Xceptional

Linkedin Live Expert QA Session

December 7, 11:00am PST

CMMC 2.0 Update Panel Discussion

Xceptional.com

cisco
Partner

Session Structure

- **Guest Introductions**
- **CMMC Background**
- **Recent CMMC 2.0 Announcement**
- **Pros-Cons of CMMC 2.0**
- **Navigating the CMMC 2.0 Waters**
- **Key Takeaways & Wrap Up**

Introductions

Host / Mark Dallmeier:

Industry Veteran, Researcher, CSO/CMO for Various Cyber & Risk Firms, MSSPs, and MSPs.

Expert / Edward Vasko:

Industry Veteran, Director of The Institute for Pervasive Cybersecurity, Boise State University

Expert / Don Maclean:

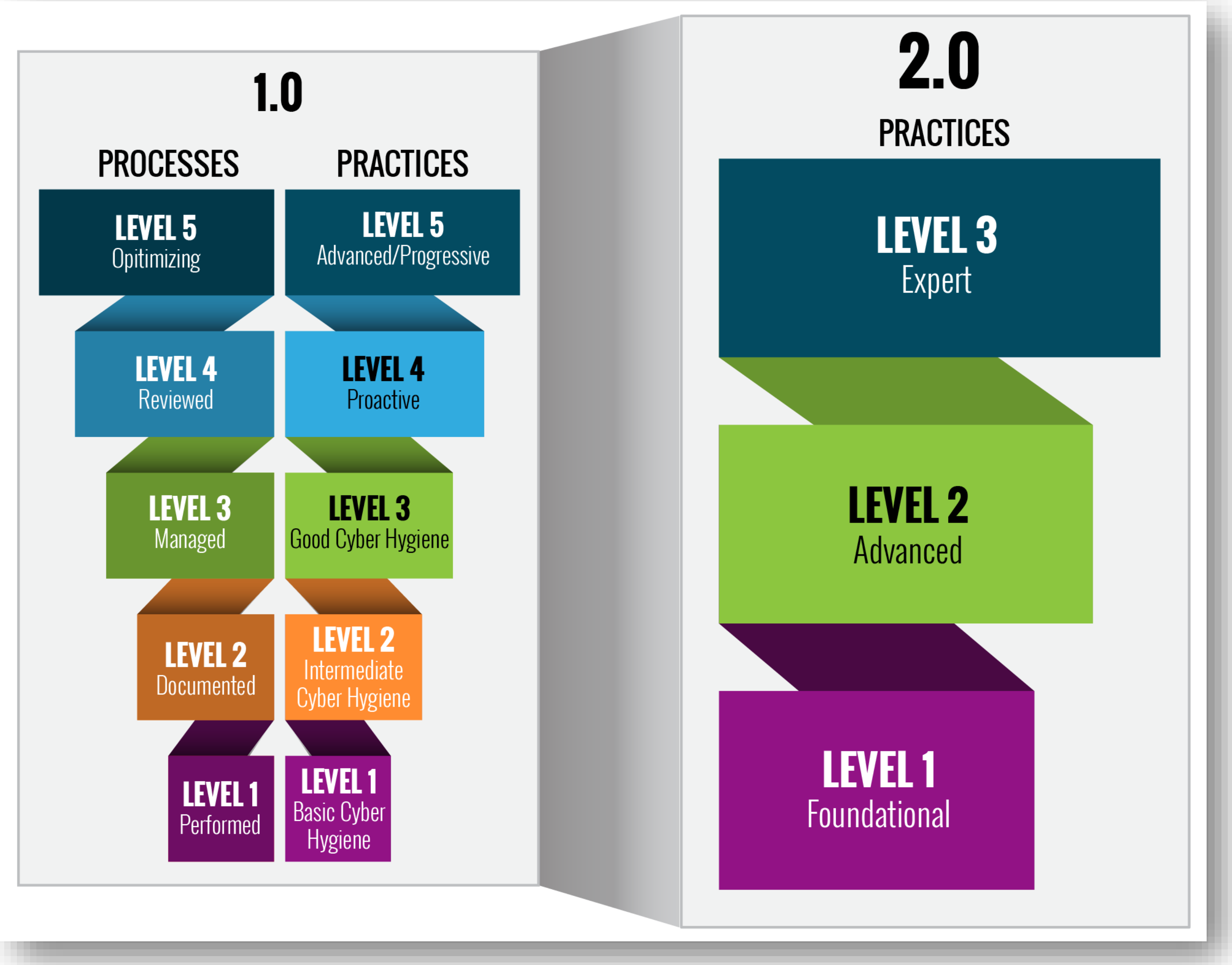
Industry Veteran, Researcher, Chief Cybersecurity Technologist, DLT

CMMC Background: Why This Matters

- **The Defense Industrial Base (DIB) is the target of increasingly frequent and complex cyberattacks.** *Research studies estimated that there are Trillions of dollars worth of sensitive data and intelligence being stolen out of the DoD supply chain.*
- **This stolen intelligence was being leveraged by enemies of the U.S. (to accelerate weapon development)** *and / or was being utilized for espionage and other attacks against U.S. agencies, and businesses.*
- **To protect American ingenuity and national security information, the DoD developed the Cybersecurity Maturity Model Certification (CMMC) to enhance DIB cybersecurity** *to meet evolving threats and safeguard the information that supports and enables our warfighters.*
- **The CMMC model is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)** *that is shared with contractors and subcontractors of the DoD.*
- **In September 2020, the Department published an interim rule to DFARS in the Federal Register (DFARS Case 2019-D041).** *Now known as CMMC 1.0.*
- **In November 2021, the Department announced CMMC 2.0 –** *an updated program and structure.*
- **The Department intends to pursue rulemaking** *in Part 32 of the Code of Federal Regulations (C.F.R.) and within the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R.*

> **"If you are unable to comply with new mandatory requirements," says one of the memos, "GE Aviation will be unable to continue to do business with your company."**
>
> *Regarding the DoD interim rule in November for Documenting Assessment actions around NIST 800-171 as a foundation for CMMC*

CMMC 1.0 / 2.0 Differences

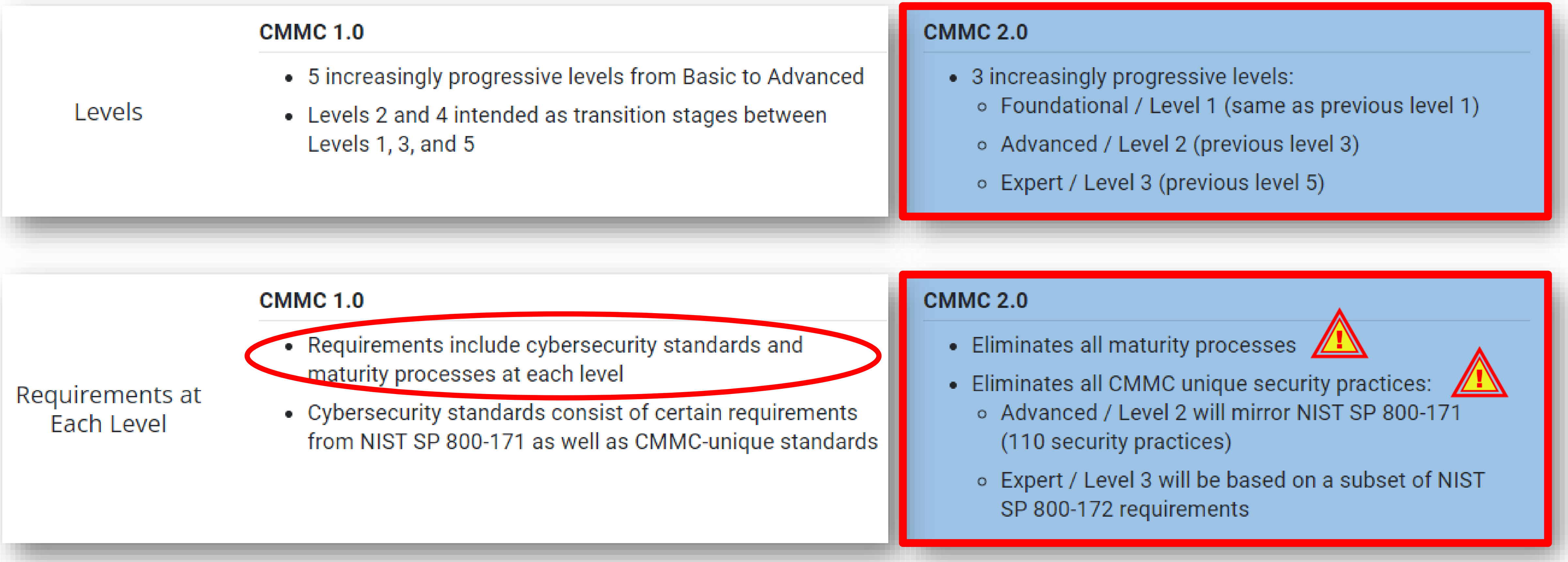


What We Understood:

- CMMC is DoD Business Focused (at the moment). Could expand.
- No Plan of Action & Milestones (POAMs).
- Can't leverage 3rd party's CMMC designation (No Piggybacking).
- Estimates from the Government are (low) for the assessment only.
- Some CMMC costs can be included within contracts; but many cannot.
- Compliance is complex and can be costly.
- This is a journey; there is no "end state".

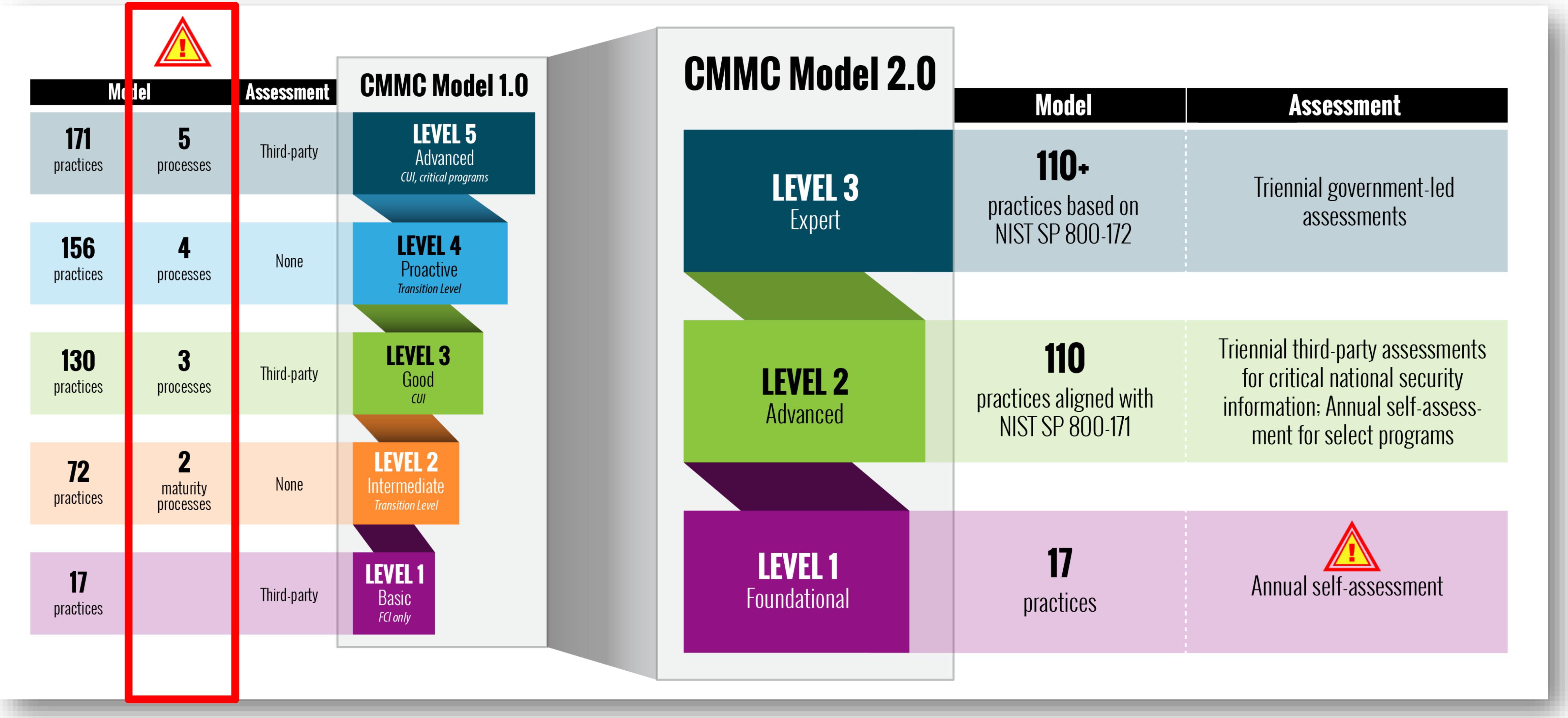
xceptional.com

CMMC 2.0 Announcement:



	CMMC 1.0	**CMMC 2.0**
Levels	• 5 increasingly progressive levels from Basic to Advanced • Levels 2 and 4 intended as transition stages between Levels 1, 3, and 5	• 3 increasingly progressive levels: ∘ Foundational / Level 1 (same as previous level 1) ∘ Advanced / Level 2 (previous level 3) ∘ Expert / Level 3 (previous level 5)
	CMMC 1.0	**CMMC 2.0**
Requirements at Each Level	• Requirements include cybersecurity standards and maturity processes at each level • Cybersecurity standards consist of certain requirements from NIST SP 800-171 as well as CMMC-unique standards	• Eliminates all maturity processes ⚠ • Eliminates all CMMC unique security practices: ⚠ ∘ Advanced / Level 2 will mirror NIST SP 800-171 (110 security practices) ∘ Expert / Level 3 will be based on a subset of NIST SP 800-172 requirements

CMMC 1.0 vs 2.0



Model	⚠	Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	⚠ Annual self-assessment

Panel Discussion & QA

Real World Situations, Feedback.

Opinions on the updated program structure.

Navigating the Waters.

Impact?

What has been the impact of CMMC on organizations within the DIB and other adjacent industries?

Progress?

Will 2.0 accelerate cyber hygiene and reduce leakage and theft of intelligence? What are the pros and cons of 2.0?

Moving Ahead?

How should organizations continue to defend and protect themselves and their systems while they wait for the final ruling? Any best practices for reducing cyber risks and attacks?

Key Takeaways & Wrap Up

Xceptional

Host / Mark Dallmeier:

Industry Veteran, Researcher, CSO/CMO for Various Cyber Risk, MSSPs, MSPs.

BOISE STATE UNIVERSITY

Expert / Edward Vasko:

Industry Veteran, Director of The Institute for Pervasive Cybersecurity, Boise State University

DLT®

A TECH DATA COMPANY

Expert / Don Maclean:

Industry Veteran, Researcher, Chief Cybersecurity Technologist, DLT

Comments, Key Takeaways: Ed, Don

Ed:

- If you've not assessed your environment, get started on Level 1 if you haven't already done so.
- Reach out to your regional Manufacturing Extension Partnership (MEP) provider for additional guidance.
- Be prepared for other changes and impacts as these changes are rippling through the DiB.

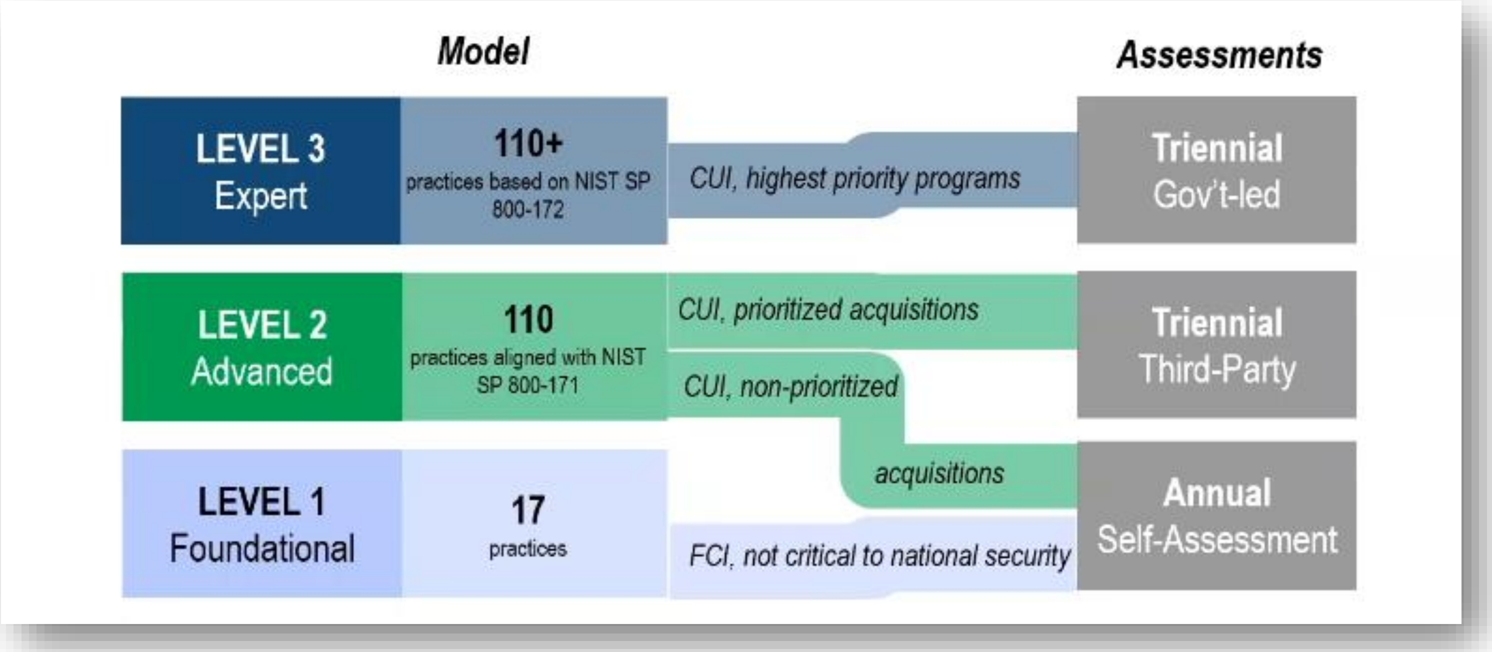
Don:

- Our enemies are still out there and will still attack you.
- FCI in isolation isn't sensitive but is useful in aggregation: bad actors will aggregate data from multiple sources to form a big picture.
- Good security is in your company's interest, with or without CMMC.
- If your company handles CUI, you will need Level 2 certification.
- Self-attestation does not mean you're "off the hook"; False Claims Act applies
- POA&Ms still not allowed for key controls.

Key Takeaways: Don Continued

Don:

- Level 3 assessments will be done by DoD, ~ but ~ companies need an L2 cert first; L3 assessment is only the L2-L3 delta.
- CMMC 1.0 training for CCPs is still valid; delta training to move to CMMC 2.0 will be provided.
- L2 is bifurcated based on acquisition priority (see graphic below, from November Town Hall).



Model

LEVEL 3 Expert

110+ practices based on NIST SP 800-172

CUI, highest priority programs

LEVEL 2 Advanced

110 practices aligned with NIST SP 800-171

CUI, prioritized acquisitions

CUI, non-prioritized acquisitions

LEVEL 1 Foundational

17 practices

FCI, not critical to national security

Assessments

Triennial Gov't-led

Triennial Third-Party

Annual Self-Assessment

Takeaways & Wrap Up: Mark

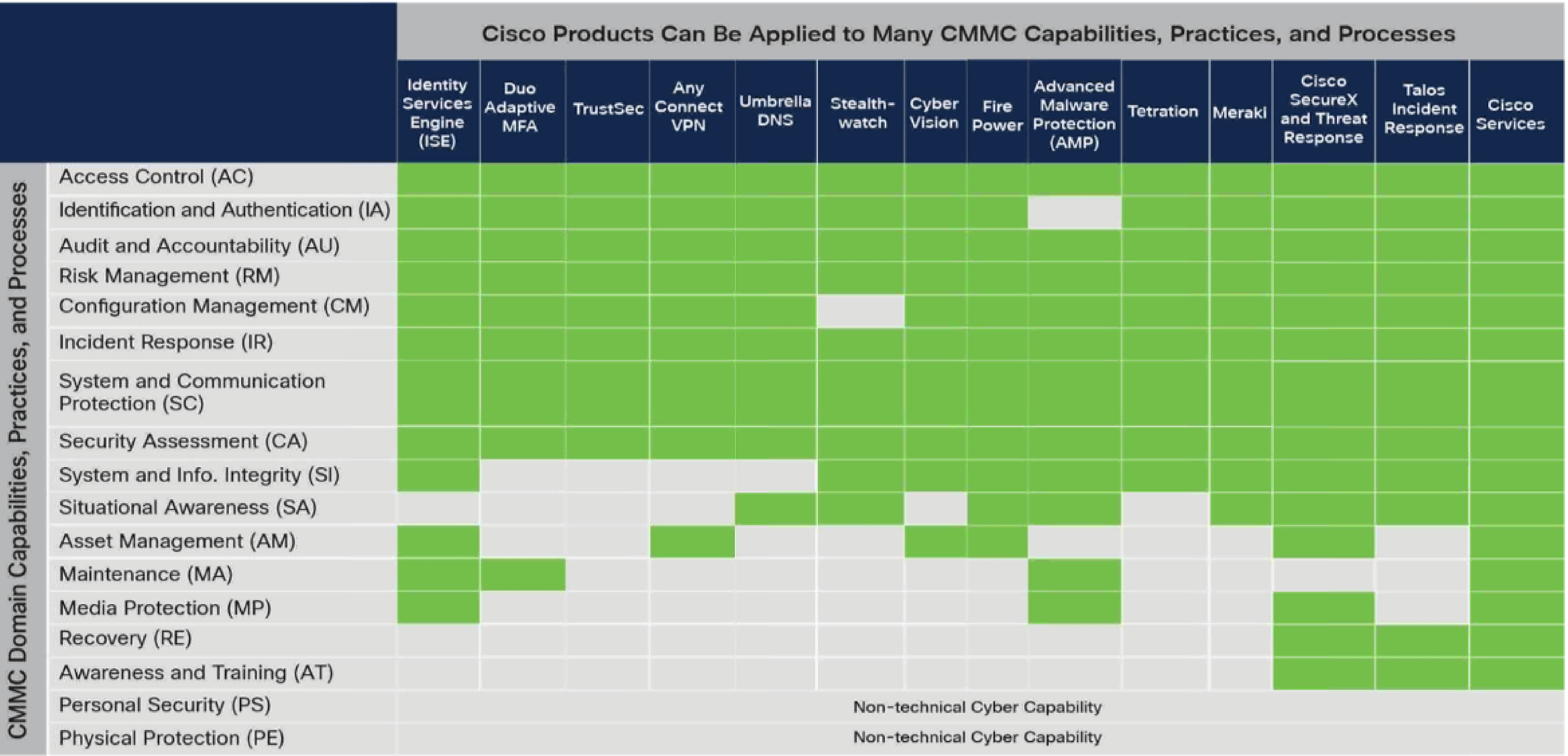
Mark:

- Do you know how much of the business and IT environment is in scope for CMMC?
- Do you know where the data is and who has access?
- Do you have a framework to build upon? (NIST CSF, NIST 800-171, NIST 800-53, etc)
- Are you leveraging 3rd parties, managed service providers, cloud providers, associations, industry partners, to gain insight into approaches?

Wrap Up, Other Considerations

- Technology Vendor Portfolio Mapping
- The 4 Ps
- Zero Trust
- Data Vaults

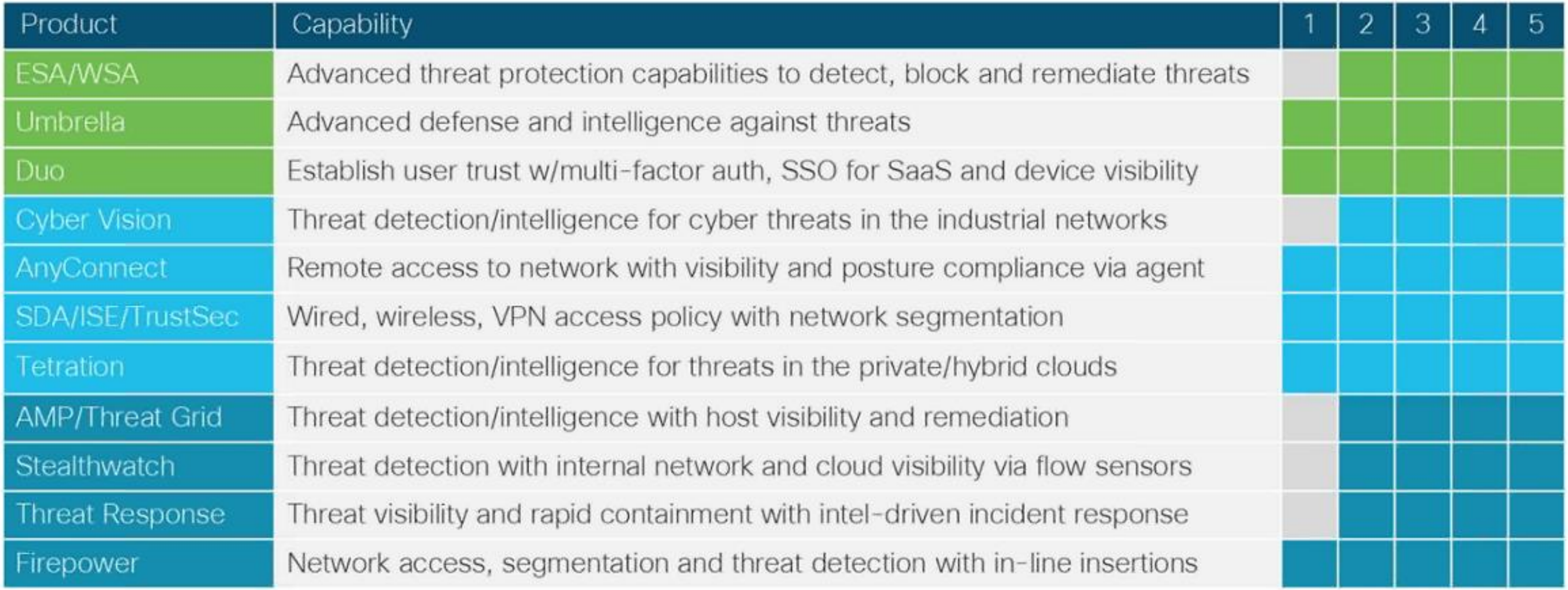
Cisco = Supporting CMMC



		Cisco Products Can Be Applied to Many CMMC Capabilities, Practices, and Processes													
		Identity Services Engine (ISE)	Duo Adaptive MFA	TrustSec	Any Connect VPN	Umbrella DNS	Stealth-watch	Cyber Vision	Fire Power	Advanced Malware Protection (AMP)	Tetration	Meraki	Cisco SecureX and Threat Response	Talos Incident Response	Cisco Services
CMMC Domain Capabilities, Practices, and Processes	Access Control (AC)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Identification and Authentication (IA)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩
	Audit and Accountability (AU)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Risk Management (RM)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Configuration Management (CM)	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Incident Response (IR)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	System and Communication Protection (SC)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Security Assessment (CA)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	System and Info. Integrity (SI)	🟩					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Situational Awareness (SA)					🟩	🟩		🟩	🟩		🟩	🟩	🟩	🟩
	Asset Management (AM)	🟩			🟩			🟩	🟩				🟩		🟩
	Maintenance (MA)	🟩	🟩							🟩					🟩
	Media Protection (MP)	🟩								🟩			🟩		🟩
	Recovery (RE)												🟩	🟩	🟩
	Awareness and Training (AT)												🟩	🟩	🟩
	Personal Security (PS)	Non-technical Cyber Capability													
	Physical Protection (PE)	Non-technical Cyber Capability													

Cisco Zero Trust Technology Portfolio

Enabling Basic to Advanced Cyber Hygiene (Supports industry regulations)



		Basic	Intermediate	Good	Proactive	Advanced
Product	Capability	1	2	3	4	5
ESA/WSA	Advanced threat protection capabilities to detect, block and remediate threats		🟩	🟩	🟩	🟩
Umbrella	Advanced defense and intelligence against threats	🟩	🟩	🟩	🟩	🟩
Duo	Establish user trust w/multi-factor auth, SSO for SaaS and device visibility	🟩	🟩	🟩	🟩	🟩
Cyber Vision	Threat detection/intelligence for cyber threats in the industrial networks		🟦	🟦	🟦	🟦
AnyConnect	Remote access to network with visibility and posture compliance via agent	🟦	🟦	🟦	🟦	🟦
SDA/ISE/TrustSec	Wired, wireless, VPN access policy with network segmentation	🟦	🟦	🟦	🟦	🟦
Tetration	Threat detection/intelligence for threats in the private/hybrid clouds	🟦	🟦	🟦	🟦	🟦
AMP/Threat Grid	Threat detection/intelligence with host visibility and remediation		🟦	🟦	🟦	🟦
Stealthwatch	Threat detection with internal network and cloud visibility via flow sensors		🟦	🟦	🟦	🟦
Threat Response	Threat visibility and rapid containment with intel-driven incident response		🟦	🟦	🟦	🟦
Firepower	Network access, segmentation and threat detection with in-line insertions	🟦	🟦	🟦	🟦	🟦

QA, Wrap Up & Next Steps

- **QA**
- **Offer: Complimentary Security Assessment**
  - Network vulnerability scan
  - Technology review and evaluation
  - Controls review
  - Summary and recommendations report

info@xceptional.com

Xceptional

Linkedin Live Expert QA Session

December 16, 11:00am PST

Planning for Zero Trust in 2022

Register Today!

Access more panels, webinars & research:

https://resources.xceptional.com/webinars

Xceptional.com

cisco Partner

Xceptional

CISCO Partner

Thank You!

xceptional.com | 858-225-6230