Attacking and Monitoring Space System Assets

Presented by John Arkoian, Mario Zuniga

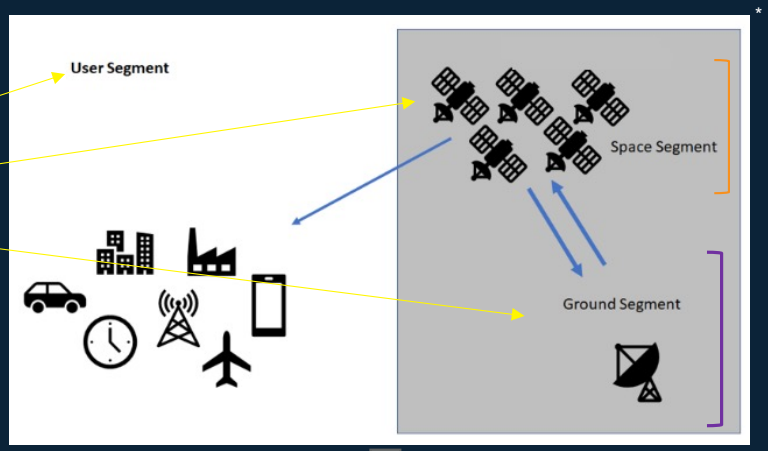
MITRE Cybersecurity Days

13 October 2021

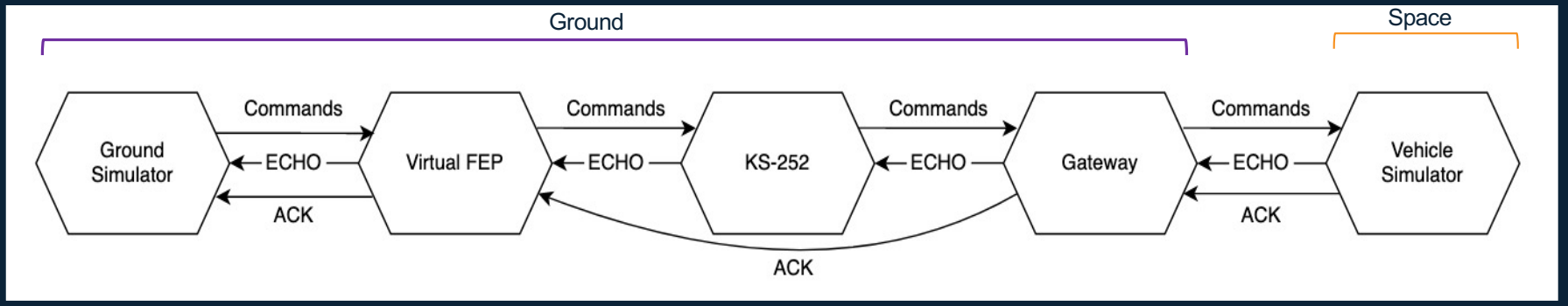
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

A Surrogate System

"Defend Cyber Here"

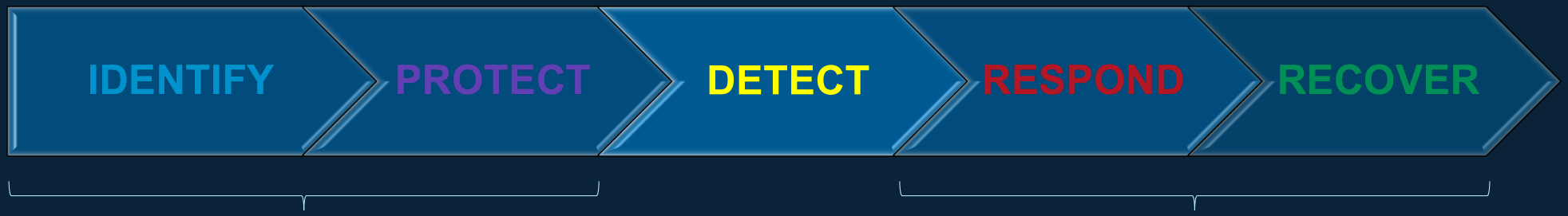


The Lab System



Adapted from: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf

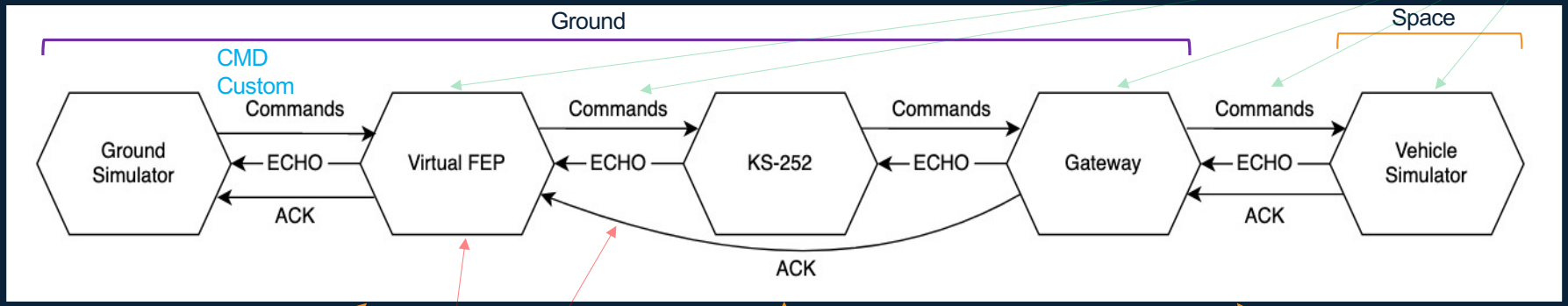
A Focus on Monitoring



Additional Dependencies (Errr… Attack Vectors)

Operational Vectors

Our Lab System

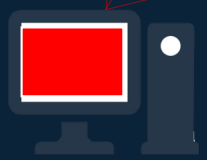


Supporting Vectors

BACnet
SNMP

GEMS

Support Infrastructure	Maintenance	Mission Needs
Power Space Cooling	System Upgrades Regular Audit Equipment maintenance	Mission Failover Needs Network Testing Crypto Re-keying

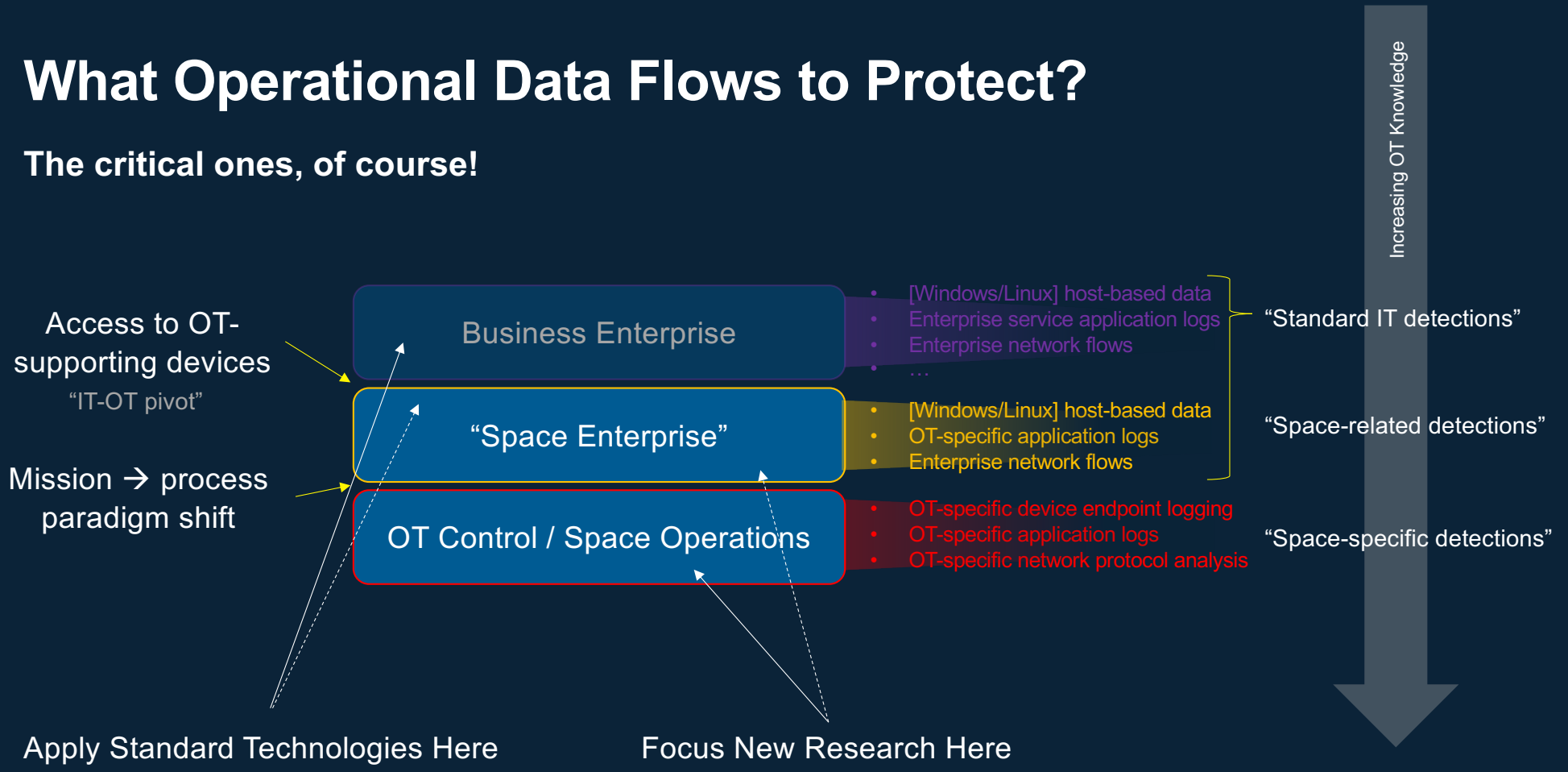


Attack

MITRE

What Operational Data Flows to Protect?

The critical ones, of course!

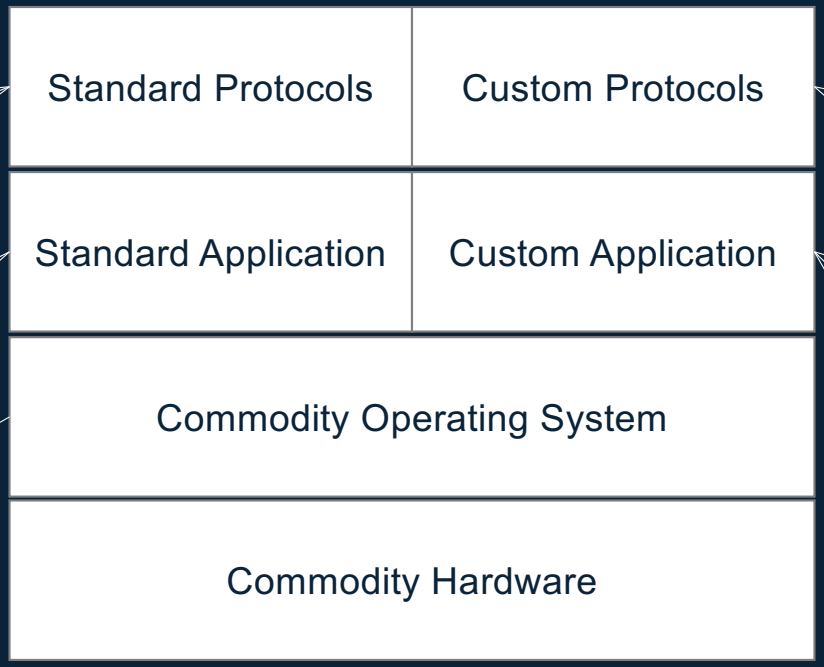


What Familiar Technologies Are Present?

Use what we can, build new tools when we can't

We have tools for:

- RDP/VNC
- HTTP
- SMB
- Syslog
- ssh
- SELinux



We need tools for:

- CMD/TLM
- GEMS
- COSMOS // NOS3
- Custom REST API
- Custom Application Logs

"Space System"

Operational Space Protocols Get Messy

- Intimate knowledge of the implementation of protocols is necessary to understand mission needs
- Building parsers and generating data from them run is the easier half of the battle
- Making actionable information from the data is the harder problem

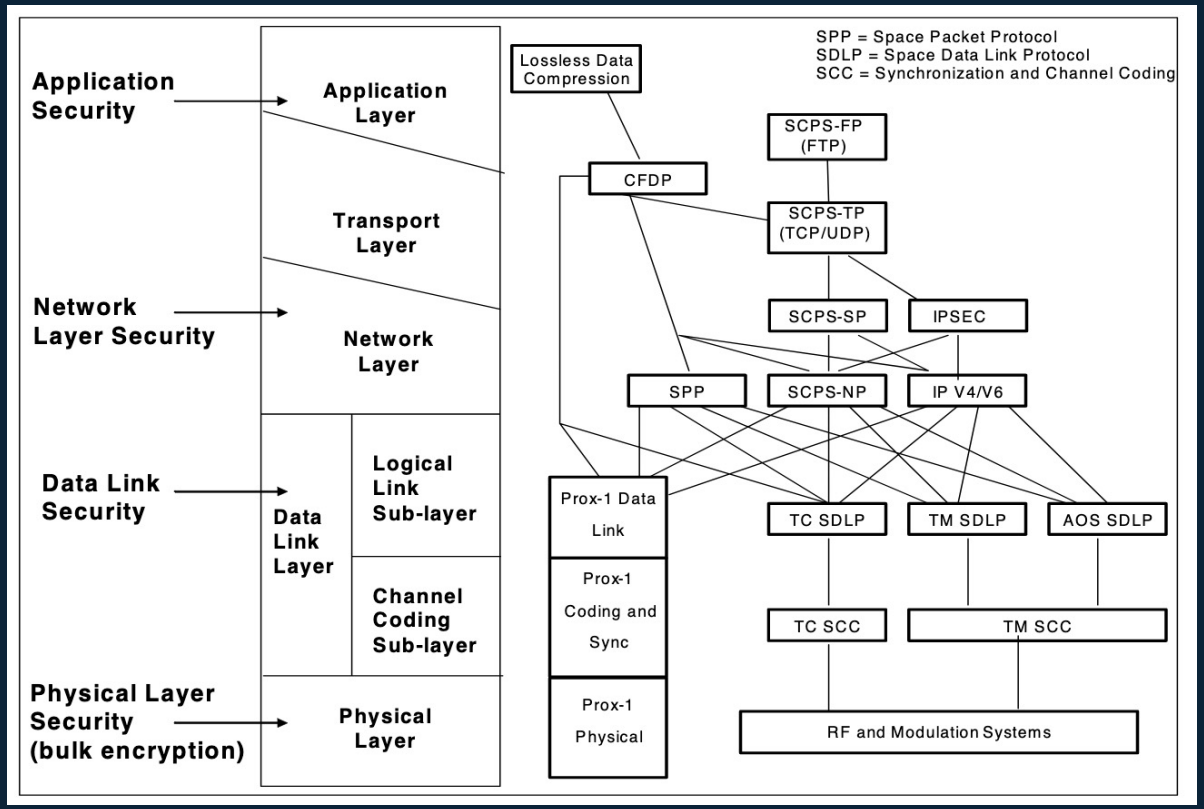
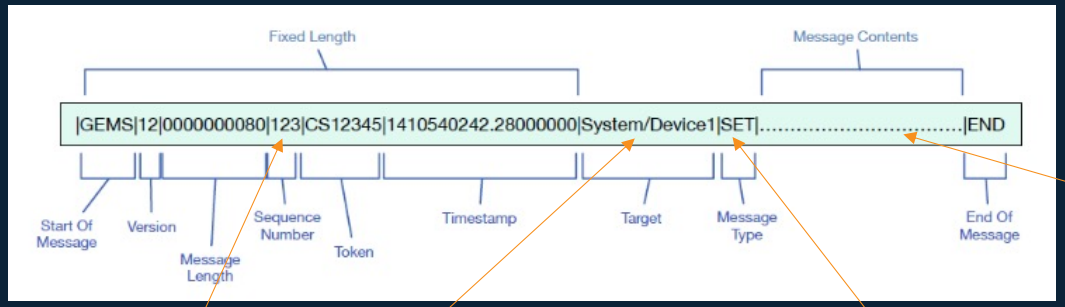


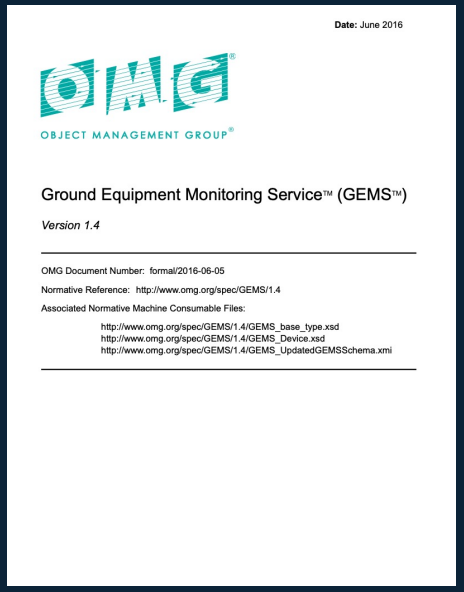
Figure adapted from CCSDS 130.0-G-3; https://public.ccsds.org/Pubs/130x0g3.pdf

Deciphering an Example Protocol

- Performing monitoring on the GEMS protocol for increased insight

- Operational context needs to know:




Date: June 2016

OBJECT MANAGEMENT GROUP

Ground Equipment Monitoring Service™ (GEMS™)

Version 1.4

OMG Document Number: formal/2016-06-05

Normative Reference: http://www.omg.org/spec/GEMS/1.4

Associated Normative Machine Consumable Files:

http://www.omg.org/spec/GEMS/1.4/GEMS_base_type.xsd
http://www.omg.org/spec/GEMS/1.4/GEMS_Device.xsd
http://www.omg.org/spec/GEMS/1.4/GEMS_UpdatedGEMSSchema.xmi

Valid Sequence Number?

System targets are well understood?

Is the Message Type Proprietary?

What do the contents of this message actually DO?

*Images from public specification OMG GEMS v1.4

Correlating with Additional Data

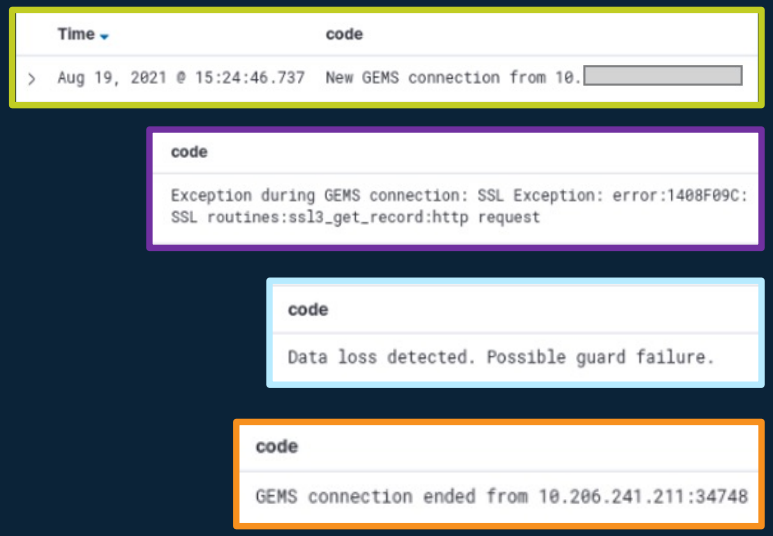
- Network-based monitoring may highlight an anomaly:

Increasing Context

Unexpected GEMS traffic message

- Pairing with host-based data can provide additional insight:

Instrumented data sources



…after a new GEMS session started

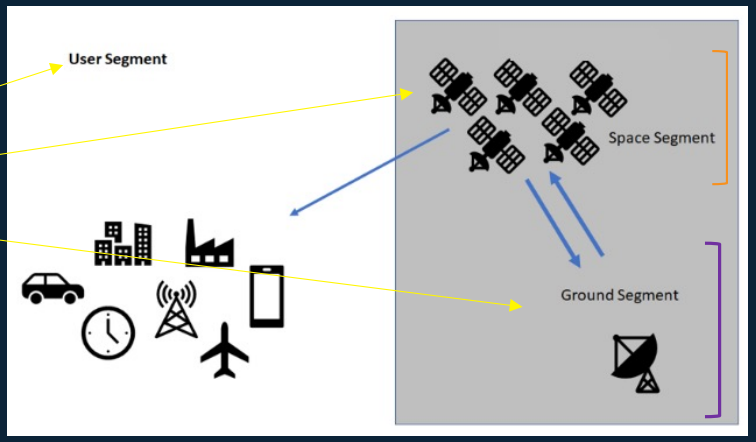
…with an associated SSL exceptions

…followed by crypto data loss

…and a clean session termination.

Tying It All Together

“Defend Cyber Here”



Develop context-aware detections that are:

- Informed by system understanding
- Relevant to operational mission
- Understood by system operators
- Actionable by mission owners

Contact for further discussion.

Nick Tsamis

ntsamis@mitre.org

@MITREcorp

linkedin.com/in/nicktsamis

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™