C3 INTEGRATED SOLUTIONS
connect, communicate, collaborate

CMMC Readiness Program

info@c3isit.com

About C3 Integrated Solutions

Technology Experience

10 years Microsoft partner

3 years experience in GCC High

Multiple Gold competencies

Client Experience

250+ Microsoft 365 clients

100+ DoD contractor clients In GCC High

Deep NIST and DFARS experience

Industry Leading

First to offer GCC High backup

First to offer hosted voice in GCC High

CMMC Registered Practitioner Org.

Microsoft Partner
Microsoft

Gold Cloud Productivity
Gold Windows and Devices
Silver Enterprise Mobility Management
Silver Collaboration and Content
Silver Security

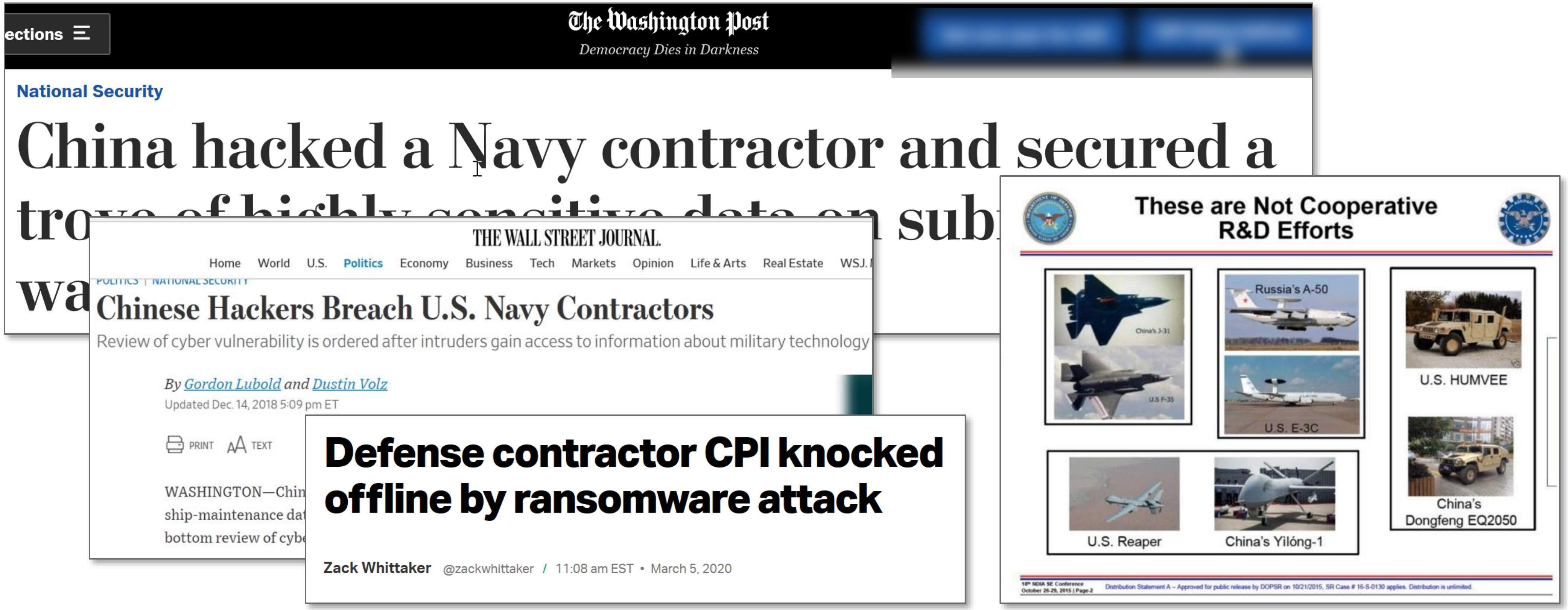
Inc.5000
N° 94
2020
IND IT MANAGEMENT

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

C3 INTEGRATED SOLUTIONS
connect, communicate, collaborate

Today's Threats

Defense Industrial Base (DIB) Is Under Constant Attack



ections ☰

The Washington Post

Democracy Dies in Darkness

National Security

China hacked a Navy contractor and secured a trove of highly sensitive data on sub

wa

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. I

POLITICS | NATIONAL SECURITY

Chinese Hackers Breach U.S. Navy Contractors

Review of cyber vulnerability is ordered after intruders gain access to information about military technology

By Gordon Lubold *and* Dustin Volz

Updated Dec. 14, 2018 5:09 pm ET

PRINT TEXT

WASHINGTON—Chin

ship-maintenance dat

bottom review of cyb

Defense contractor CPI knocked offline by ransomware attack

Zack Whittaker @zackwhittaker / 11:08 am EST • March 5, 2020

These are Not Cooperative R&D Efforts

18th NDIA SE Conference
October 26-29, 2015 | Page-2

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

INTEGRATED SOLUTIONS
connect, communicate, collaborate

Cybersecurity Maturity Model Certification (CMMC)

Designed to Ensure DIB Companies Meet Minimum Levels of Cybersecurity

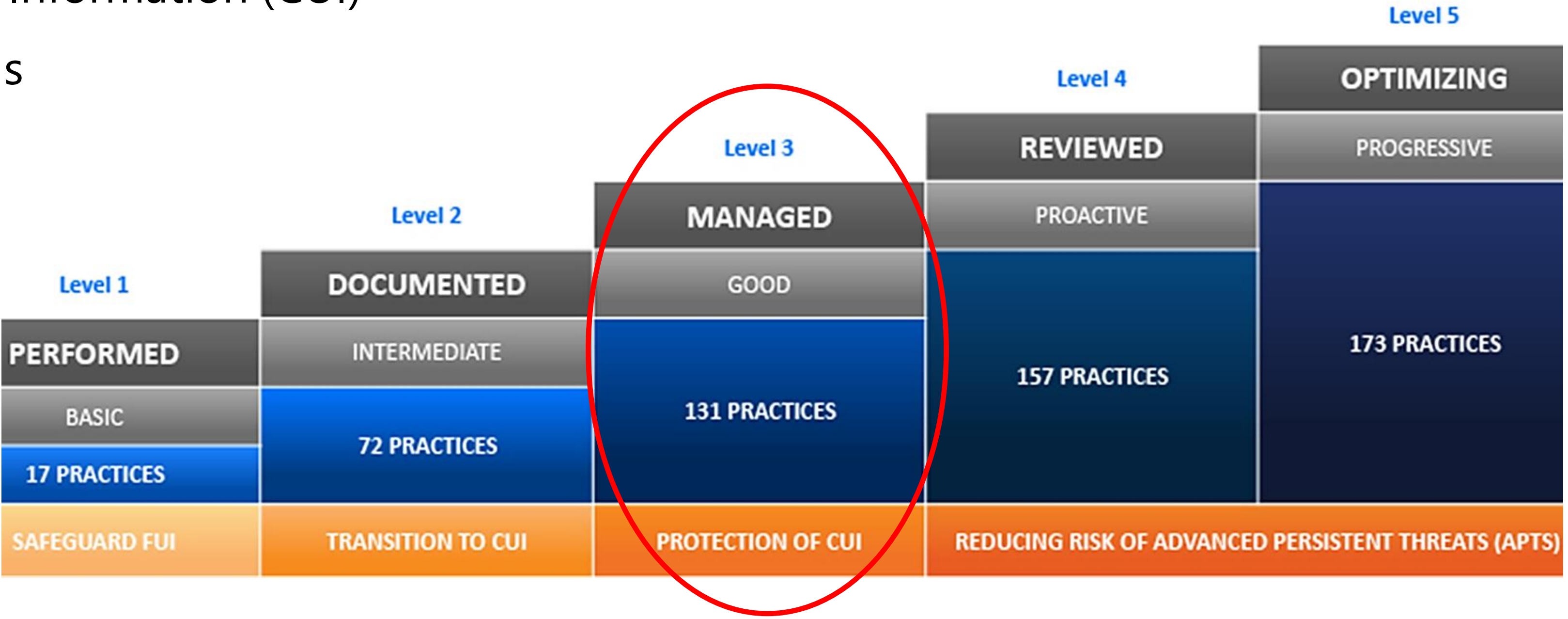
- Sets new cybersecurity rules for Defense Industrial Base
- Builds upon DFARS 7012 and NIST 800-171
- **ALL** defense contractors will need to be certified
    - 300,000 company population
- Additional federal agencies are considering following
- Went into effect **via interim rule on Nov. 30, 2020**

CMMC – Level 3 Requirements

Protecting CUI Requires a Comprehensive Cybersecurity Strategy

Level 3

- Protect Controlled Unclassified Information (CUI)
- 130 Practices – Security controls
- 3 Processes – Maturity



Level 1
PERFORMED
BASIC
17 PRACTICES
SAFEGUARD FUI

Level 2
DOCUMENTED
INTERMEDIATE
72 PRACTICES
TRANSITION TO CUI

Level 3
MANAGED
GOOD
131 PRACTICES
PROTECTION OF CUI

Level 4
REVIEWED
PROACTIVE
157 PRACTICES

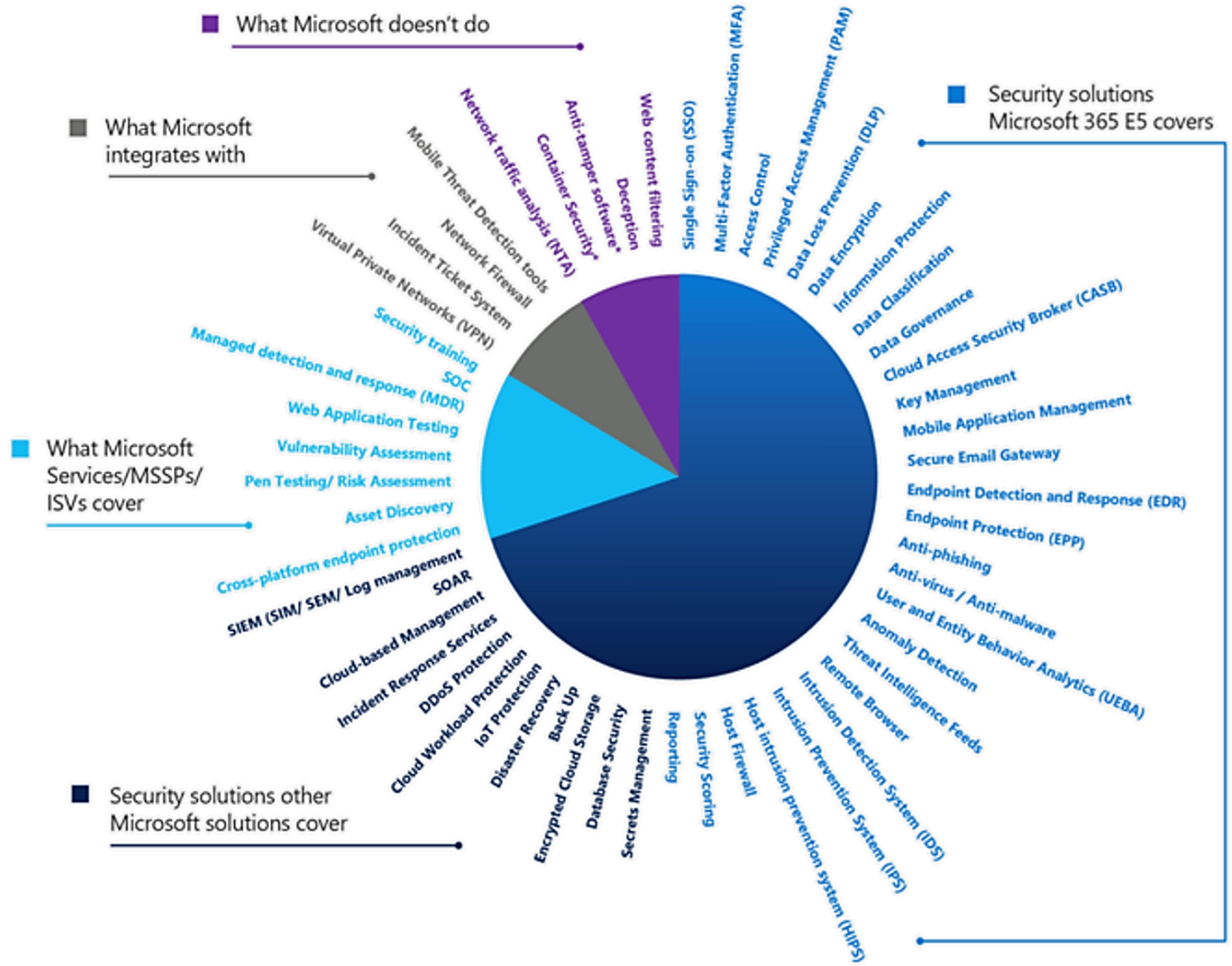
Level 5
OPTIMIZING
PROGRESSIVE
173 PRACTICES

REDUCING RISK OF ADVANCED PERSISTENT THREATS (APTS)

Microsoft 365

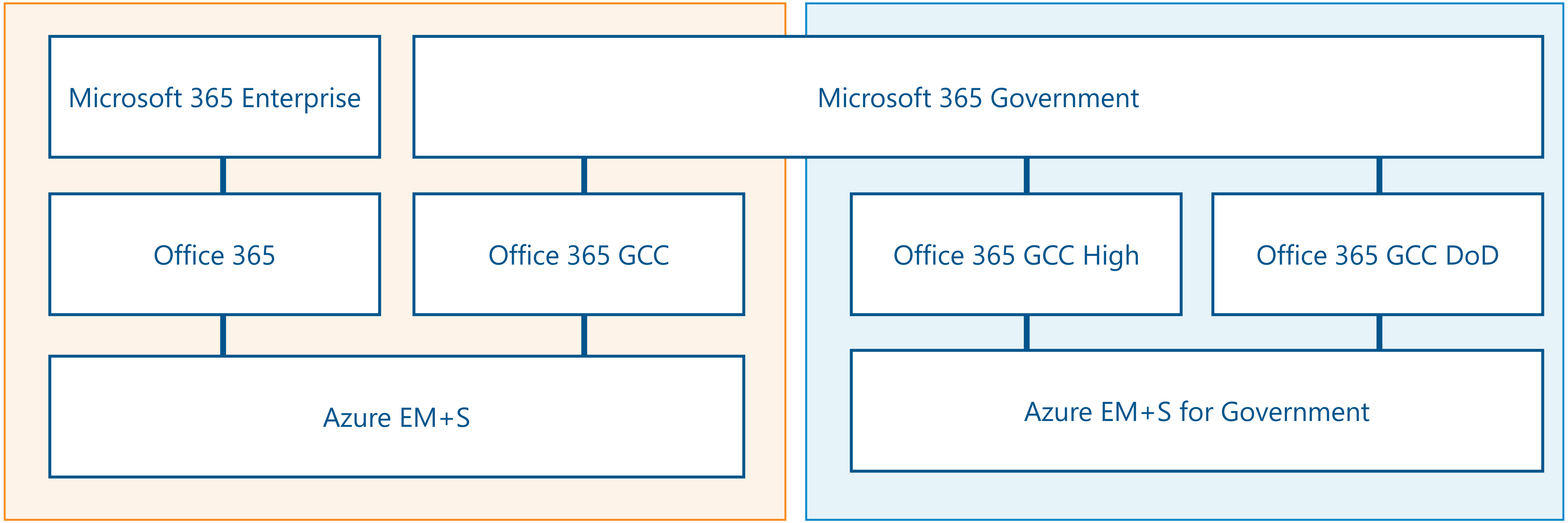
The Core of Your Security and Compliance Strategy

Microsoft 365 Can Replace Over 26 Vendor Solutions



Source: Kiran NR Cyber-security blog

Microsoft 365 Versions



US Data Residency
Global Support and Admin

US Data Residency
US Support and Admin

Microsoft Compliance

Meeting CUI and ITAR Requirements

	Commerical	M365 GCC	M365 GCC High
Data Center	US and OCONUS	CONUS Only	CONUS Only
Accreditation	FedRAMP High	FedRAMP High	FedRAMP High
NIST 800-171	Maybe*	Maybe*	Yes
DFARS 7012	No	Yes	Yes
CMMC	Level 1-2	Level 1-3*	Level 1-5
CUI/CDI	No	Maybe	Yes
ITAR / EAR	No	No	Yes

- Only GCC and GCC High meet CMMC Level 3 and DFARS 7012 requirements
- Only GCC High meets CUI Specified (ITAR, Nuclear, NOFORN) requirements

*CUI Specified (e.g., ITAR, Nuclear, etc. are not suitable. Requires U.S. Sovereignty).

C3 INTEGRATED SOLUTIONS
connect, communicate, collaborate

The CMMC Readiness Program

Delivering Compliance on Your Terms

Answering the Call

Meeting the Challenge of CMMC

THE CHALLENGE

- Small-midmarket firms most vulnerable
- Maturity
  - Underinvested in IT, cyber
  - No documentation
- Resources
  - Little to no IT or cyber staff
- Culture
  - Cyber not relevant

THE SOLUTION

- Leverage the Microsoft Cloud
  - Microsoft 365 GCC or GCC High
  - Azure Government
- Incremental
  - Build from a foundation
  - Add services incrementally
- Modular, flexible

C3 CMMC Readiness Program

A Methodical Approach to CMMC Compliance

PROGRAM OBJECTIVES

- Technology forward
    - Cloud focused
- Incremental
- Flexible
- Modular
- Builds maturity around the technology
- Mapped to compliance
    - Develop documentation
    - Prepare for audits

Microsoft 365

Azure Government

Delivering Security and Compliance

Two-Phased Approach

IMPLEMENTATION

- Onboard to compliant platform
- Access Control
- Device Management
- Threat hunting
- Event Detection and Response (EDR)
- Security Incident Event Manager (SIEM)

SUPPORT

- Ongoing support and assistance
- Security monitoring
- Managed services

C3 CMMC Readiness Program

IMPLEMENTATION

DEPLOY[2]

- Discovery
- Provisioning
- Onboarding
- Data Migration

SECURE

- Access Control
- Device Management

DEFEND

- Threat Hunting
- Endpoint Protection
- Cloud App Security
- SIEM

GOVERN

- Data Labeling
- Information Protection
- Workspace Governance

SUPPORT[1]

MONITOR

- Security Operations Center
- Detect
- Respond
- Protect

MANAGE

- Advisory
- Support
- Remote Monitoring

STRATEGIC

vCIO, Policies, Strategic Reviews, Change Management, and Documentation

1 Support phase not included in pricing.
2 Data Migration not included in pricing

Implementation

Providing Assistance to Deploy, Secure, Defend, and Govern

Deploy

DEPLOY

The journey starts with **DEPLOY** where the focus is onboarding to the Microsoft 365 GCC High platform. This includes evaluating legacy data stores, planning the overall effort, provisioning the services, and migrating the data.

License Focus: Office 365 E3, Back-up, Voice

Onboarding

Licensing*

Data Migration*

- Email
- OneDrive
- Teams
- SharePoint

Ancillary Services*

- Backup
- Voice

*Not included in price

Secure

SECURE

With **SECURE**, conditional access policies in Azure Active Directory are combined with features like device enrollment and app protection policies to ensure that all access to GCC High is secured and compliant.

License Focus: Azure AD, EndPoint Manager

Access Control
Conditional Access
Mobile Devices
Windows 10 Devices

Defend

DEFEND

With **DEFEND**, we transition from passive to active pursuit of threats and breaches. Advanced security settings around Advanced Threat Protection, Windows Defender, and Cloud App Security among other capabilities are activated to ensure the environment’s overall security. The logs from these services as well as those native to GCC High are then aggregated in Azure Sentinel.

License Focus: E5 Step-up, Azure Sentinel

Threat Hunting
Endpoint Protection
Cloud App Security
SIEM Deployment

Govern

GOVERN

In the **GOVERN** phase, we focus on securing the flow of CUI both within and outside of the system boundaries. Document categorization and labeling are used to apply policies limiting access, encrypting files and marking appropriately. Within the Teams and SharePoint environment we also offer cutting-edge services to ensure unauthorized users never access restricted workspaces.

License Focus: DLP, AIP, Workspace Governance

Data Classification
Information Protection
Workspace Governance

Support*

Providing Ongoing Assistance Post-implementation

* Not included in price

Monitor

MONITOR

In the **MONITOR** phase, we provide the constant vigilance with 24x7 Security Operations Center that can detect, respond and protect the environment. MONITOR also includes an industry-leading executive dashboard to manage the compliance posture.

License Focus: Security Operations Center

Security Ops Center
Detect
Respond
Protect
ARMED Exec Dashboard

C3 INTEGRATED SOLUTIONS
connect, communicate, collaborate

Manage

MANAGE

With **MANAGE**, we provide a range of options to support the ongoing management and administration of the IT environment. This may include retainers for administrative level support, remote monitoring, and even end-user support services.

License Focus: Pro Support Services, MSP

Professional Support Services
End User Support
Remote Monitoring

INTEGRATED SOLUTIONS
connect, communicate, collaborate

Thank you!

For more information, email info@c3isit.com

November 2020

Follow us on social media:

@c3isit

/c3integrated

/company/c3-integrated-solutions