
DRAGOS
INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY
SAFEGUARDING CIVILIZATION

BOUNDING CYBER IN DBT

Evaluating the effectiveness of nuclear power plant cyber defenses against adversaries with cyber capabilities.

Dr. Jacob Benjamin

Principal Industrial Consultant

DRAGOS

SANS ICS Summit

Asia Pacific (APAC)

November 13, 2020

DESIGN BASIS THREAT (DBT)

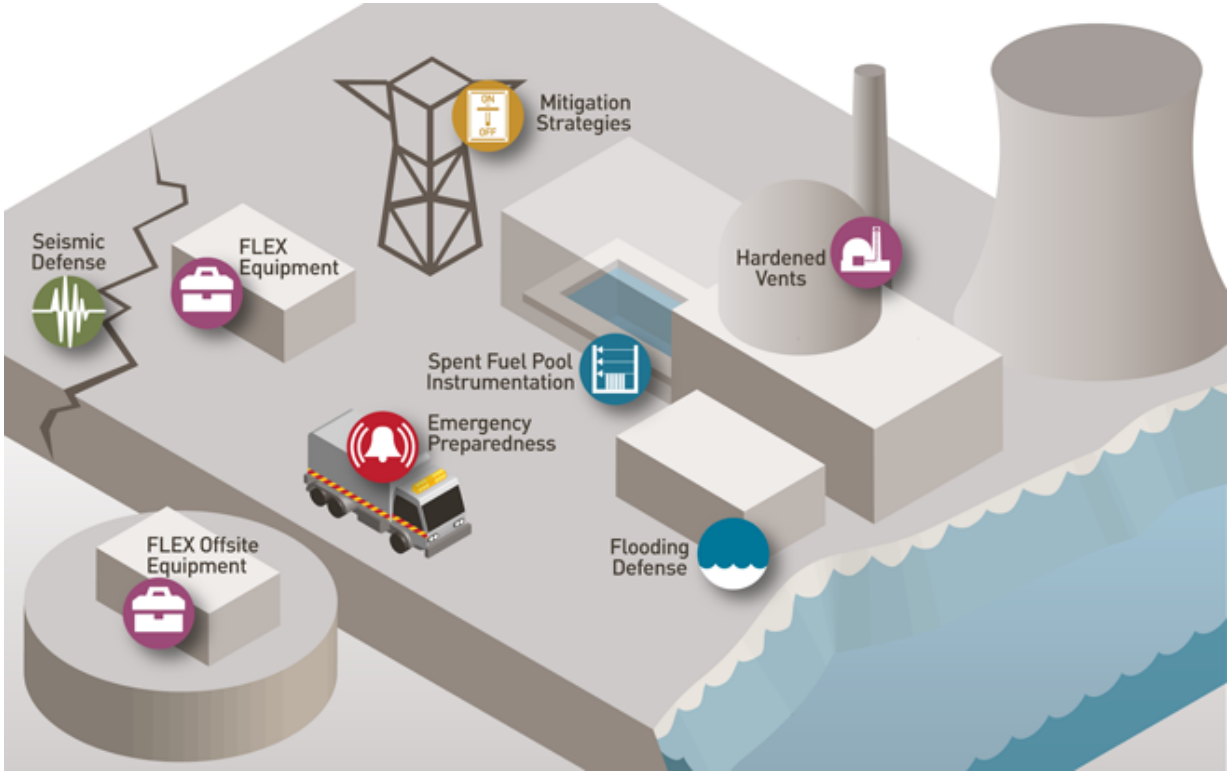
BASICS

WHAT IS DBT?

HOW ARE THEY DEVELOPED?

WHAT DOES A DBT LOOK LIKE?

ARE THERE CYBER DBTS?



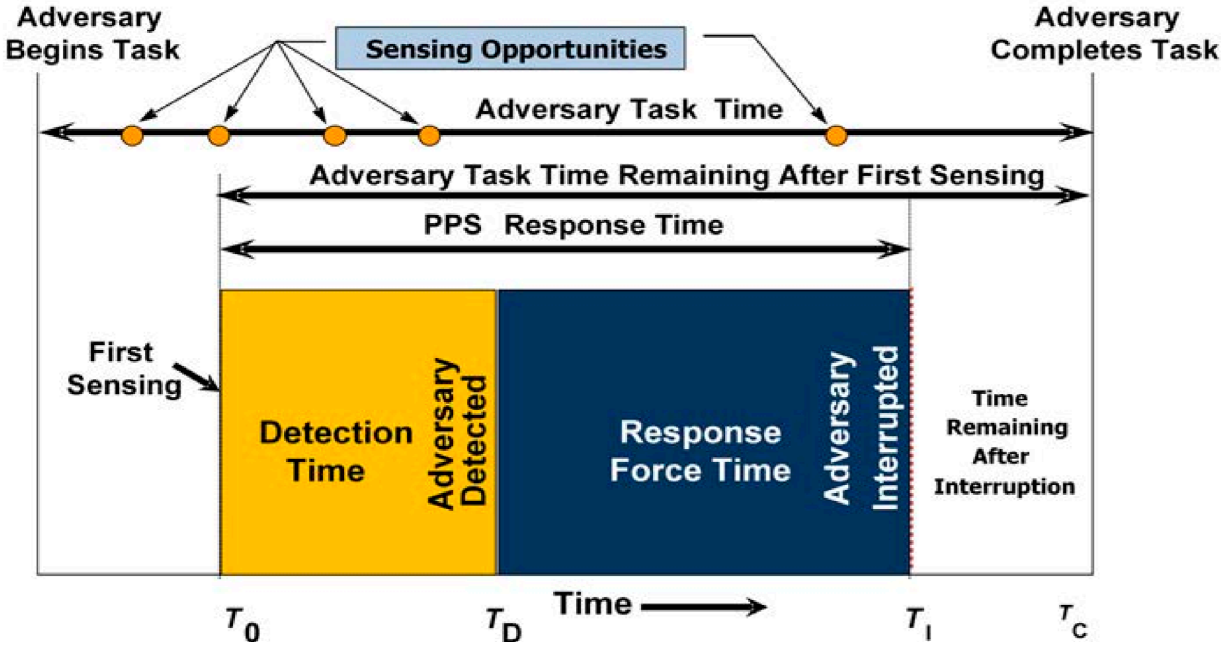
EXAMPLE DBT

IAEA DBT WORKSHOP

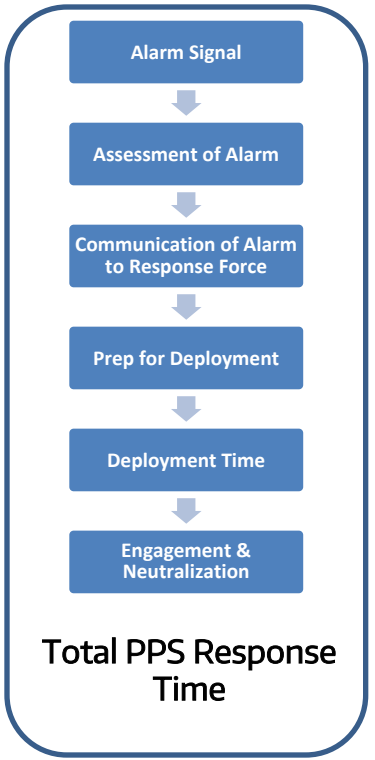
Attempt of theft of a significant amount of Nuclear Material (e.g. 10Kg of Pu) by a group of 6 outsiders equipped with 10 Kg TNT explosive, automatic weapons (including light infantry weapons) and specific commercially available intrusion tools. They have a comprehensive knowledge of the facility and associated physical protection measures. Willing to die or to kill. No collusion with insider.

PHYSICAL SECURITY ASSESSMENTS

Response Time vs Adversary Task Time



NSS 27-G



NUCLEAR CYBER SECURITY

Cybersecurity risk mitigation for nuclear power plants began in 2002 and 2003, when the NRC included cybersecurity requirements in the Physical Security and Design Basis Threat Orders.

Voluntary Cyber Program

NEI 04-04

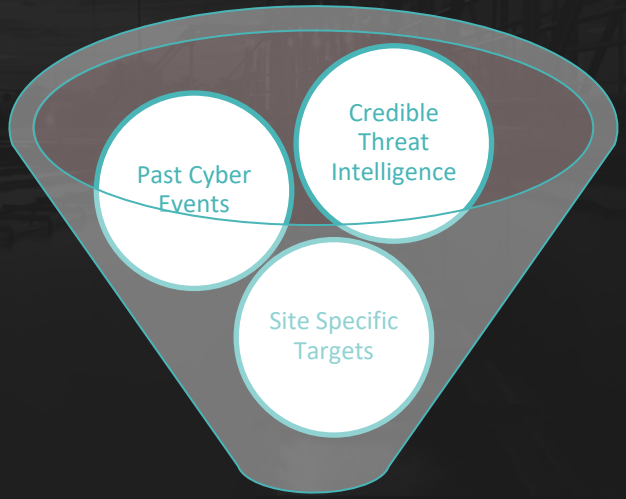
The Cyber Rule

10 CFR 73.54

Implementing Cyber Security Plans

NEI 08-09 & NEI 13-10

USING TRADITIONAL DBT ANALYSIS FOR CYBER



Cyber DBT

PAST CYBER EVENTS

Nuclear Sector & Energy Sector

CREDIBLE THREAT INTELLIGENCE

World View, CISA, etc.

SITE SPECIFIC TARGETS

Crown Jewel Analysis

MITRE ATT&CK
THREAT BEHAVIOR LEXICON

- MITRE ATT&CK is an encyclopedia of **threat behaviors**.

Enterprise Mobile

ICS

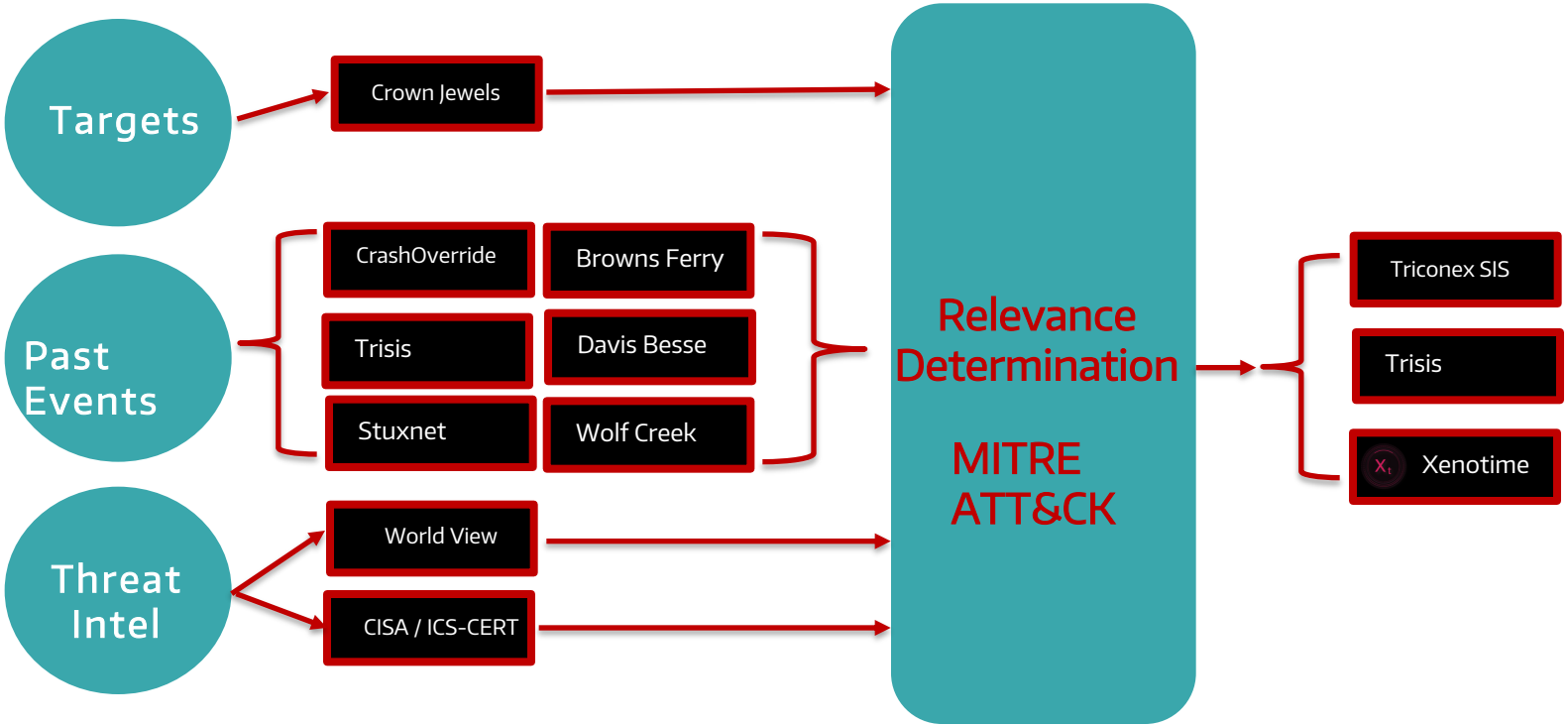
TECHNIQUES
Achieve Goals

TACTICS
Technical Goals

Collection	Command and Control	Inhibit Response Function	Impair Process Control
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading
Detect Program State		Block Reporting Message	Modify Control Logic
I/O Image		Block Serial COM	Modify Parameter
Location Identification		Data Destruction	Module Firmware

CYBER DBT DEVELOPMENT

EXAMPLE

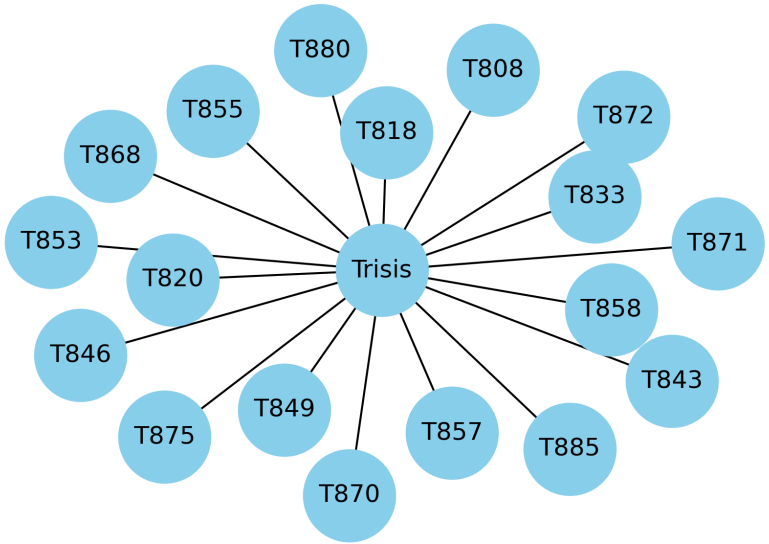


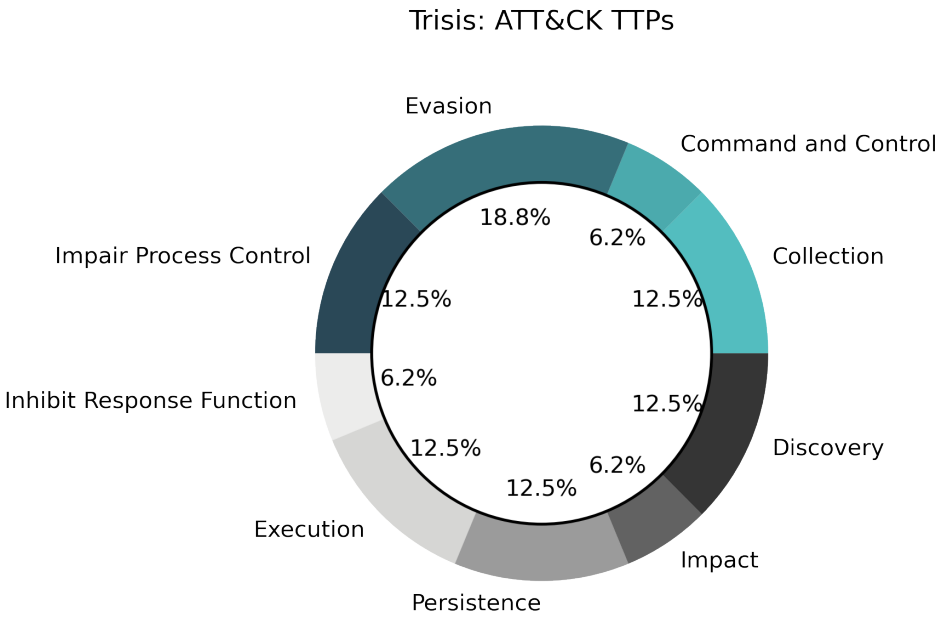
XENOTIME TTPS

THREAT BEHAVIOR FROM CYBER DBT

#	Name	Tactic(s)
T817	Drive-by Compromise	Initial Access
T822	External Remote Services	Initial Access, Lateral Movement
T859	Valid Accounts	Persistence, Lateral Movement
T862	Supply Chain Compromise	Initial Access
S0013	Trisis	Various (see next slide)

TRISIS
THREAT BEHAVIORS





RESULT

CYBER DBT

Attempt to cause physical damage to **Safety Instrumentation Systems**. The adversary has been known to use **Drive-By Compromise, External Remote Services, Valid Accounts,** and **Supply Chain Compromise,** and **ICS-Tailored Malware**. They have destructive capabilities, understand process implications, and have specific knowledge of industrial control systems. Willing to to cause physical harm or kill. No collusion with insider.

QUANTITATIVE DATA FROM CYBER DBT

A list of potential adversaries and their attributes, characteristics, and possible actions.

Analysis determining whether specific adversaries are relevant to potential targets.

FACILITY

Targets comprised of SIS

ADVERSARY

Destructive Capabilities & Intent
ICS Process Knowledge
Specific Techniques & Tactics

REQUIRED DEFENSES

Prevent / Detect list of TTPs
Resilient against custom tools & novel malware.

MITIGATION COVERAGE

LEVERAGE THE CYBER DBT

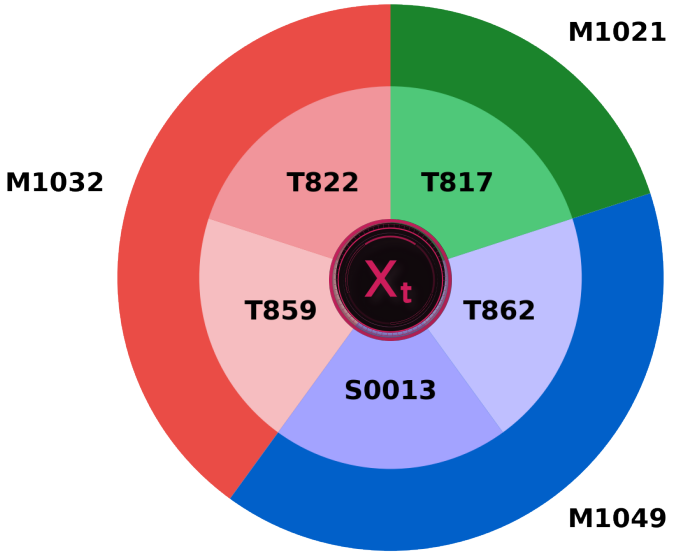
TTP	Name	Mitigations
T822	External Remote Services	M1042, M0135, M1032, M1030
T859	Valid Accounts	M1047, M1037, M1032, M1027, M1026, M1018
T817	Drive-by Compromise	M1021
T862	Supply Chain Compromise	M1049, M1016
S0013	Trisis	M1049, M1040, M1038, M1035, M1030

VISUALIZING MITIGATION COVERAGE

LEVERAGING THE CYBER DBT

ATT&CK	Name
M1032	Multi-factor Authentication
T859	Valid Accounts
T822	External Remote Services
M1049	Antivirus / Antimalware
S0013	Trisis
T862	Supply Chain Compromise
M1021	Restrict Web-Based Content
T817	Drive-by Compromise

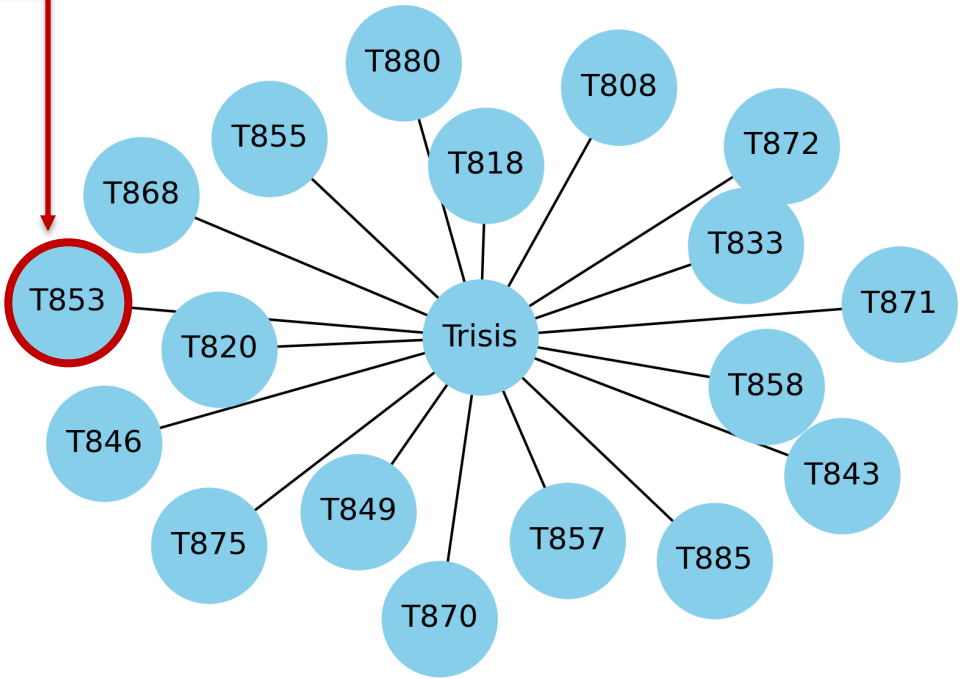
Xenotime: Mitigation Coverage




PREVENTION is ideal,
but DETECTION is necessary.
DETECTION, without
RESPONSE, is of little value.

TRISIS
THREAT BEHAVIORS

- **Scripting**
- PowerShell
- AppleScript
- Windows Command Shell
- Unix Shell
- Visual Basic
- Python
- JavaScript/JScript



CYBER DBT

HOW CAN THEY BE USED?

MITIGATIONS

Identification
Implementation
Efficacy
Prioritization

DETECTIONS

Identification
Development
Evaluation

INCIDENT RESPONSE

Incident Response Playbooks
Identifying Beyond DBT Scenarios

TRAINING

Preparedness
Realistic Scenarios

COMPARISON
OF APPROACHES

COMPLIANCE	CYBER DBT
Generic	Specific
Prescriptive	Threat-informed
Ineffective	Measurable

VS


THANK YOU
DRAGOS