Coast Guard/CISA Partnership & National Cybersecurity Assessments and Technical Services (NCATS) Capabilities Presentation

Presenter: LT Bryan Koch, USCG
Updated: July 25, 2019

Coast Guard & CISA Partnership

- The Coast Guard is partnering with and supporting the Cybersecurity and Infrastructure Security Agency in its missions to protect our nation’s critical infrastructure
- Coast Guard directly supports the CISA Threat Hunt and Incident Response Team & Vulnerability Assessments Team
- Both services are available to state/local government agencies and critical infrastructure partners free of charge

About Us

Mission: Enable our stakeholders to understand and manage risk to our Nation’s critical infrastructure

Our Vision is to be the premier, trusted partner for identifying and managing vulnerabilities

Goals

Reduce Stakeholder Risk and Increase National Resilience

Enable data-driven decisions

Influence operational behaviors

A Straightforward Strategy

Conduct assessments to develop practical operational understanding

Test a diverse sample of high value assets and nationally significant systems and functions with the same flexibility and tactics as advanced adversaries

Promote 3rd party qualification and build national capacity

Work collaboratively with other agencies, vendors, and private sector partners

CISA
CYBER+INFRASTRUCTURE

What we do, and *Why*

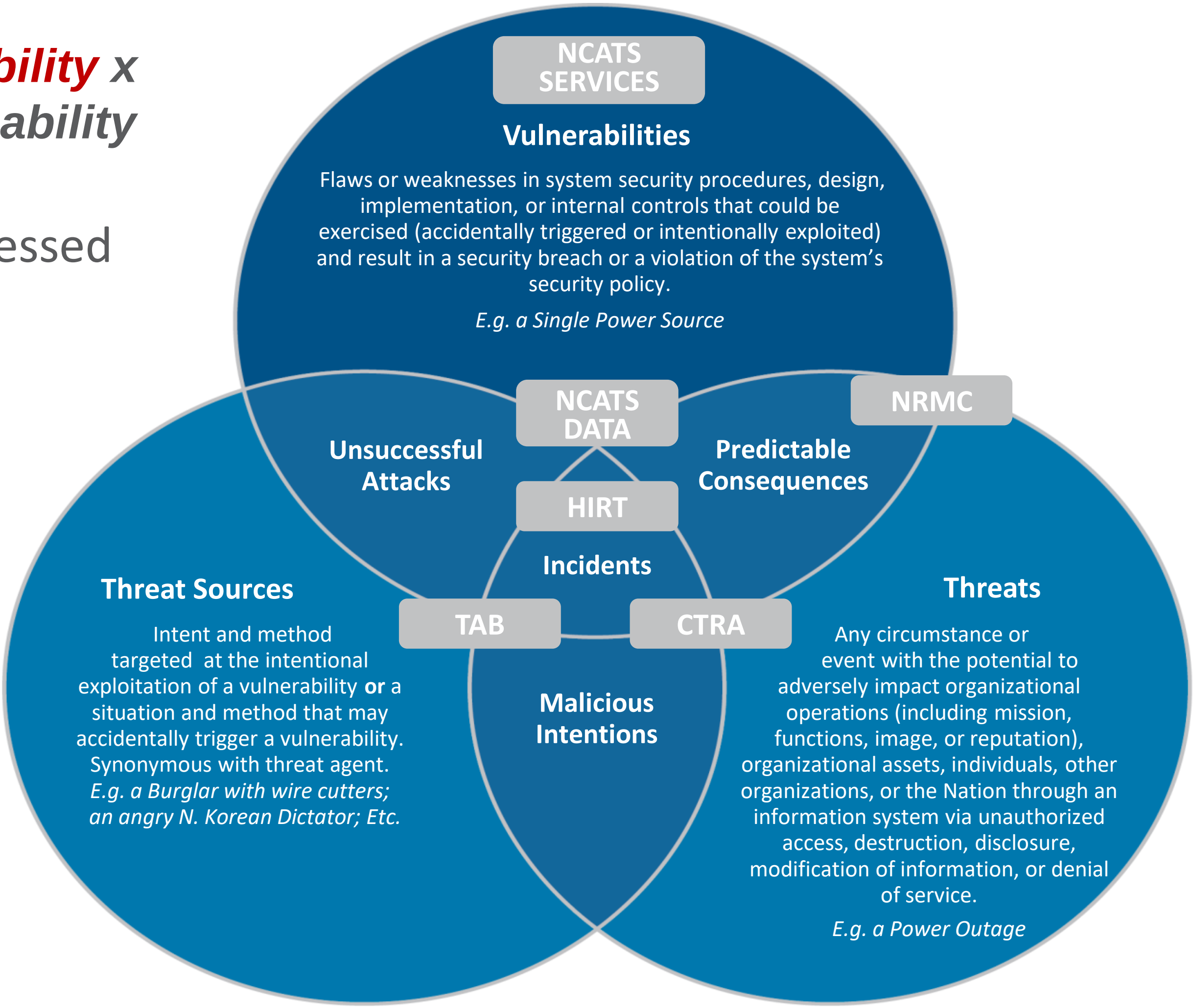
It is all about Risk Management

Risk = Actor x Vulnerability x Threat x Impact x Probability

Vulnerability can be addressed proactively to reduce risk

Combined with threat intelligence it can

- Enrich Risk Analysis
- Inform Urgency
- Enable Data Driven Decisions



NCATS SERVICES

Vulnerabilities

Flaws or weaknesses in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

E.g. a Single Power Source

NCATS DATA

NRMC

Unsuccessful Attacks

Predictable Consequences

HIRT

Incidents

TAB

CTRA

Threat Sources

Intent and method targeted at the intentional exploitation of a vulnerability **or** a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

E.g. a Burglar with wire cutters; an angry N. Korean Dictator; Etc.

Malicious Intentions

Threats

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.

E.g. a Power Outage

CISA
CYBER+INFRASTRUCTURE

Our Services

Identify and eliminate operational and technical vulnerability

Since vulnerability is the only element of risk that can be controlled

Cyber Hygiene

- What is my exposure?
- What do adversaries and malicious actors know about me?
- What do I need to know to manage risk?

Vulnerability Evaluation

- Do I have a strong design?
- Am I aligned with best practices?
- Have I addressed the most likely risks?
- What vulnerabilities are in my environment?
- What is my residual risk?

Advanced Operations

- Are my defenses working?
- Is my platform, product, or service secure against a nation state attack?
- How well am I operating?

our focus should be on proactive elimination of vulnerabilities

and helping others understand and manage their risk

CISA
CYBER+INFRASTRUCTURE

Our Services

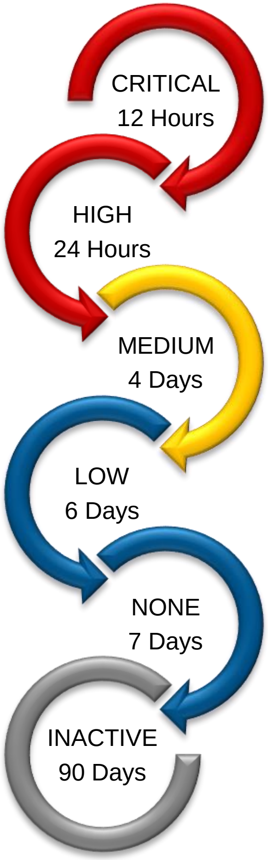
The Value Proposition

	CyHy	RPT	VADR	RVA	RTA	CPE
Duration	Ongoing	6 weeks	1-2 week(s)	2 weeks	90 days	6 weeks
Perspective	Untrusted; External	Cooperative; External	Cooperative; Internal and External	Cooperative; Internal and External	Adversarial; External	Academic; Laboratory
Objective	Assess and Monitor Exposure	Identify Exploitable Attack Vectors	Assess Technical Design and Program Maturity	Identify System Vulnerabilities	Assess Detection and Response Capability	Harden Products
Value to Customer	Greater insight into exposure; assists with risk management		Improved Processes, Policies, and Design	Decreased Risk	Benchmark and Train Staff	Products are more secure and resilient out of the box
Value to DHS (ROI)	Greater insight into exposure; assists with triage and urgency		Practical understanding of operational maturity and vulnerability		Attack Chain, Measurable Events Response	See Above

CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene

System & Application Vulnerability Scanning



- Scanning of Internet accessible systems
- Helps individual customer understand their exposure
- Informs national risk management efforts
- Weekly reports

CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene

Open Source Intelligence, Posture and Exposure Monitoring

- Monitors of variety of data sources for attack precursors, indicators of compromise, and signs of data leakage or exfiltration
- Compliments vulnerability scanning to inform risk management
  - Monitoring of Data Sources can be heavily automated
  - Customer support and validation critically important
- Many possible data sources and elements

Cyber Hygiene

Phishing Evaluations and Campaigns

- Measures propensity to click on phishing lures
- Library of crafted emails of varying levels of sophistication (obvious to stealthy) and targeting (general to targeted)
- Sent without warning and at random
- Can be used to test technical controls, user awareness and susceptibility
- Helps provide focused guidance and justify additional resources

Cyber Hygiene

Remote Penetration Testing

- Emphasis on the perimeter and rapid identification and elimination of external vulnerabilities and attack paths prior to their exploitation by a malicious actor
- Leverages all of the other Cyber Hygiene services and data collected as a starting point
- Ideal for testing centralized data repositories and assets accessible online

Vulnerability Evaluation

Validated Architecture Design Review

- Evaluates an organization’s systems, networks, and security services to determine if they are designed and built in a reliable and resilient manner
- Based on standards, guidelines, and best practices
- Includes design architecture review, system configuration and log file review, and analysis of network traffic
- Key discoveries and practical recommendations for improving the organization’s operational maturity and enhancing their cybersecurity posture are provided.

Vulnerability Evaluation

Risk and Vulnerability Assessment

- One-on-one engagements with customers that combine national threat and vulnerability information with data collected and discovered through onsite assessment activities
- Provides customers risk analysis reports with actionable remediation recommendations prioritized by risk
- Components include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration management reviews of servers and databases, and operational response maturity evaluation.

Advanced Operations

Red Team Assessment

- Emulates an advanced nation state adversary
- Distinct methodology and goals from vulnerability assessment and penetration testing
- Evaluates the people, processes, and technologies responsible for defending the network
- Incorporates a series of measurable events
- Provides actionable insight into the organizations cybersecurity posture
- Practical training for technical personnel
- Best suited for mature organizations

Advanced Operations

Critical Product Evaluation

- Evaluate Products to assess the Out-of-Box security of Critical Infrastructure systems or product lines.
  - Larger impact by assessing systems before distribution
  - Provide mitigations to vendor and/or customer base before system is employed
  - Improve the Cybersecurity Posture of entire environment where product is employed with a single assessment vs. conducting numerous assessments at individual customer sites

Service Prioritization

Factors Considered

Basis in CARVER method

- Criticality
- Accessibility
- Recuperability
- Vulnerability
- Effect
- Recognizability

Adjusted based on

- Service Trigger
- Sector / COI History
- Stakeholder History

- Data should be a diverse representation of all stakeholders
- No customer or sector should receive disproportionate resources

Scheduling

- Assessments are scheduled 90 – 120 days in advance to allow for logistical coordination
- Service queue is sorted quarterly by priority score from highest to lowest and reviewed by a scheduling review board
  - Manual review is intended to refine and tune the algorithm until the scheduling process can run fully automated
  - If necessary the review board will override and reorder, with justification and documentation, the prioritized list
  - The highest scoring candidates are selected for assessment in the upcoming quarter

Current Operational Capacity

Service	Duration	Wait Time	Capacity
Cyber Hygiene	Ongoing	None	No limit
Phishing Campaign Assessment	6 Weeks	~ 3 months	32
Validated Architecture Design Review	1 Week	~ 3 months	50
Risk & Vulnerability Assessment	2 Weeks	~ 9 months	60
Remote Penetration Test	4 Weeks	~ 3 months	64
Red Team Assessment	90 Days	~ 6 months	4

FOR INFORMATION OR TO MAKE A REQUEST:

NCATS@HQ.DHS.GOV

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE