MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Lessons Learned from PRMA Assessments

Alex Gordon

Gabriel Helms

Peregrine Technical Solutions, LLC.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

BLUF

1. The cybersecurity methodology for OT and ICS is stove-piped.
2. Mission Assurance considerations are often not integrated into cybersecurity assessments, methodology, or investments for OT/ICS
   a) Current frameworks do not incorporate Mission Assurance dependencies outside of the system accreditation boundaries
   b) Limited capabilities to continuously protect, detect, and respond to threats in near real time for OT/ICS
   c) Decisionmakers lack the visibility or background on OT/ICS cybersecurity
   d) Investment decisions are reactive and focused on addressing specific vulnerabilities verses strategic in nature based on prioritized Mission Assurance objectives.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

An Integrated Approach to OT/ICS Security

Current OT/ICS Security calls for developing, coordinating and integrating independent efforts and frameworks for assessing OT/ICS, developing day to day situational awareness, threat detection, response and cyber-hygiene for OT/ICS, and Integrating threat-based analysis to identify near and long-term strategic investments, with mission assurance as the backbone of the construct providing an all-inclusive interdependent process for the protection of OT/ICS infrastructure.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Platform Resilience Mission Assurance (PRMA)

1. Platform Resilience Mission Assurance (PRMA) assessments have provided key insights on cybersecurity vulnerabilities to DoD's Critical Infrastructure IT/OT and Control Systems.

2. Peregrine was contracted by the Office of the Assistant Secretary of Defense for Energy, Installations and Environment for to perform individual PRMA functions under three separate efforts.
   a) Joint Mission Assurance Assessments (JMAA) 24 Assessments.
   b) SME support to MOSAICS JCTD.
   c) SME support to DoD cybersecurity Analysis and Review (DoDCAR).

MOSAICS
2020 INDUSTRY DAY

Peregrine TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Mission Assurance

DOD INSTRUCTION 3020.45 MISSION ASSURANCE (MA) CONSTRUCT

a) Provides a framework for risk management across all protection and resilience programs.
b) Accounts for the full range of threats and hazards to the capabilities and supporting assets, not just cyber threats.
c) Mission Assurance considerations are often not integrated into Assessments, Protect, Detect, Respond and Recover methodology, and strategic cybersecurity investments for OT and IT systems.
d) Traditionally not integrated with other frameworks.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Joint Mission Assurance Assessments (JMAA)

Joint Mission Assurance Assessments (JMAA)

a) Assesses the cybersecurity of Critical Infrastructure legacy Control Systems (CS), Operational Technology (OT) and Industrial Control systems (ICS).
b) Senior leadership tends to think about mission readiness in terms of airframes, bombs, missiles, ships, tanks etc., training and available funding.
c) Most warfighters do not account for reliability of OT/ICS that are proving support activities.
d) Overall Responsibility often in question.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Real-Time Situational Awareness

Situational awareness, continuous protection, detection, and response to all threats in near real-time for OT and ICS

a) The MOSAICS JCTD validates the need for real-time response actions to disrupt operations.
b) The implementation or integration of this capability into a MA construct is a challenge.
c) No clear guidance on aligning this capability with the cybersecurity mission of the SOC versus the OT/ICS systems as they are mapped to the supported installation's mission.
d) Must be aligned and mapped to Mission Assurance requirements to provide decision makers with real-time information and SA of mission impacts.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Threat-Based Assessment for OT/ICS

Threat based approach to cybersecurity for ICS

a) DoD Cybersecurity Analysis and Review (DoDCAR) *"MITRE ATT&CK"* which is a threat-based, cybersecurity architecture for assessments.
b) Provides leadership insight and knowledge to make well-informed, threat-prioritized cybersecurity investment decisions.
c) Synchronize and balance cybersecurity investments, minimize redundancies, eliminate inefficiencies, and improve all-around mission performance.
d) Enables dependable mission execution.
e) Traditionally not integrated with other frameworks.

MOSAICS
2020 INDUSTRY DAY

Peregrine TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Risk Management Framework for OT/ICS

Risk Management Framework for ICS

a) Originally Implemented for IT systems: *DoD 9510 "Risk Management Framework (RMF) for DoD Information Technology (IT)".*
b) Focuses on protection of information processed and stored on an information system.
c) OT/ICS systems do not process or store traditional Information.
d) Mission owners are not part of the RISK Approval process.
e) No formal mapping to mission essential task.
f) Mission essential task vary based on service and organization.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Other Considerations

1. Integration of MA into Red Team and Blue Team exercises.
2. Defense industrial base priorities and facilities that support Warfighter METL.
3. Commercial service providers for installation OT/ICS priority of service based on installation METL.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Conclusion and Lessons Learned

1. Each effort and concept are successful and provide some level of protection individually.
2. Significant overlap with regards to the cybersecurity OT/ICS.
3. Should be tied together under one construct based on Mission Assurance and the Task Critical Assets they support.
4. OT/ICS systems must be weighed specifically to the mission supported.
5. Can be addressed through process and technology development.

MOSAICS
2020
INDUSTRY
DAY

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Questions?

Peregrine
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Dr. Leigh Armistead, President (CISSP)
114 Ballard Street, PO Box 520
Yorktown, VA 23690-0520
Larmistead@goldbelt.com
Phone: (757) 234-6664
Cell: (757) 871-3949
Fax: (757) 234-6505