CMMC Preparedness: RPO vs DIY

5 Reasons To Use A CMMC-RPO

KTL SOLUTIONS

June 3, 2021

Housekeeping

- Feel free to ask questions in the chat box. We will answer as many as we can during the Q&A session at the end of the webinar.
- If we don’t get to your questions today, a KTL consultant will reach out to you.
- This webinar is being recorded. You will be sent a link to the recording after the webinar, as well as a PDF copy of the deck.

Meet the Speakers

Stephen Reid
Director of Sales and Marketing,
KTL Solutions

John Mulhall, CMMC-RP
President of Divergent Solutions Group and Security & Compliance Consultant, KTL Solutions

David Bedard, CMMC-RP
Senior Account Manager, Aerospace & Defense,
KTL Solutions

Disha Patel, CMMC-RP
Account Manager, Aerospace & Defense,
KTL Solutions

Agenda

- Introducing KTL Solutions
- CMMC News and Updates
- What is a CMMC-RPO?
- 5 Reasons to Use a CMMC-RPO
- Azure Marketplace Offerings
- Business Applications
- Q&A

KTL Solutions

- IT consulting firm serving clients for over 20 years
- Certified Microsoft Gold Partner
- Provide licensing, Azure Government, and Dynamics Services
- **One of the first CMMC Registered Provider Organizations (CMMC-RPO)**
- One of the first partners selected for the Agreement for Online Services for Government (AOS-G) in 2017
- Specialize in assisting government contractors
- Offer a suite of products and services

CMMC News & Updates

- CMMC-AB: Updated FAQs May 26

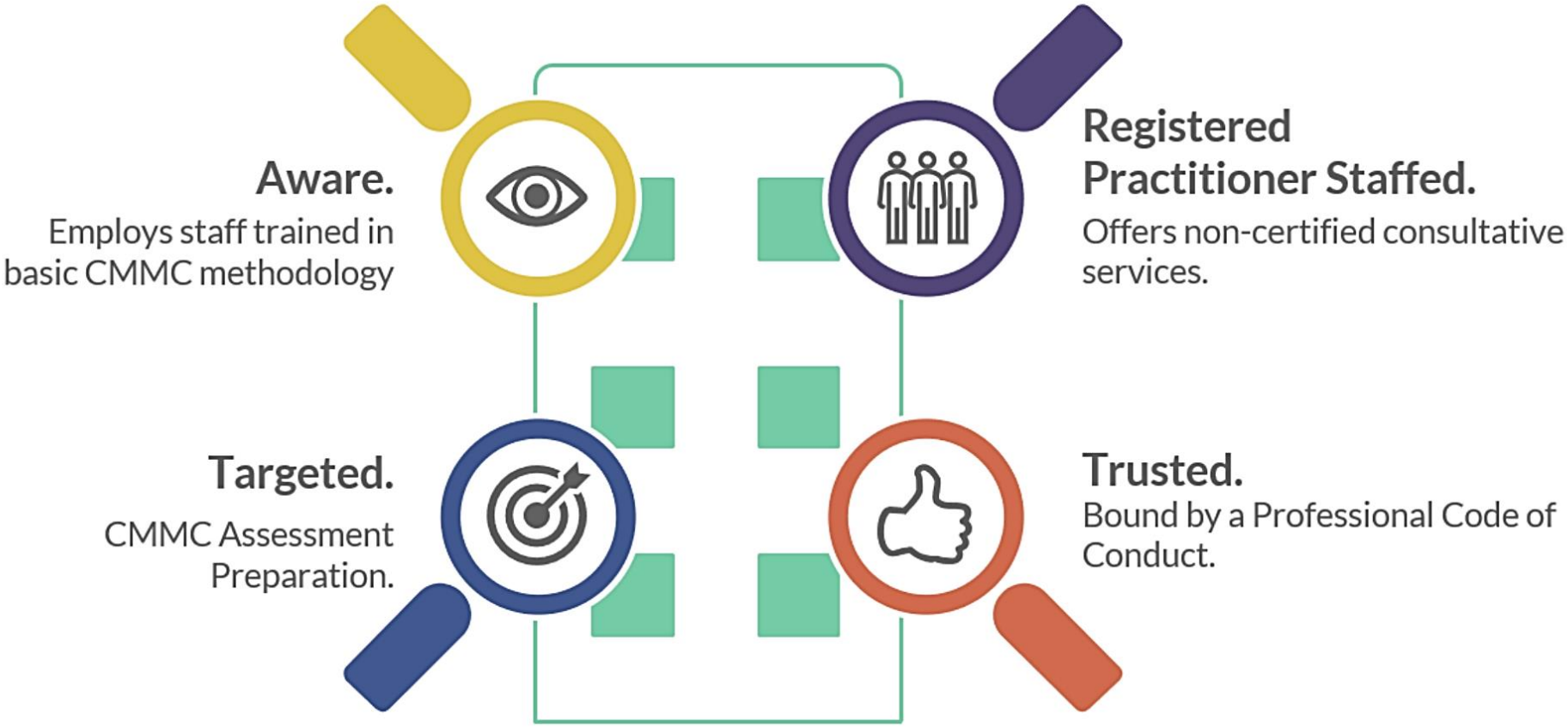
- **Jesse Salazar**, Deputy Assistant Secretary of Defense for Industrial Policy
  - May 17 testimony before the **Senate Armed Services Committee**
    - Focused on DIB
    - Discussed “Predatory” cyber criminals
    - Named 3 Objectives of the CMMC
    - Written Testimony
    - Video of Proceedings

CMMC
ACCREDITATION BODY
Cybersecurity Maturity Model Certification

KTL SOLUTIONS

What is a CMMC-RPO/RP?

The RPOs and RPs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients. They are the “implementers” and consultants, but do not conduct Certified CMMC Assessments.



5 Reasons To Use A CMMC-RPO

If you're in the DoD supply chain, you know CMMC requirements are on the way. A CMMC RPO employs CMMC RPs (Registered Practitioners) who will interpret CMMC guidelines and help you chart a course to CMMC compliance.

CMMC-RP Specialized Skills

1. Interpreting CMMC Requirements
2. Scoping the Extent of Compliance
3. Performing a Gap Analysis
4. Creating a Remediation Plan
5. Preparing Evidence of Security Control Implementation

KTL SOLUTIONS

1. Interpret CMMC Requirements

- Level 1 compliance seems simple because you don't have to document your adherence to any standards, but many companies will ultimately need to certify at Level 3. At that Level you need security controls in place along with documentation that includes tangible evidence.
- The official CMMC assessment guidelines for Level 3 are hundreds of pages long including 130 separate practices and processes requiring attention. Roughly half of these are technical and half cover data access policies.
- **A Registered Practitioner (RP) is trained to translate CMMC standards into security controls, saving your team time and frustration by providing guidance and recommendations.**

2. Scope the Extent of Compliance

- Step one in CMMC compliance is to determine your system boundary, exactly what data you need to protect and where it's stored on your network.
- By defining your system boundary first, you can determine which section of your network can be segmented out so that CMMC will only be applied to the network segment that is in scope.
- **An RP can help determine how this data flows through your organization and will provide recommendations for segmenting your network and modifying processes in order to isolate DoD data.**
- Focusing the scope of CMMC standards will also help you save on assessment costs at audit time.

3. Perform a Gap Analysis

- After you've identified which data requires protection and where it's stored, you need to take stock of what security practices are already in place that can be applied to compliance, and where you fall short. A Registered Practitioner can do a Gap Analysis to reveal that information.
- **An RP will review the CMMC controls one by one for yes or no confirmation.**
  - **If the answer is YES, the RP will then look to see if you have evidence for the control.**
  - **Any NO answers will go to a list for remediation.**
- It is critically important to get a Gap Analysis done as soon as you know that CMMC compliance is required because it will give you a clear picture of your readiness for an audit. Depending on your situation, you may need to invest in hardware or software, as well as get ongoing management tasks in place. You also need time to train your team to follow your non-technical policies.
- You must also demonstrate that compliance has been in place for a period of time.

Example: Controls for Updating Threat Profiles/Adversary Tactics, Techniques, Procedures, Maturity Level 4.

Cybersecurity Maturity Model Certification (CMMC)

cybersecuritysoc

Edit

Saving as private workbooks is going away in early 2021. You will be able to access/edit your existing private workbooks but new workboooks will be saved as Shared workbooks →

RM.4.149

Requirement

- Update Threat Profiles/Adversary Tactics, Techniques, Procedures (ML-4)

CMMC Guidance

This practice enables organizations to proactively increase their ability to include the adversary perspective in their cybersecurity planning and incident response. Organizations should know that setting up a security perimeter around their enterprise is no longer enough to keep that enterprise protected against the adversaries of today. Understanding the adversaries TTPs, and documenting how these techniques could be used against an organization is one of the first steps needed in order to keep the adversaries at bay. If an adversary gains access to an organization's enterprise, knowledge of their actions, what their standard operating procedures are, and what they may be going after can be a key part in eradicating them from your enterprise. See practice IR.4.100 for use of this information.

Microsoft Recommendation

Catalog Threat TTPs in the MITRE ATT&CK Framework with Azure Sentinel Hunting

Required Log (Log Source)

- SentinelGithub (Azure Sentinel) Get Azure Sentinel

Navigate

Azure Sentinel > Hunting

Microsoft Reference

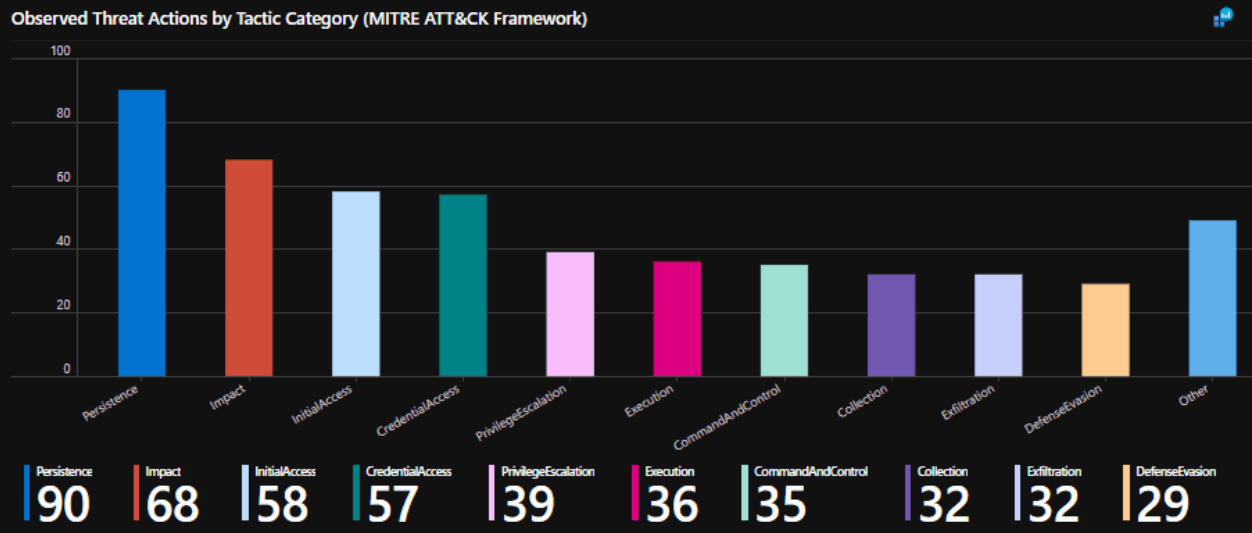
- Threat Hunting: Why Your SOC Needs a Proactive Hunting Team

CMMC Model

- CMMC Model

CMMC Control References

- CMMC
- NIST CSF v1.1 DE.AE-2
- CERT RMM v1.2 VAR:SG2.SP1



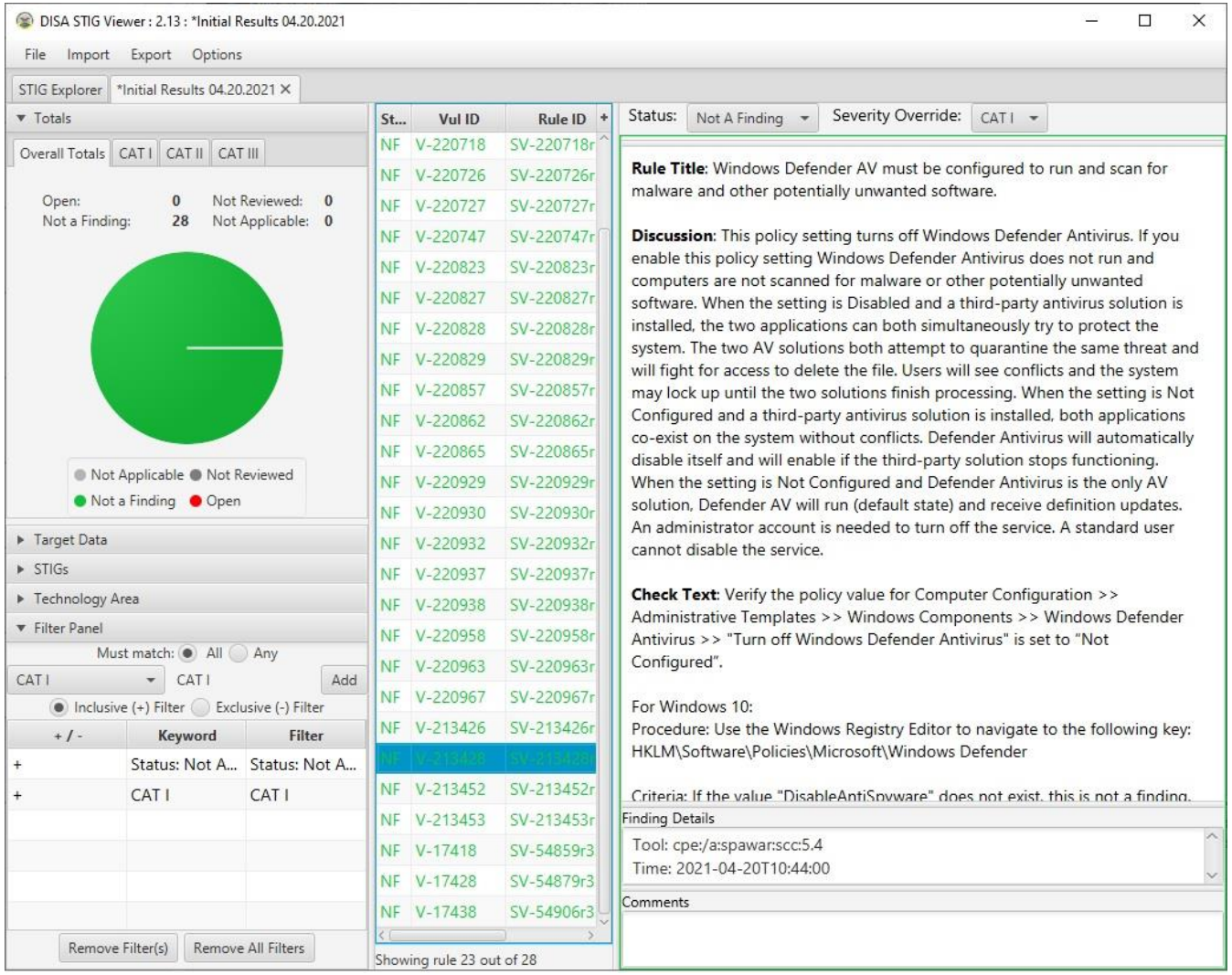
4. Create a Remediation Plan

- Once your Gap Analysis is complete, you end up with a list of controls that need to be implemented. These aren't always clear cut. If you need additional technical measures, a Registered Practitioner (RP) can help you identify the technologies that will be compatible with your IT environment.
- When it comes to policies and procedures, many companies turn to purchasing ready made policy and procedure packages.
- **An RP can assist in determining if it would be easier to build or buy and customize a package.**
- Compliance isn't just about passing an audit, but also about setting up processes and practices to provide ongoing security. The list of recommendations provided by an RP will be made with long-term management in mind.

5. Prepare Evidence of Security Control Implementation

- Preparing for a CMMC audit means that you not only have to have the controls in place, but you must also verify them.
  - Level 2 requires documentation for your security controls.
  - Level 3 requires documentation, plus two pieces of objective evidence for each control.
- **An RP can help you identify and organize appropriate evidence so they are easily accessible during your audit.**

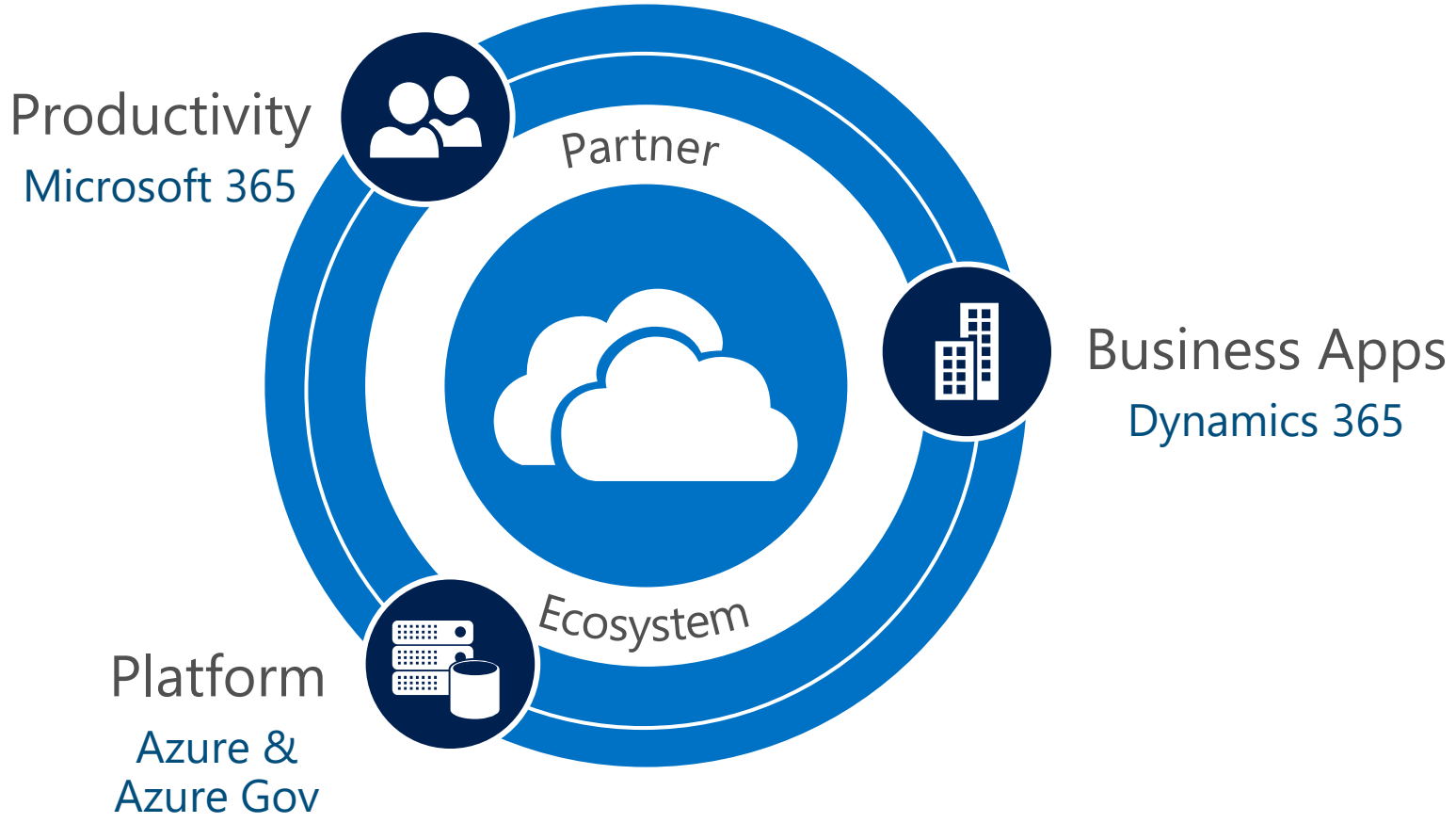
Example: Evidence of Security Control Implementation



Microsoft Azure Marketplace

KTL Solutions CMMC Consulting Offers

Microsoft Cloud for Business



Dynamics 365 Intelligent business applications in the cloud

Microsoft AppSource

Office 365

Project Service Automation

Sales

Customer Service

Microsoft Dynamics 365

Field Service

Marketing

Finance

Power BI

Cortana Intelligence Suite

Azure IoT Suite

Common application platform: PowerApps, Microsoft Flow, Common Data Model

KTL SOLUTIONS

Dynamics 365 Customer Engagement Apps

- Available in all 3 clouds (Commercial, GCC & GCC-H)
- End to End Customer Engagement Applications
  - Sales
  - Customer Service
  - Field Service
  - Marketing Automation Solutions
- Solutions built specifically for Federal Contractors:
  - Early Discovery
  - Opportunity Management
  - Capture Planning
  - Proposal Planning
  - GovWin, Beta.Sam.gov and Gov Search connectors
  - Contract Lifecycle Management

KTL SOLUTIONS

Dynamics 365 Business Central

- SaaS version deployed in Commercial cloud
- GCC & GCC-H deployed on VM's in Azure GOV
- Core Capabilities:
  - Accounting and Financial Management
  - Manufacturing
  - Supply Chain Management
  - Reporting and Analytics
- Solutions built for Federal Contactors:
  - Functionality for Professional Service & Project Based Businesses
  - Advanced project accounting
  - End-to-end Project management
  - Resource Management
  - Project Reporting and Analytics

KTL SOLUTIONS

Q & A

For more information, visit our website www.ktlsolutions.com or contact us at info@ktlsolutions.com