Organizing for Resilient Operational Response




Jerry Cochran, CISSP, CISM
Director
jerry.cochran@microsoft.com

Microsoft
Global Security Strategy and Diplomacy
Trustworthy Computing

Security Ecosystem Trends

Horizontal Integration

Microsoft

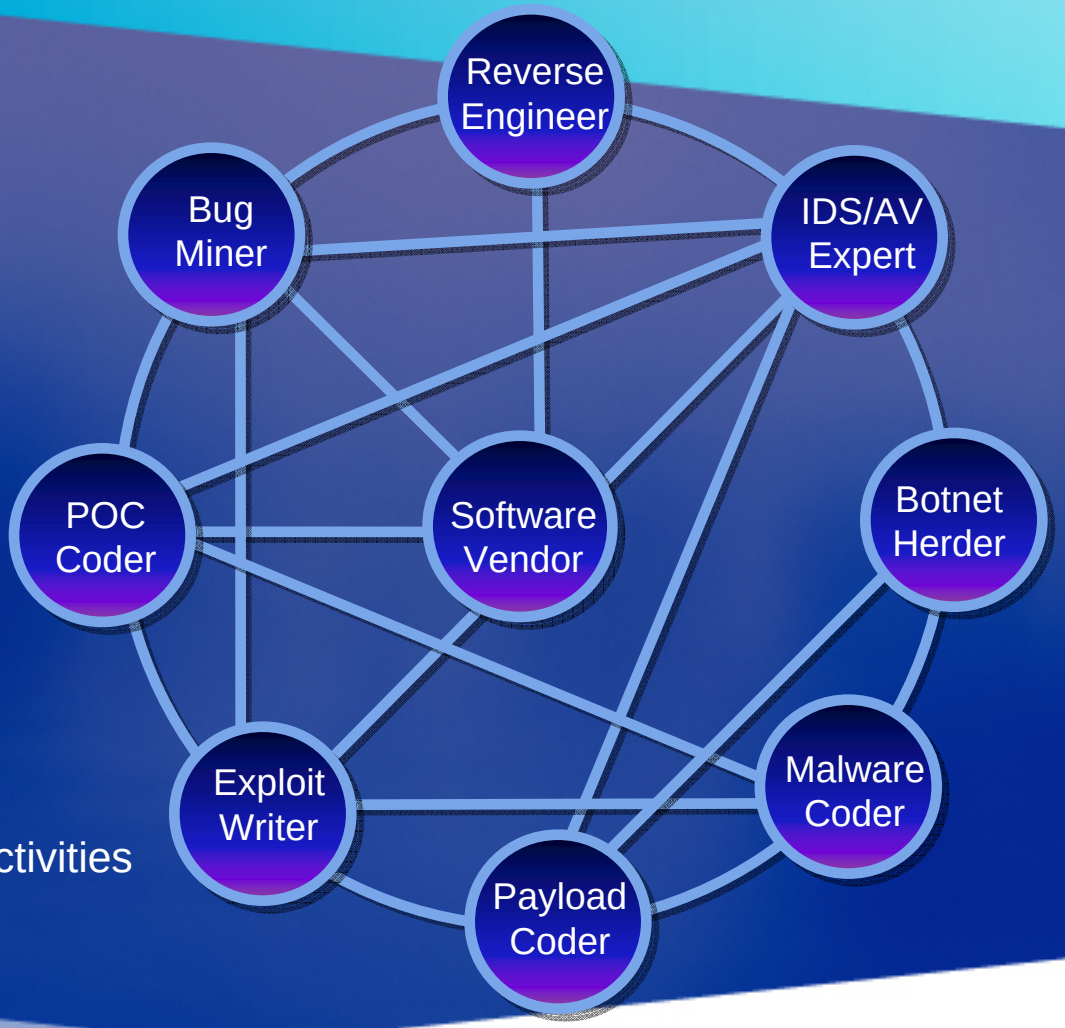
Global Security Strategy and Diplomacy
Trustworthy Computing

Security Response Interactions

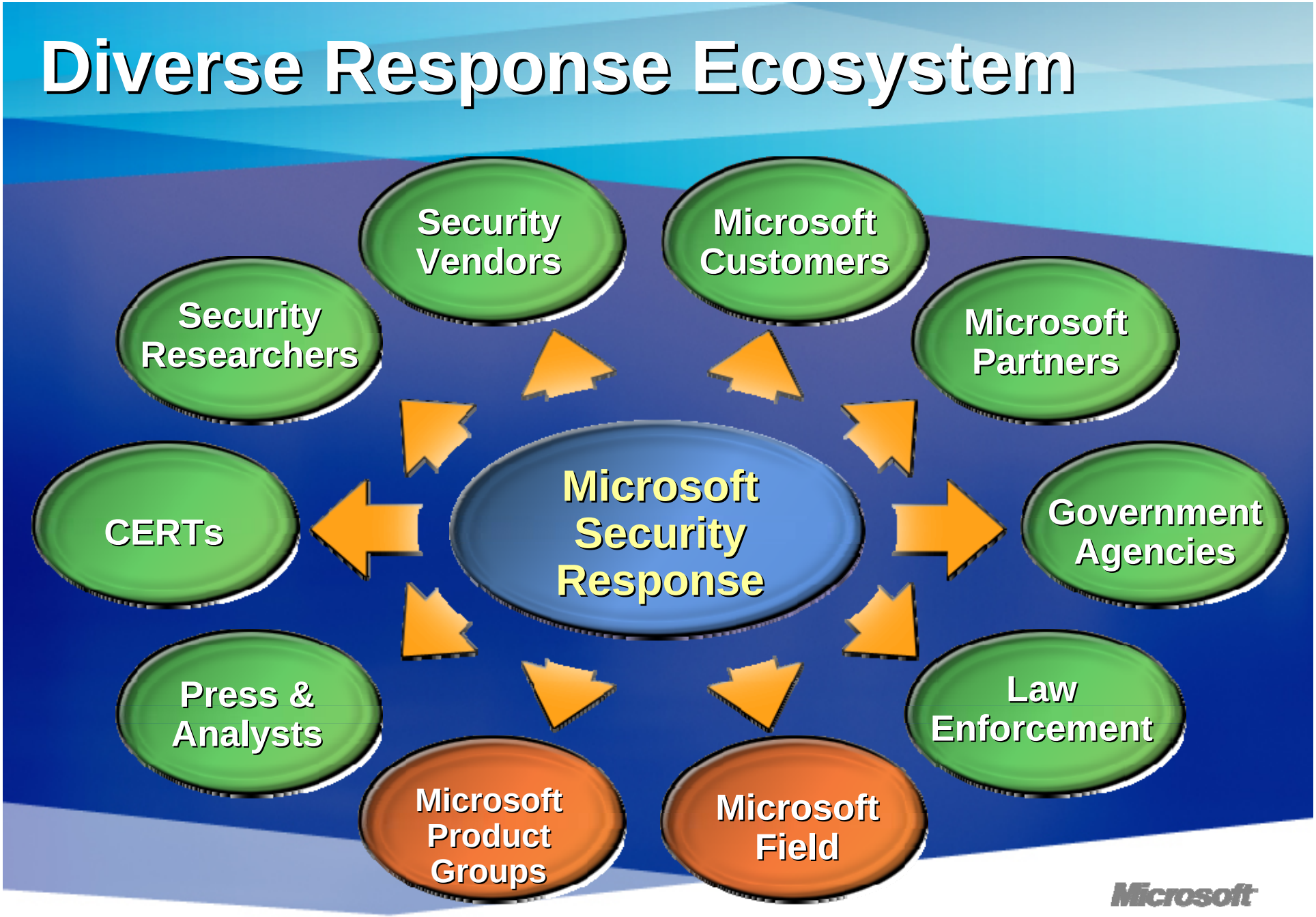
Actors
- Understand decision making process
- Engage all segments
- Follow the “herds”

Technology
- Identify attack & research trends
- Extinguish classes of issues

Economics
- Promote legitimate business models
- Change the Equation:
  - ✓Increase the cost of malicious activities
  - ✓Reduce malicious actor ROI



Diverse Response Ecosystem



Microsoft

Global Security Strategy and Diplomacy
Trustworthy Computing

Responding to a Security Incident

Microsoft Software Security Incident Response Plan

Watch

- Observe environment to detect any potential issues
- Leverage existing relationships with:
  - Partners
  - Security researchers and finders
- Monitor customer requests and press inquiries

Alert and Mobilize

- Convene and evaluate severity
- Mobilize security response teams and support groups into two main groups:
  - Emergency Engineering Team
  - Emergency Communications Team
- Start monitoring WW press interest and customer support lines for this issue

Assess and Stabilize

- Assess the situation and the technical information available
- Start working on solution
- Communicate initial guidance and workarounds to customers, partners and press
- Notify and inform Microsoft sales and support field

Resolve

- Provide information and tools to restore normal operations
- Appropriate solution is provided to customers, such as a security update, tool or fix
- Conduct internal process reviews and gather lessons learned

Microsoft
Global Security Strategy and Diplomacy
Trustworthy Computing

Microsoft Response Program Areas

Community-based defense – Microsoft Active Protection Program

Rapid response communications – SCPCert

Defensive security knowledge – Exploitability Index

Isolate malicious software – MS Vulnerability Research

Support of worldwide law enforcement and legislatures

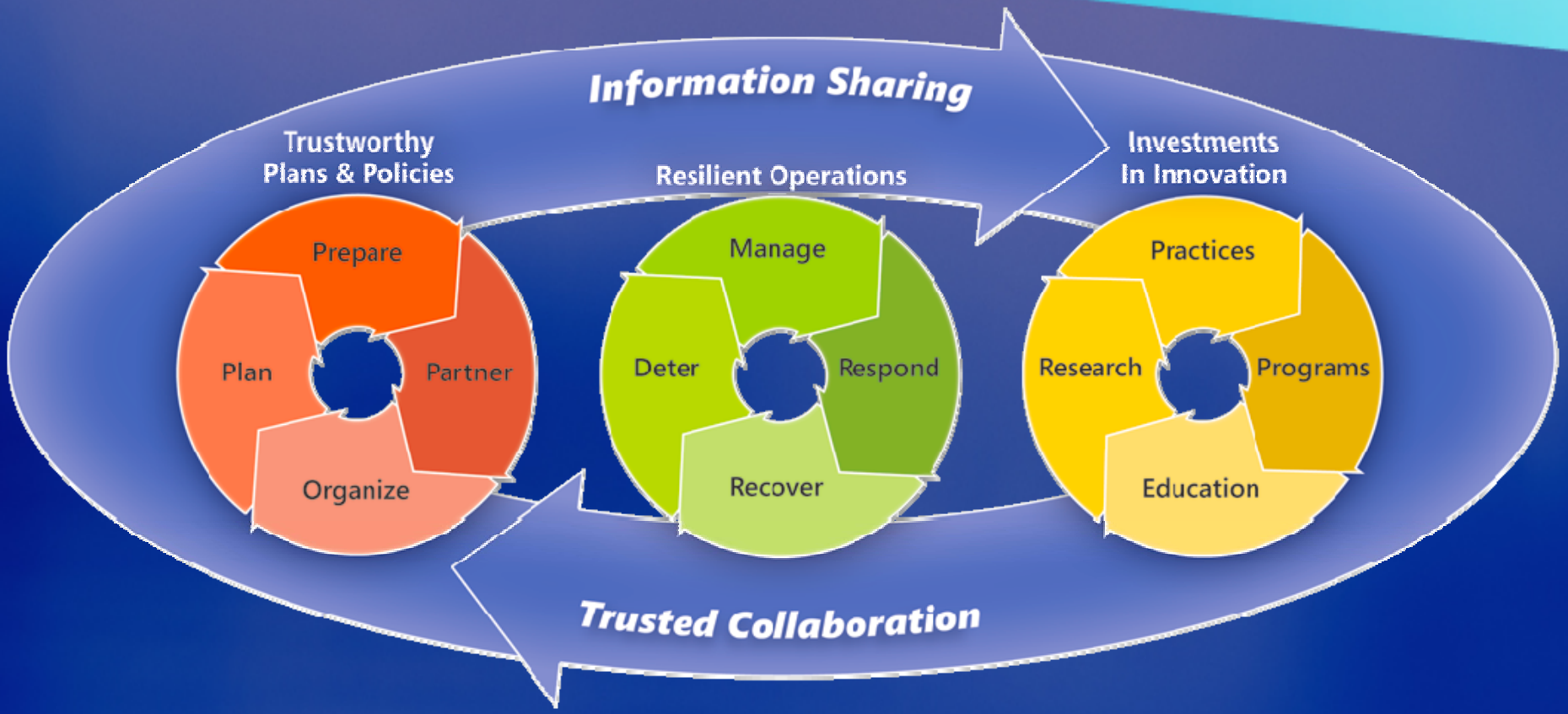
Coordinating Multi-vendor response

- ***International Consortium for Advancement of Security on the Internet (ICASI)***
  - Drive excellence and innovation in security response practices; and
  - Enable ICASI collaboration to proactively analyze, mitigate, and resolve multi-vendor, global security challenges
- Five Industry Members: Cisco, IBM, Intel, Juniper, Microsoft
- Operational Response Coordination
  - *Unified Security Incident Response Plan*

www.icasi.org

Microsoft
Global Security Strategy and Diplomacy
Trustworthy Computing

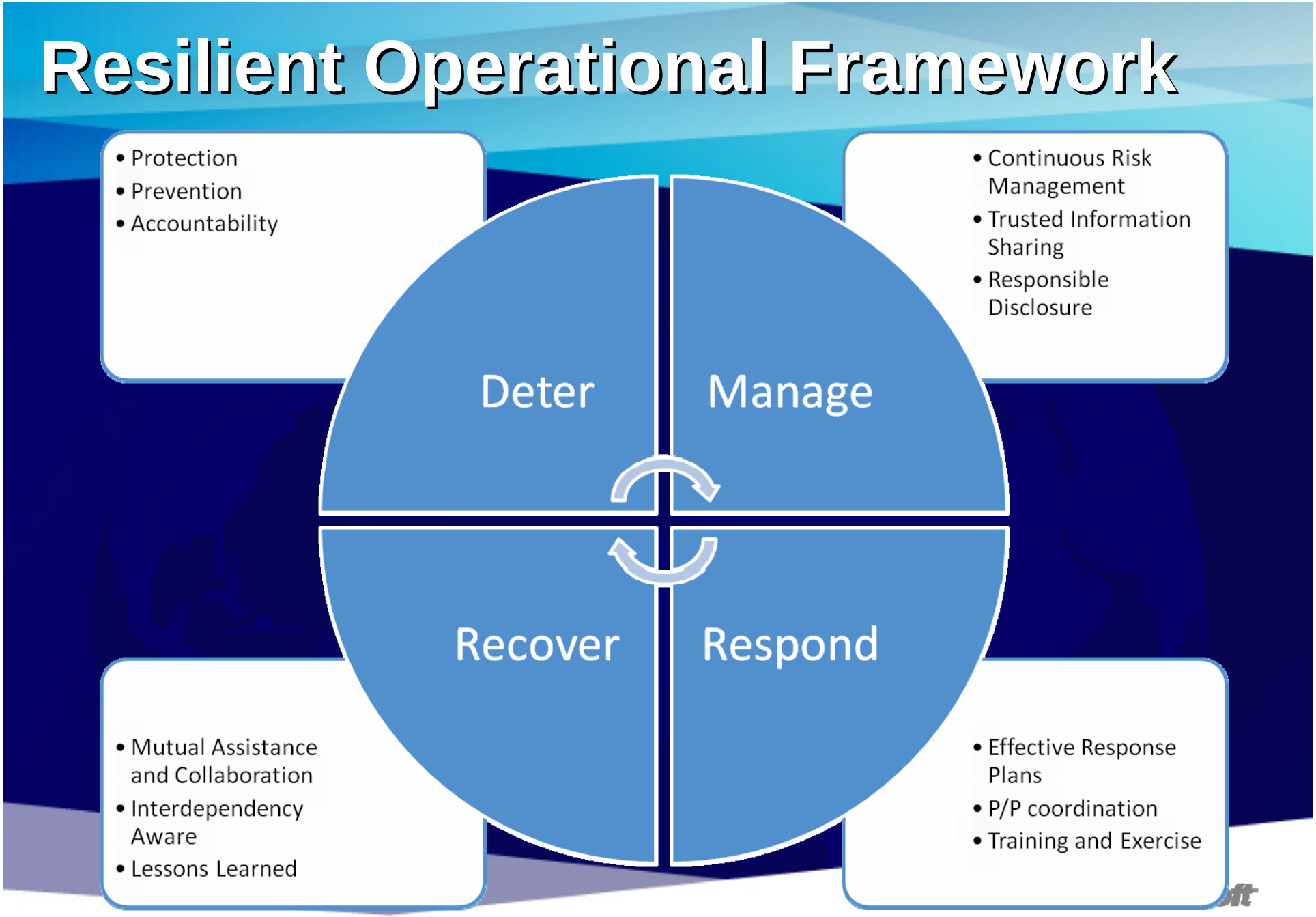
A Security and Resiliency Continuum



Microsoft

Global Security Strategy and Diplomacy
Trustworthy Computing

Resilient Operational Framework



Microsoft®

Your potential. Our passion.™

Microsoft

Global Security Strategy and Diplomacy
Trustworthy Computing