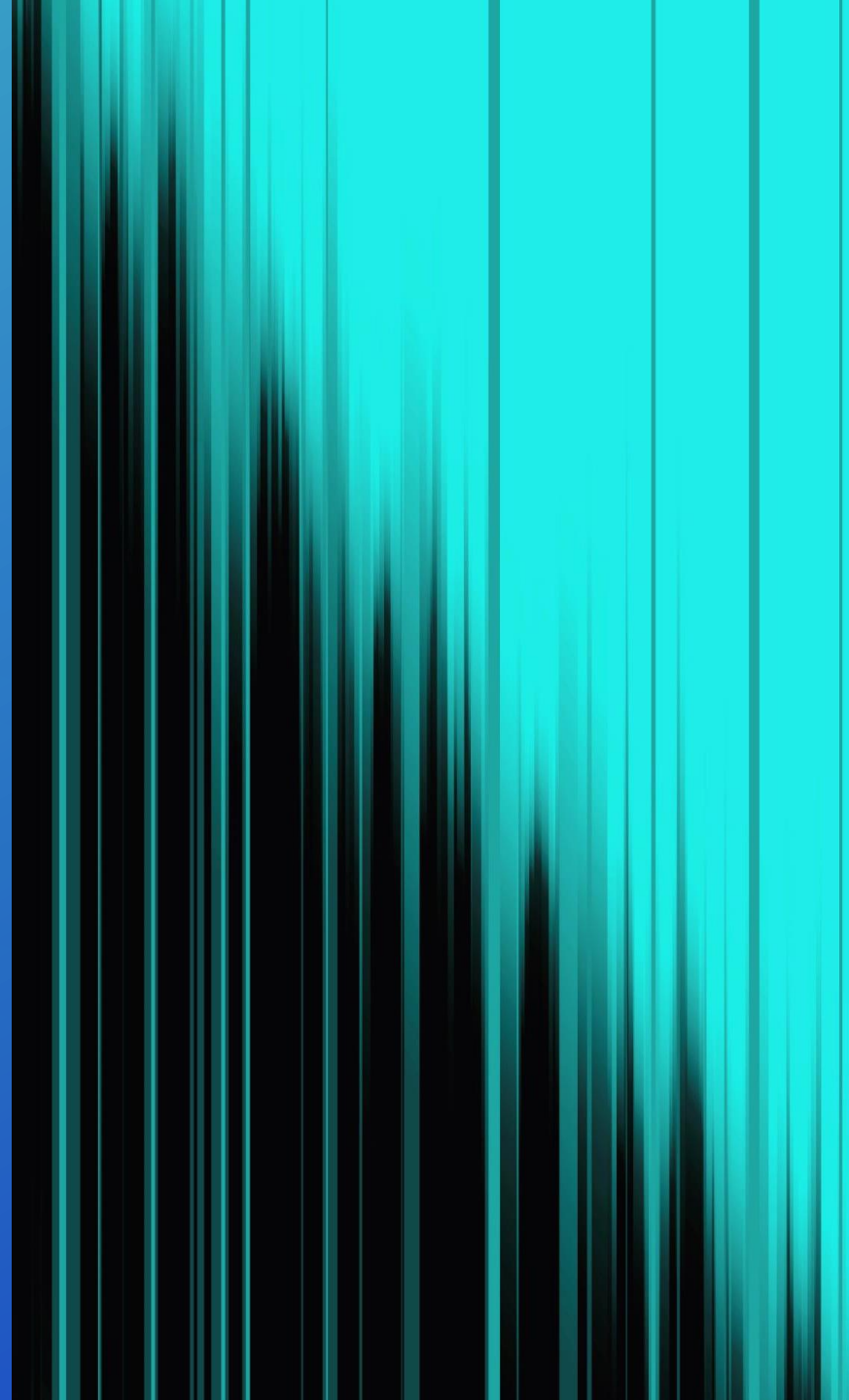
EXTERNAL ATTACK SURFACE MANAGEMENT

CHINTAN GURJAR



CHINTAN GURJAR

- 9 years of experience
- Security Engineering Manager
- MSc. Computer Security & Forensics - University of Bedfordshire, UK
- CEH, OSCP, CCFA, CCFH, CTIA
- Interests: Threat & Vulnerability Management, Threat Hunting, Shadow IT, Attack Surface Analysis, Security Management, Penetration Testing, UBEA
- https://github.com/iamthefrogy/FYI

chintangurjar@outlook.com

AGENDA

WHY

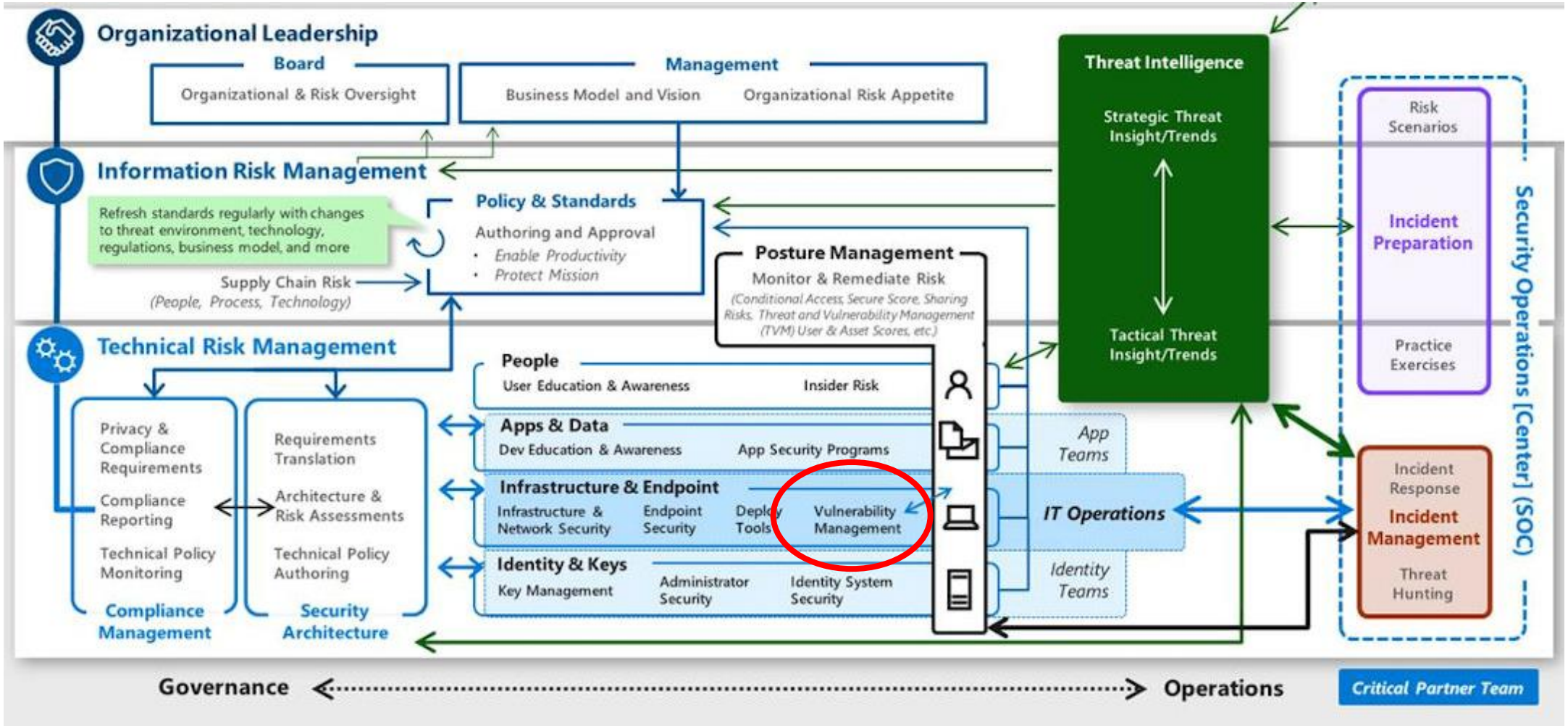
WHAT

HOW

TIPS & TRICKS

BENIFITS

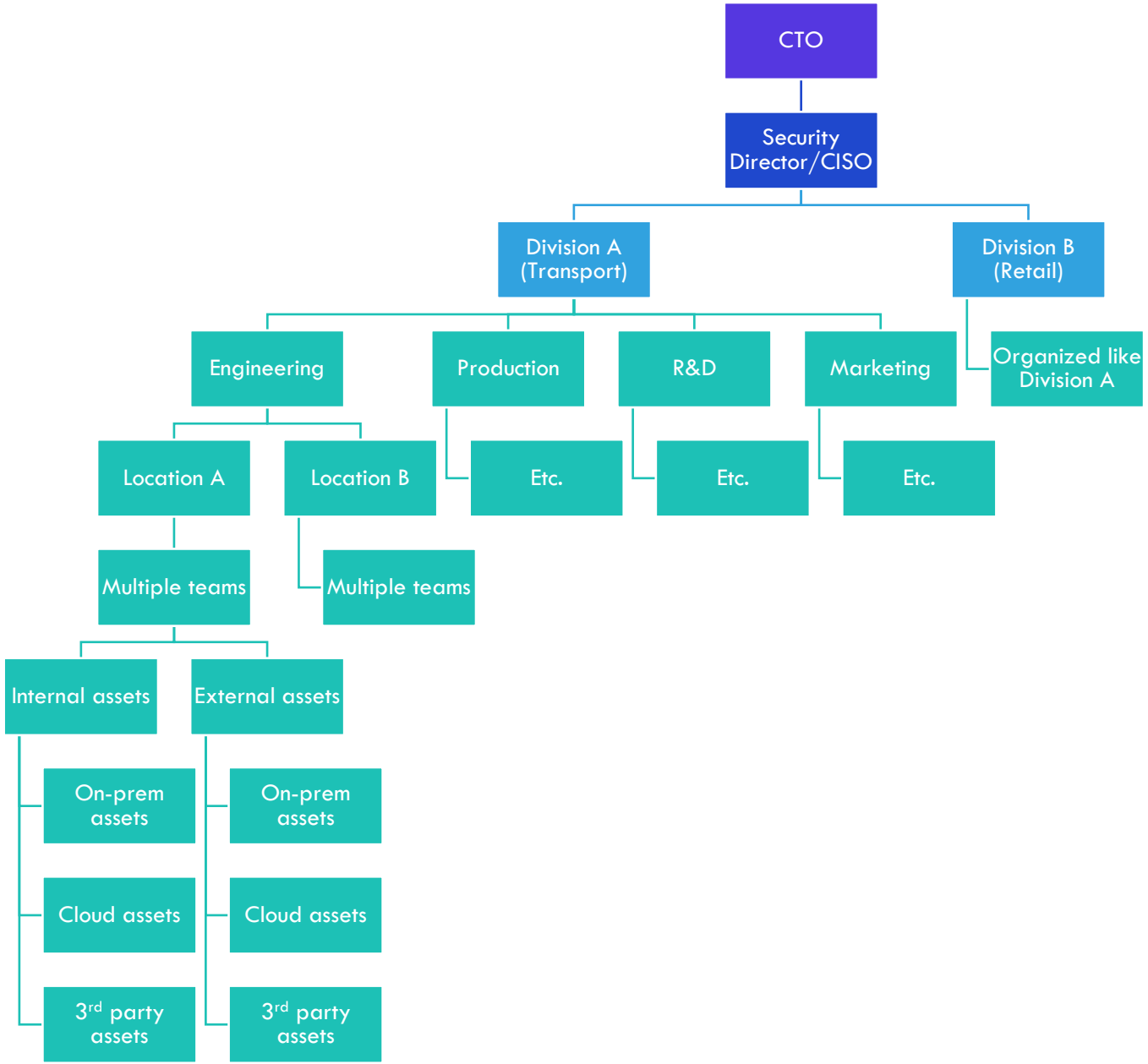
WHERE DOES IT FIT INTO CYBER LANDSCAPE



https://www.microsoft.com/security/blog/2020/08/06/organize-security-team-evolution-cybersecurity-roles-responsibilities/

WHAT

- E-Corp. Large Enterprise's External Assets



WHAT

- E-Corp. Large Enterprise's External Assets
  - Knowns
  - Unknowns (Focus Area)

W H Y

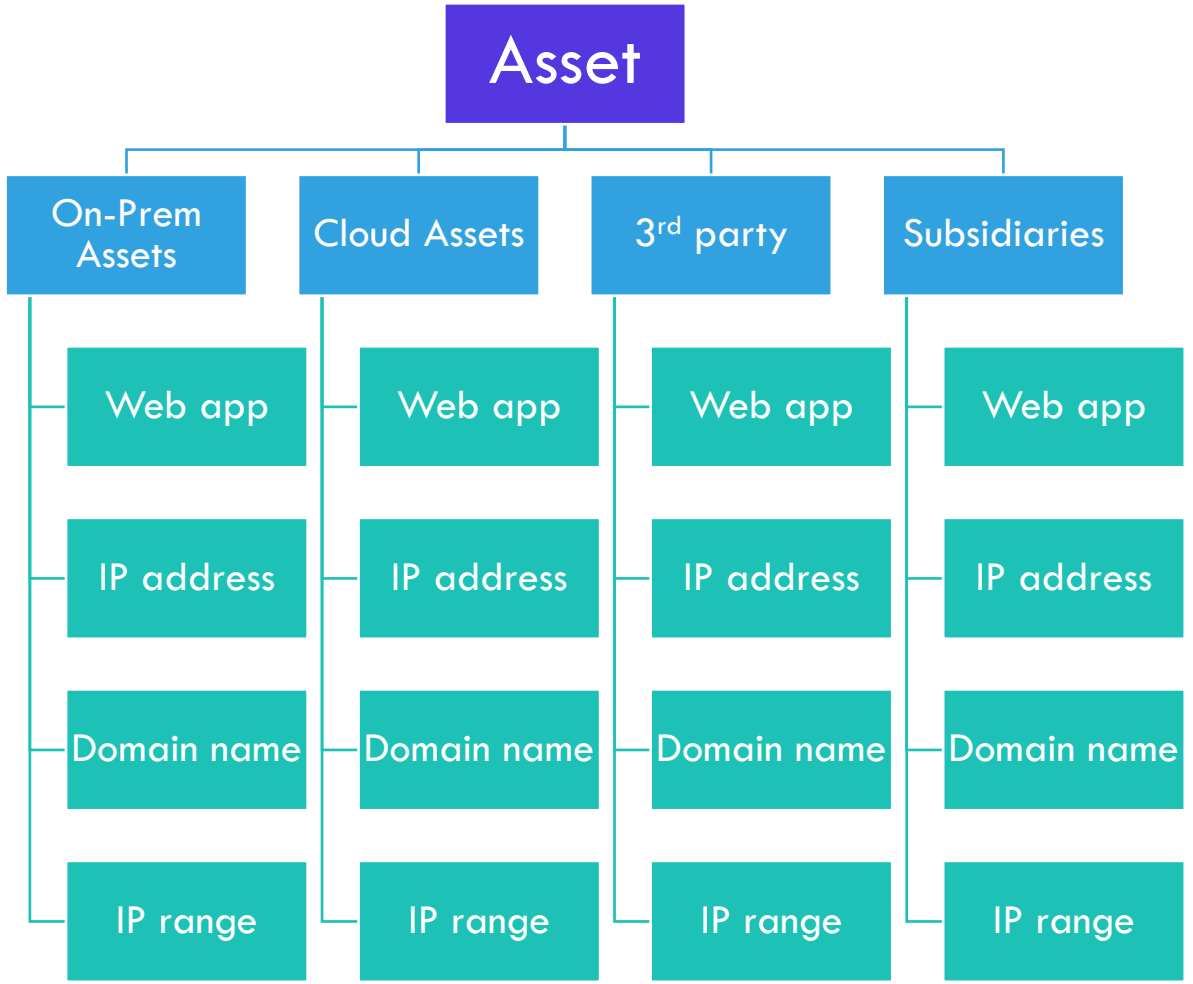
- **Knowns**
  - Known Risk
  - Managed
  - Automated
  - Remediated
- **Unknowns**
  - No clue at all

- **Why Unknowns**
  - No asset inventory
  - No external to Internal mapping & vice versa
  - Subsidiaries & Third-parties
  - Multiple regions across the world
  - No centralised IS policies or compliance in place

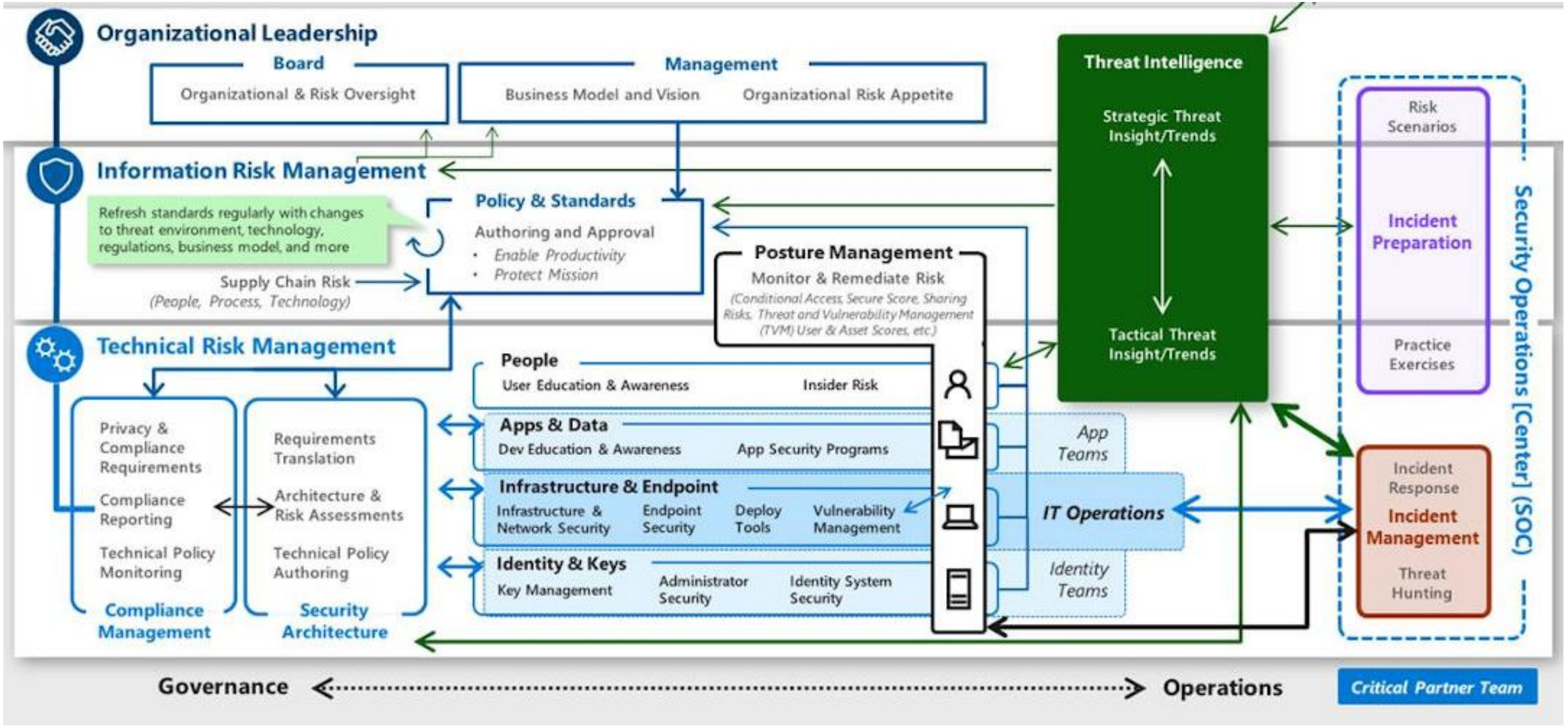
Multiple reasons…

H O W

- Four simple steps:
  1. **Find Unknown Assets** →



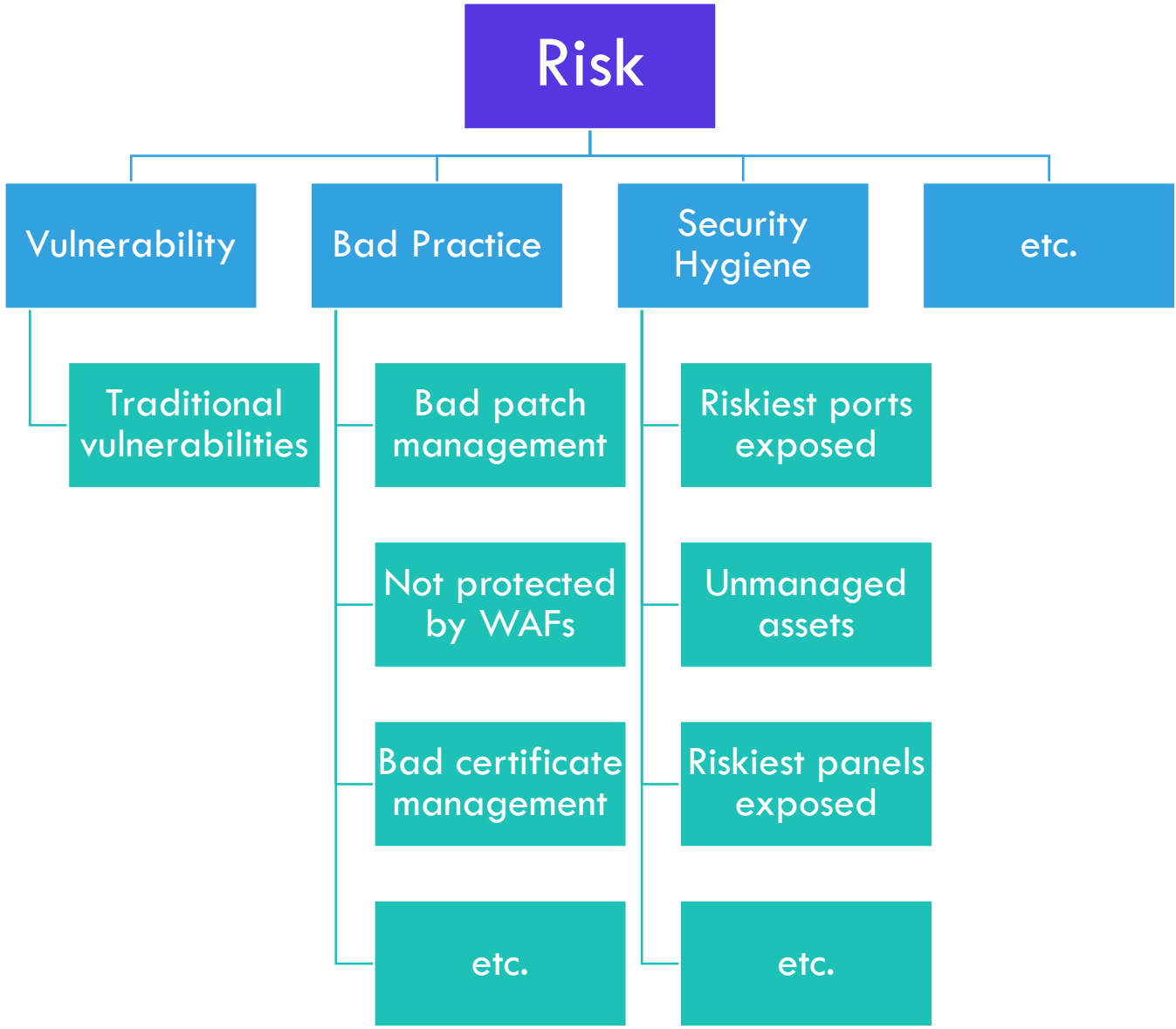
- **How to find external unknown assets:**
  - Use an existing asset inventory as starting point
  - Utilize open-source tools (Amaas, Subfinder, Sublist3r, Findomain, Dnscan, Crt.sh, WHOIS, Dnsdumpster, etc.)
  - Utilize existing security scanners' inventory from Vulnerability Management team (Qualys, Tenable, Nexpose, Netsparker, Acunetix, etc.)
  - Use DNS and domain registrar companies your organization use
  - Commercial solutions
  - Automation frequency
  - Intelligence automation for finding Δ
  - Utilize threat intelligence solutions from your organization


Organizational Leadership
Board
Organizational & Risk Oversight
Management
Business Model and Vision
Organizational Risk Appetite
Information Risk Management
Refresh standards regularly with changes to threat environment, technology, regulations, business model, and more
Policy & Standards
Authoring and Approval
Enable Productivity
Protect Mission
Supply Chain Risk
(People, Process, Technology)
Posture Management
Monitor & Remediate Risk
(Conditional Access, Secure Score, Sharing Risks, Threat and Vulnerability Management (TVM) User & Asset Scores, etc.)
Technical Risk Management
Privacy & Compliance Requirements
Compliance Reporting
Technical Policy Monitoring
Compliance Management
Requirements Translation
Architecture & Risk Assessments
Technical Policy Authoring
Security Architecture
People
User Education & Awareness
Insider Risk
Apps & Data
Dev Education & Awareness
App Security Programs
Infrastructure & Endpoint
Infrastructure & Network Security
Endpoint Security
Deploy Tools
Vulnerability Management
Identity & Keys
Key Management
Administrator Security
Identity System Security
App Teams
IT Operations
Identity Teams
Threat Intelligence
Strategic Threat Insight/Trends
Tactical Threat Insight/Trends
Risk Scenarios
Incident Preparation
Practice Exercises
Security Operations [Center] (SOC)
Incident Response
Incident Management
Threat Hunting
Governance
Operations
Critical Partner Team

HOW CONT.

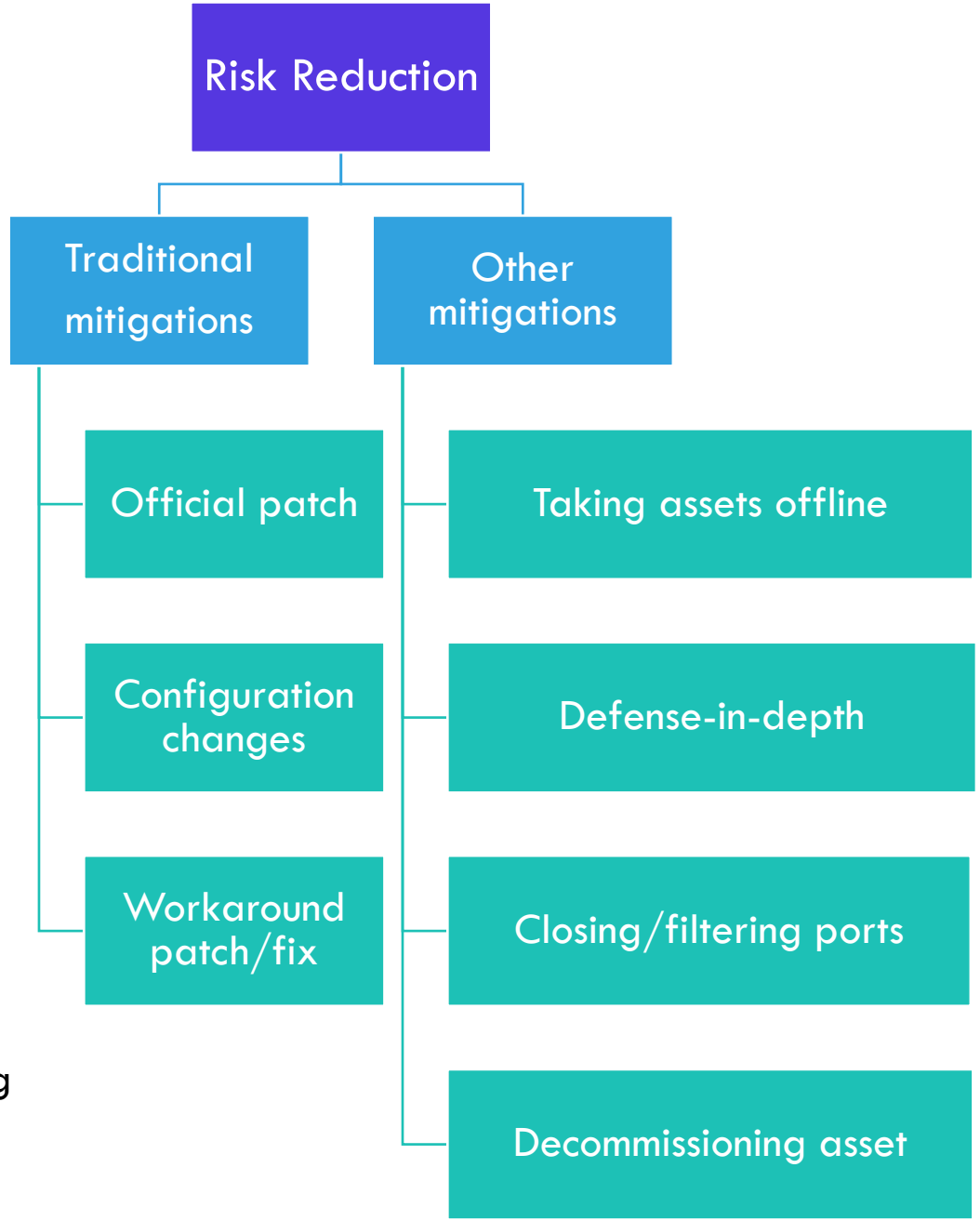
- Four simple steps:
  1. Find Unknown Assets
  2. **Assess Risks** →

- **How to assess risk**
  - Questions to ask yourself:
    - How would you see this asset from an attacker's viewpoint? (Point of interest or not?)
    - What critical data it could store or connect to in the backend?
    - Does it need to be on the Internet?
    - Is this colleague facing application or public facing application?



HOW CONT.

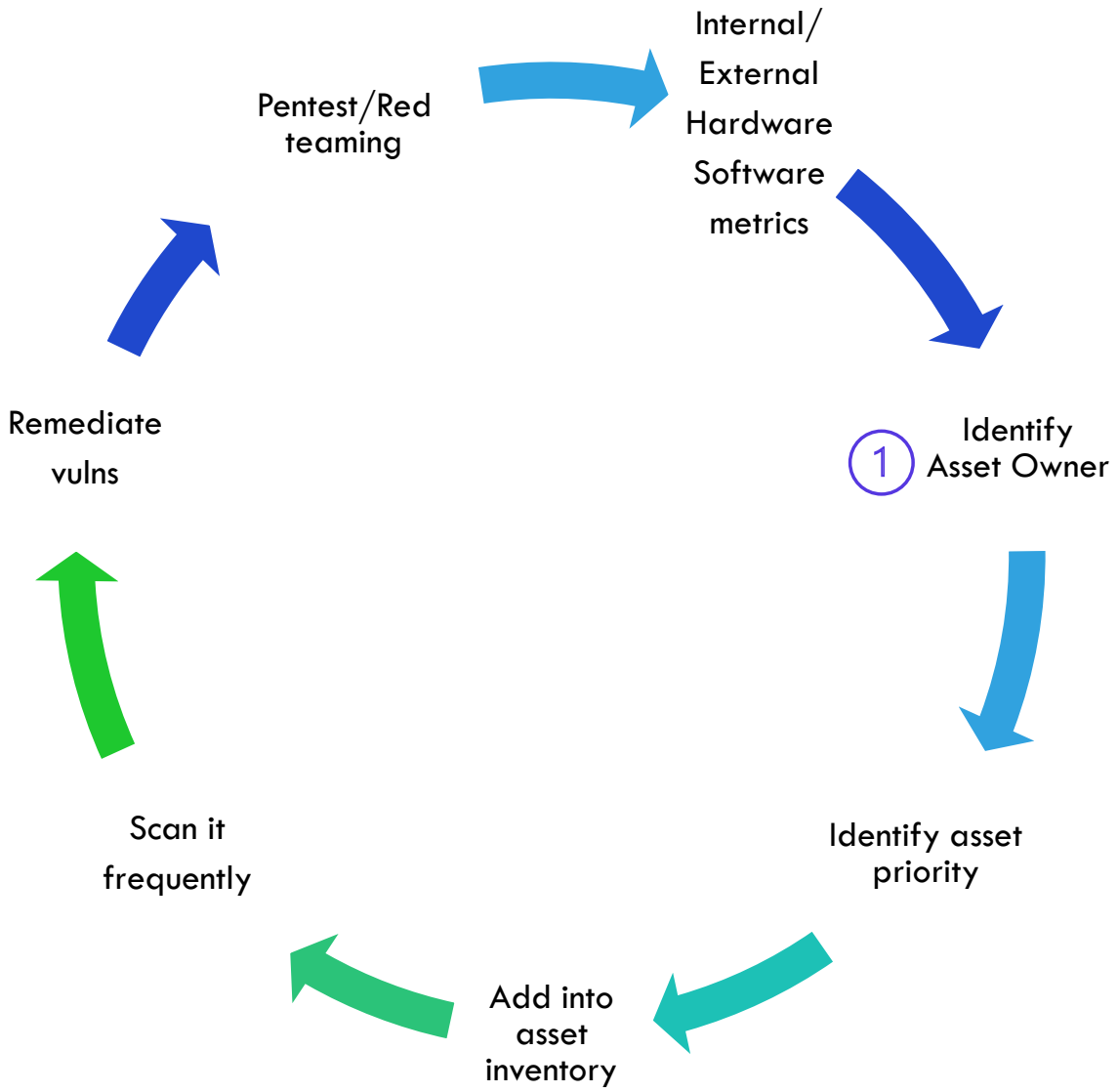
- Four simple steps:
  1. Find Unknown Assets
  2. Assess Risks
  3. **Reduce Risks**
- **How to assess risk**
  - Questions to ask yourself:
    - Does this port need to be on the Internet?
    - Does this asset need to be on the Internet?
    - Should I close/filter port or update software package installed on it? Both? Priority?
    - Can fix be pushed from central management for all assets?
    - Root cause analysis – Talk to Central Team for defining policies and standards for common bad practicies



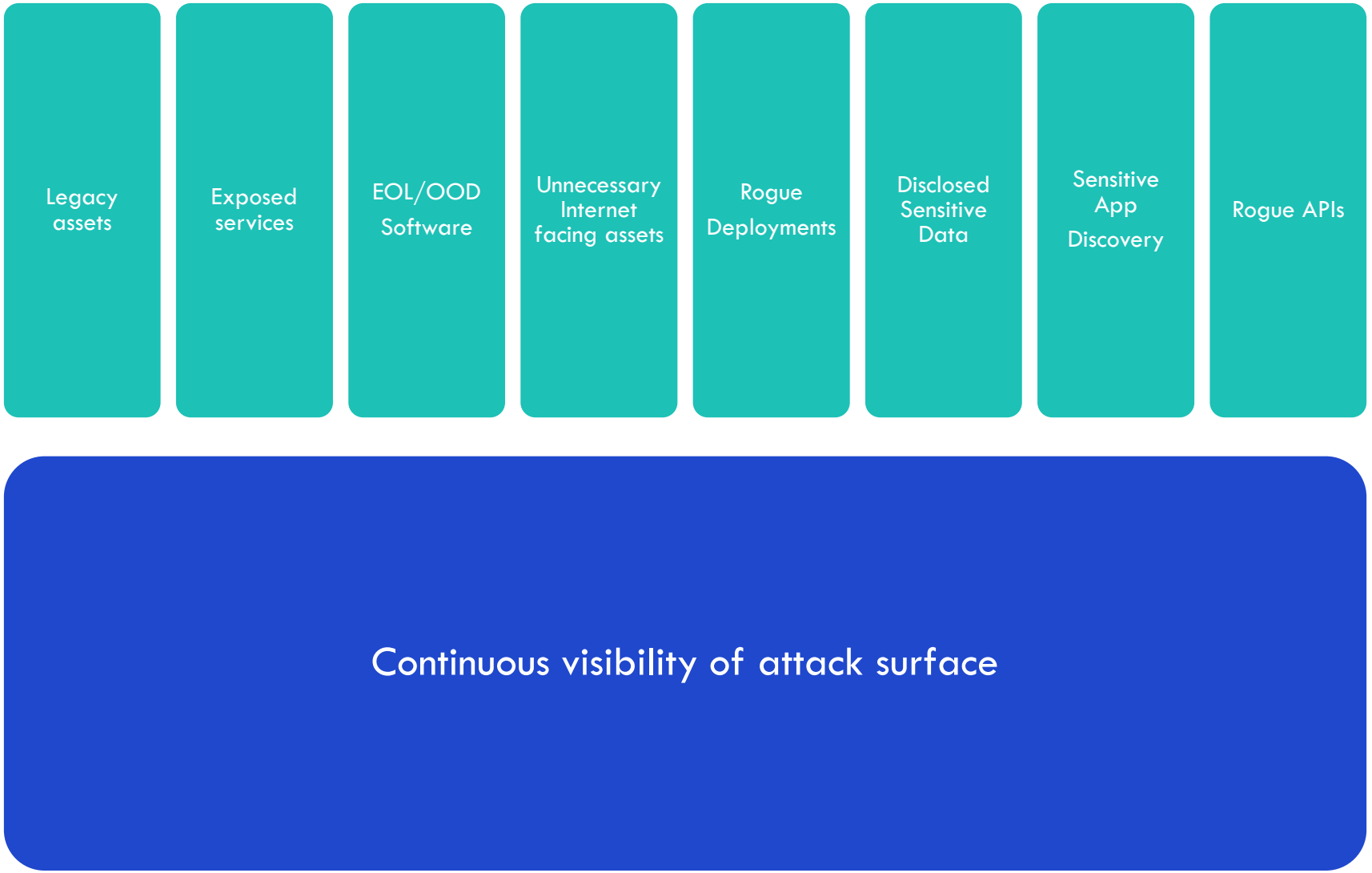
HOW CONT.

- Four simple steps:
  1. Find Unknown Assets
  2. Assess Risks
  3. Reduce Risks
  4. **Manage in future**

- **How to manage newly found unknown asset in future:**
  - Define asset priority with data classification methodology
  - Add into asset inventory with all the details
  - Schedule scan using standard scanners (Auth-Non auth, scan profile, scan frequency, things to be ignored, etc.)
  - Remediate issues (multiple ways)



BENEFITS


Legacy assets
Exposed services
EOL/OOD Software
Unnecessary Internet facing assets
Rogue Deployments
Disclosed Sensitive Data
Sensitive App Discovery
Rogue APIs
Continuous visibility of attack surface

THANK YOU & QUESTIONS?