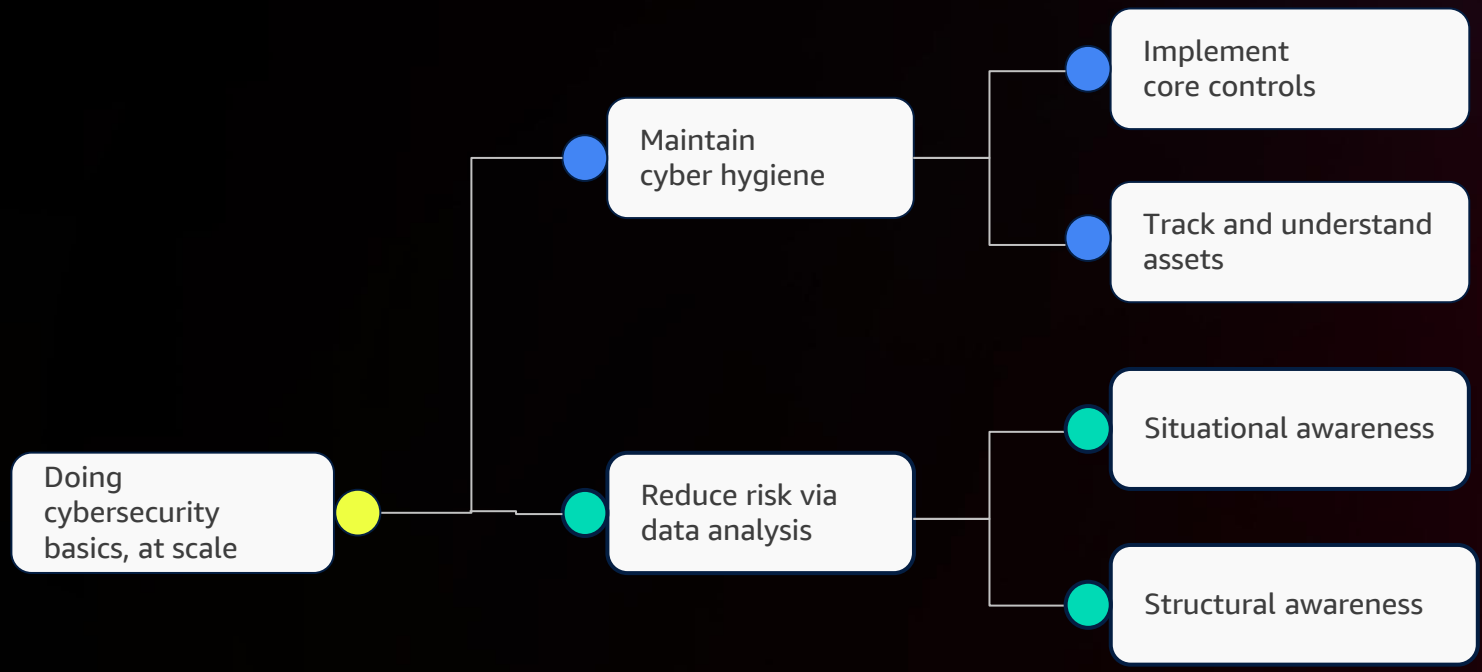
Rethink the basics for good cyber hygiene

- Begin with implementing core controls – such as multi-factor authentication (MFA), ongoing security awareness training, endpoint protection, etc.
- Track all cyber assets (not just IT assets) and their relationships (how the dots are connected)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Doing security basics well, at scale

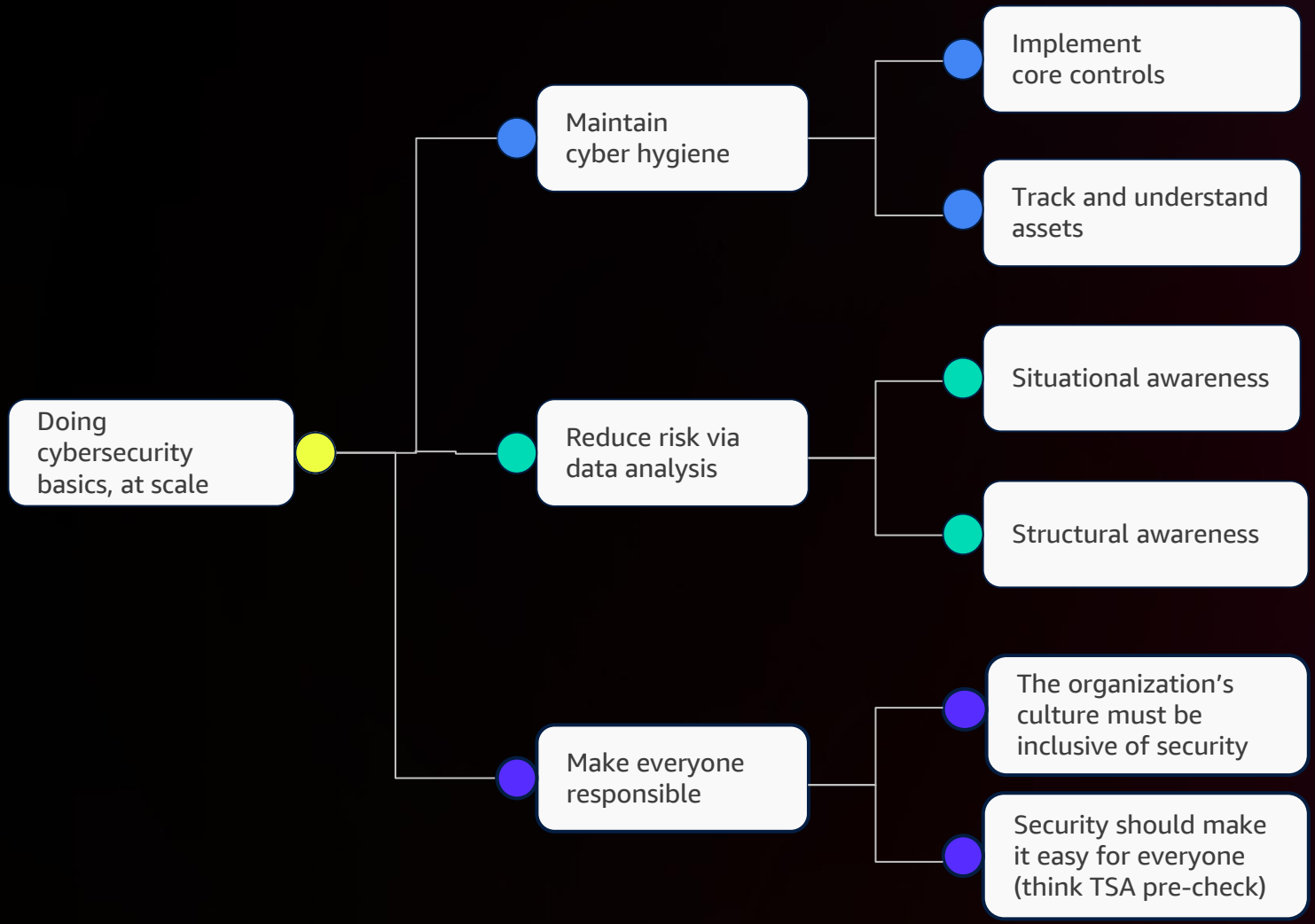


Gain both structural awareness and situational awareness

- Structural awareness comes from stateful data, often found in configuration analysis.
- Situational awareness comes from activities and behavioral analysis

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Doing security basics well, at scale

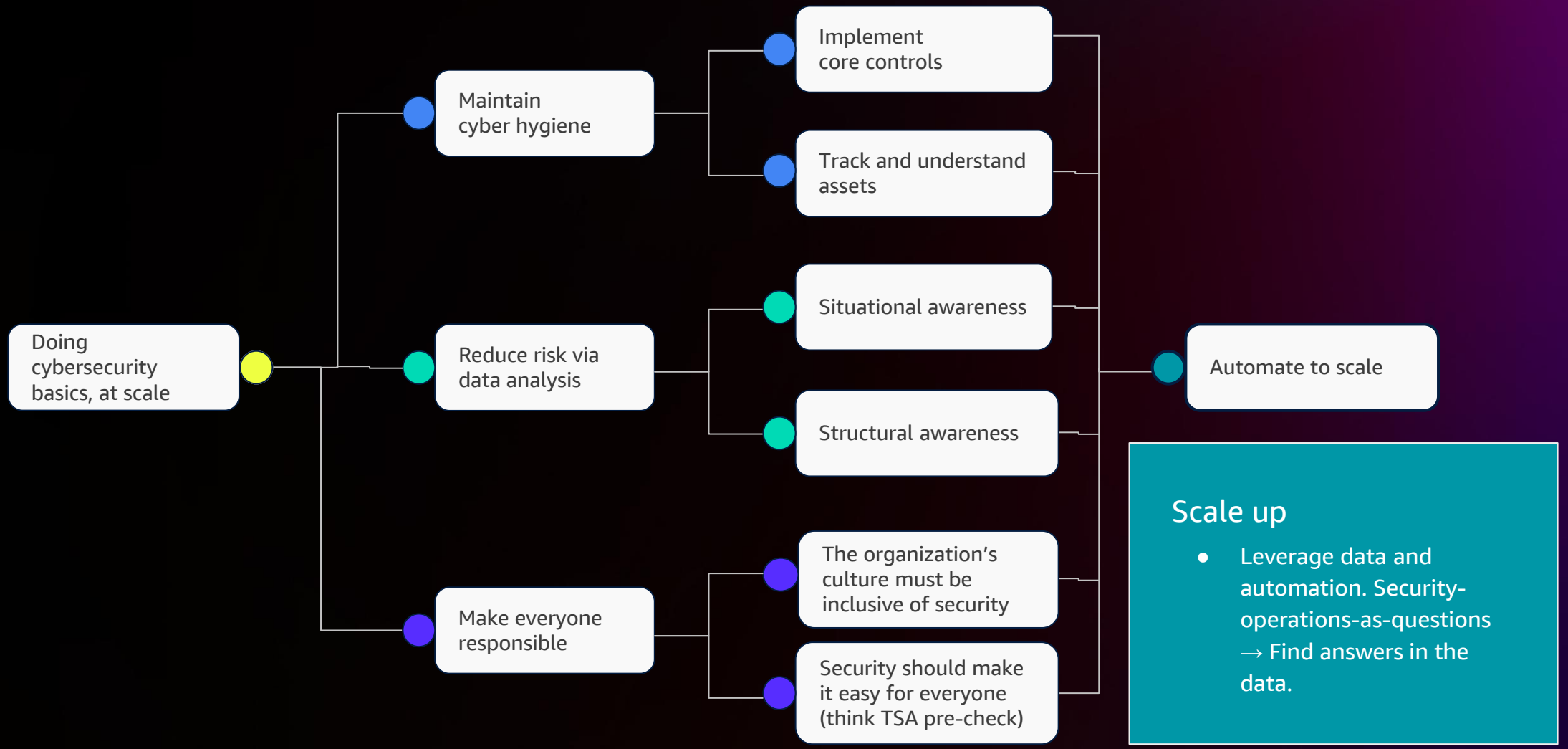


Involve people across the organization

- Form a mutually supportive and beneficial relationship between security and the business (especially engineering)
- Unusable security can be worse than no security

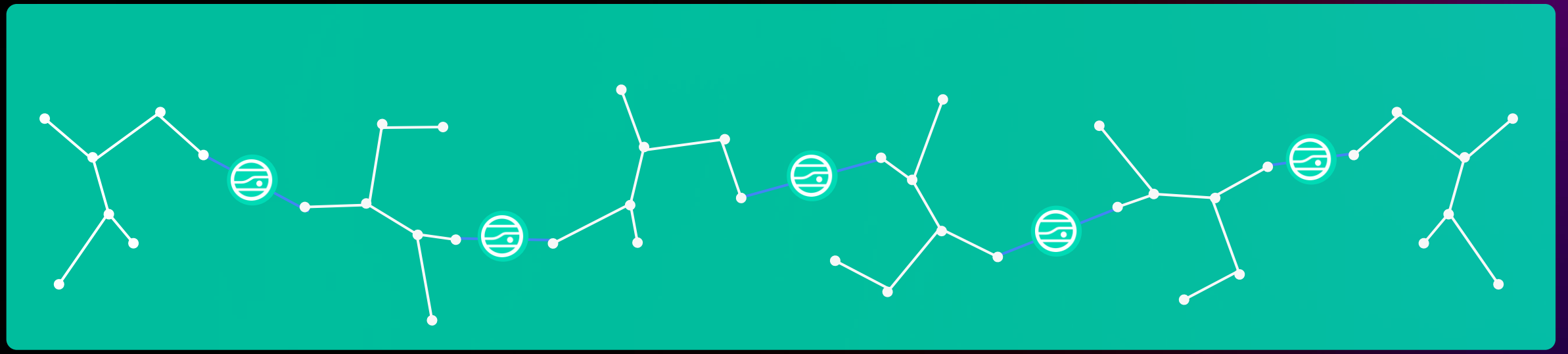
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Doing security basics well, at scale



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.





Application code	Server workloads	Endpoint devices	Data	User identities	Cloud Infra/network

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

- Implement core controls and track cyber assets
- Conduct data analysis with both structural and situational data
- Build community across your organization
- Use data and automation to gain true visibility and scale

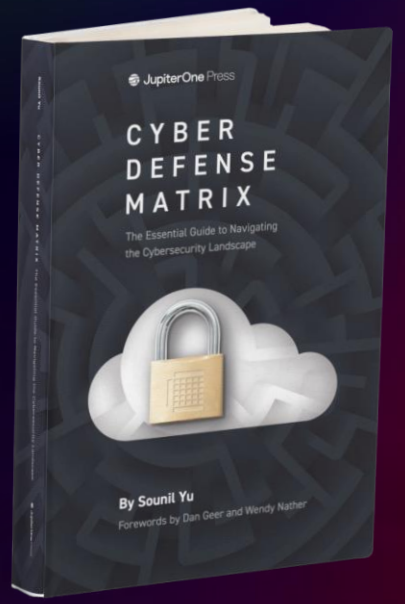


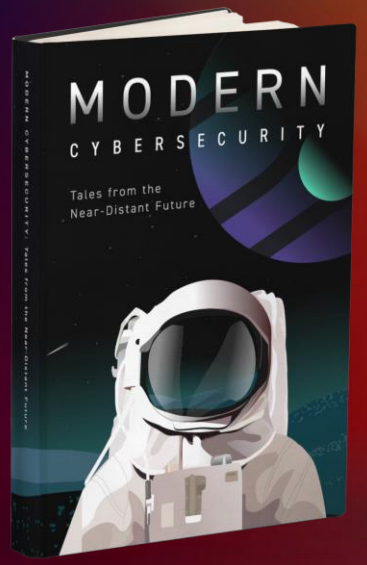
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources









All available on: https://try.jupiterone.com/resources

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Shane Jones
shane.jones@jupiterone.com
JupiterOne.com | askj1.com | github.com/JupiterOne



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.