

White Hat Operations: Building an Effective Pen Testing Team

Agenda

- Distinctions between Red Team and pen testing
- Selling points for upper management
- Disadvantages and limitations
- Build the foundation and team
- Define the tool set and refine the processes
- Planning, Execution, Post Execution, and Report Writing
- Follow-up

Pen Testing and Red Team Distinctions

| Type | Scope | Objectives | Tradecraft |
|----------------------------|---|--|---|
| Penetration Testing | Network, Web App, Solution, Social engineering (phishing) | <ul style="list-style-type: none"> Enumerate vulnerabilities Validate with known exploits Show impact to what is scoped Exercising Blue team is *not* an objective although we will collaborate with them so they can shadow the attack and tighten up their defenses later | <ul style="list-style-type: none"> Utilize known TTPs Stealth is not a factor <ul style="list-style-type: none"> Phishing requires the targets to be unaware but at the organizational level, this activity is a cooperative one |
| Red Teaming | Organization: Cyber/Comms/Operations/Social/ sometimes physical (Not NCATS) | <ul style="list-style-type: none"> Determine minimum necessary vulnerabilities/attack path(s) needed to achieve agreed upon objectives Validate with known/unknown exploits Show impact to what is scoped As a separate activity or as part of the same one, exercise blue teams to measure how well they protect, detect, respond and in some cases recover against adversarial attacks | <ul style="list-style-type: none"> For specific threat emulation, exercise known TTPs For other cases, utilize any TTP allowed within the ROE to include 0-days developed by the assessing team. Stealth is everything unless there is a specific threat being emulated that has a particular "signature". Trusted agents are used to aid in insider threat or blue team monitoring situations. |

Why Build a Test Team

Compliance and governance

RPCI-DSS regulations

Identifies unknown deficiencies, weakness, and misconfiguration

Bolsters reputation

HVA discovery and susceptibility

User awareness and training

Asset discovery

Justifies additional defensive/offensive spending

Helps refine Incident Command process

You get to wear a hoodie

Identifies network strengths

Security tool validation

Justifies the stickers on your laptop

Vulnerability identification

Risk prioritization (low, medium, high)

People fear you for no good reason

It's fun!

Compliance and governance

Incident Response training

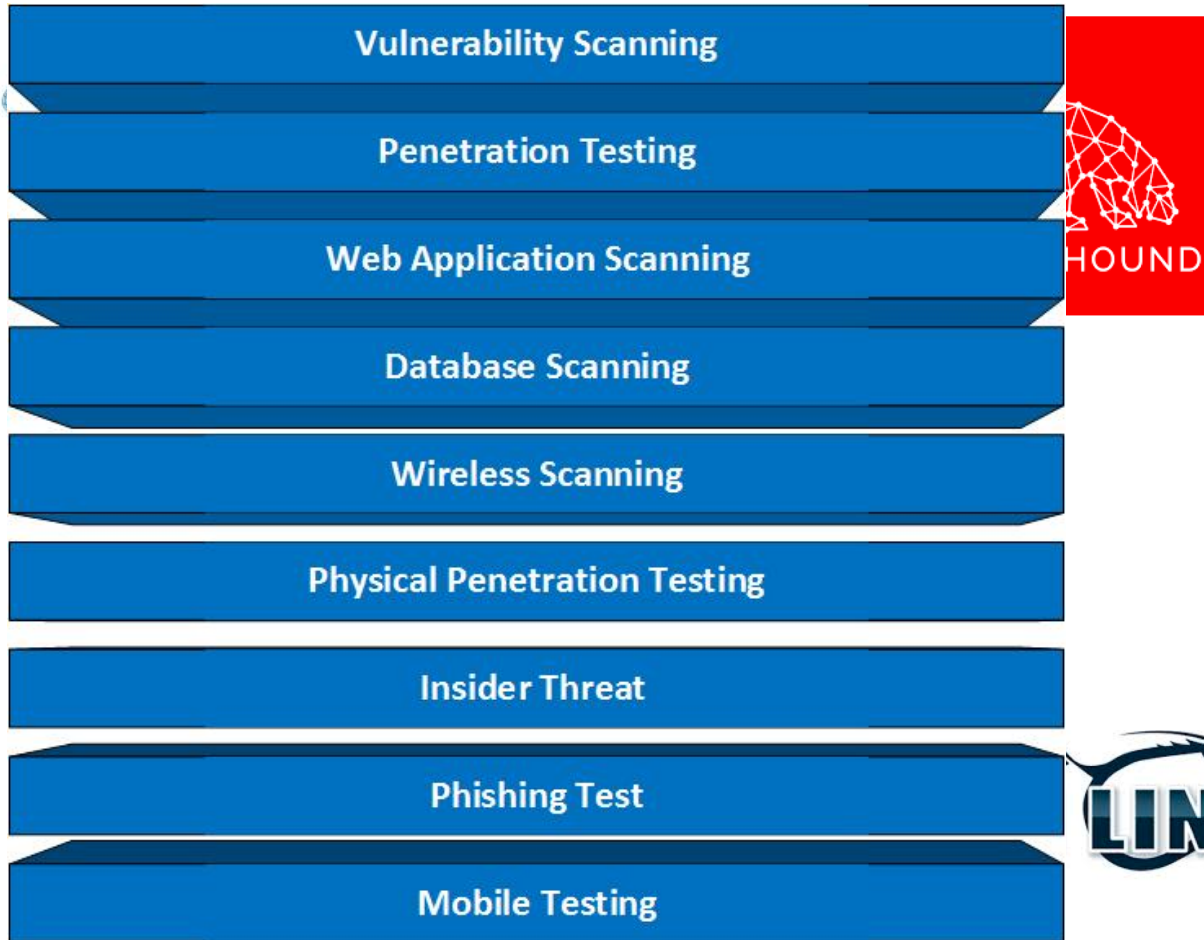
Potential Disadvantages and Limitations

- Covers just the target application, infrastructure, or environment that has been selected
- Focuses on the exposures in technical infrastructure, so it is not intended to cover all the ways in which critical or sensitive information can leak out of your organization
- *Plays only a small part (despite often including social engineering tests) in reviewing the people element (often the most important element of an organization's defense system)*
- Is only a snapshot of a system at a point in time
- Can be limited by legal or commercial considerations, limiting the breadth or depth of a test
- May not uncover all security weaknesses, for example due to a restricted scope or inadequate testing
- Provides results that are often technical in nature and need to be interpreted in a business context
- Ensure that the organization has reached at least a moderate level of INFOSEC maturity and cyber hygiene

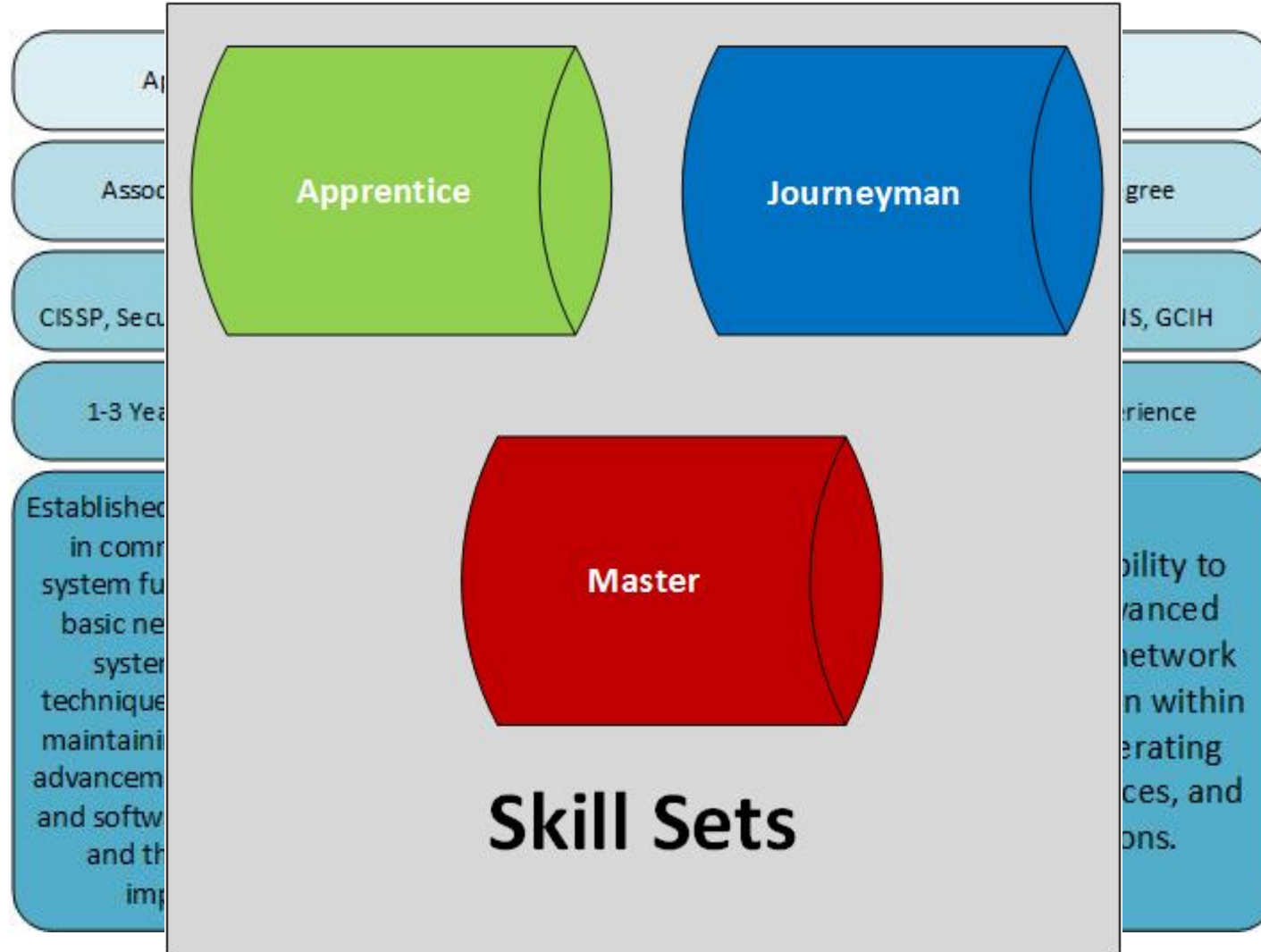
Lay the Groundwork and Build a Foundation

- Leadership and legal approval
- Funding
- Create and develop documentation
 - Mission statement
 - Organizational charts
 - Rules of Engagement
 - Scoping documents
 - CONOPS, test plans, FAQs, process flows
 - Reporting templates and/or generators
 - Follow-up processes
 - Measure success
- Align with an existing, established framework such as NIST cybersecurity framework, ISO 27001, ISF, etc.

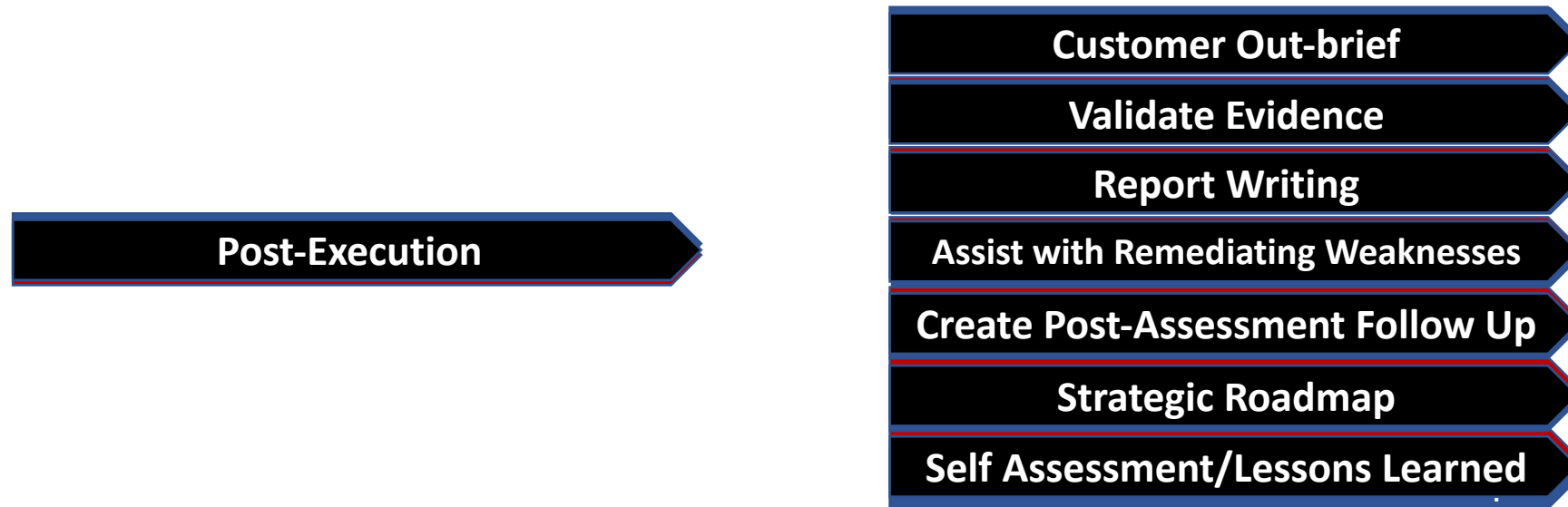
Define the services and tools



Build the team



Refine the processes



SELECTION OF ASSESSMENT SERVICES

[Redacted] authorizes DHS to perform the required service(s) as part of the HVA RVA, on the networks/systems listed below in this Appendix A, as described in the Risk & Vulnerability Assessment Catalog, Version 3.2, Appendix C.

External testing will be conducted by the RVA team from a range of attributed or unattributed IP addresses that may not be identified to [Redacted] and that may change periodically without notice to [Redacted]. Agency defense systems, such as intrusion detection or prevention systems, may detect and react to this testing activity. As such, the agency Site Monitor should be prepared to react accordingly by, for example, ensuring a perceived attempted intrusion related to this testing is not incorrectly reported outside of the agency as an incident. Internal testing will be conducted by the RVA team either on-site or through a virtual private network (VPN) provided by [Redacted].

Notify SOC
External Part

tes and
mes

Procure Sco
Documen

Pre—
t Briefs

| Authorized Testing Sites & Services | | | | | |
|---|---|-------------------------------------|-------------------------|------------------------------------|------------------|
| 1. Penetration Testing 2. Phishing Assessment 3. Web Application Assessment | | | | | |
| Site Name/Address | Authorized IP Addresses/ Network for Assessment | IP/Network Excluded from Assessment | Need for Admin Access ? | Select: External, Internal/On-site | Authorized Dates |
| Site Name/Address | IP For Assessment | IP Excluded | Yes or No | E or I/O | Date |
| | | | ▼ | ▼ | |
| | | | ▼ | ▼ | |
| | | | ▼ | ▼ | |
| | | | ▼ | ▼ | |
| | | | ▼ | ▼ | |
| | | | ▼ | ▼ | |



**Homeland
Security**

Evidence
and C

**National Cybersecurity Assessment and Technical
Services (NCATS)**



Data Handling and Storage Guide (DHG)

Com
Asses

Prepared for



**Department of Homeland Security Headquarters (DHS HQ)
CS&C**

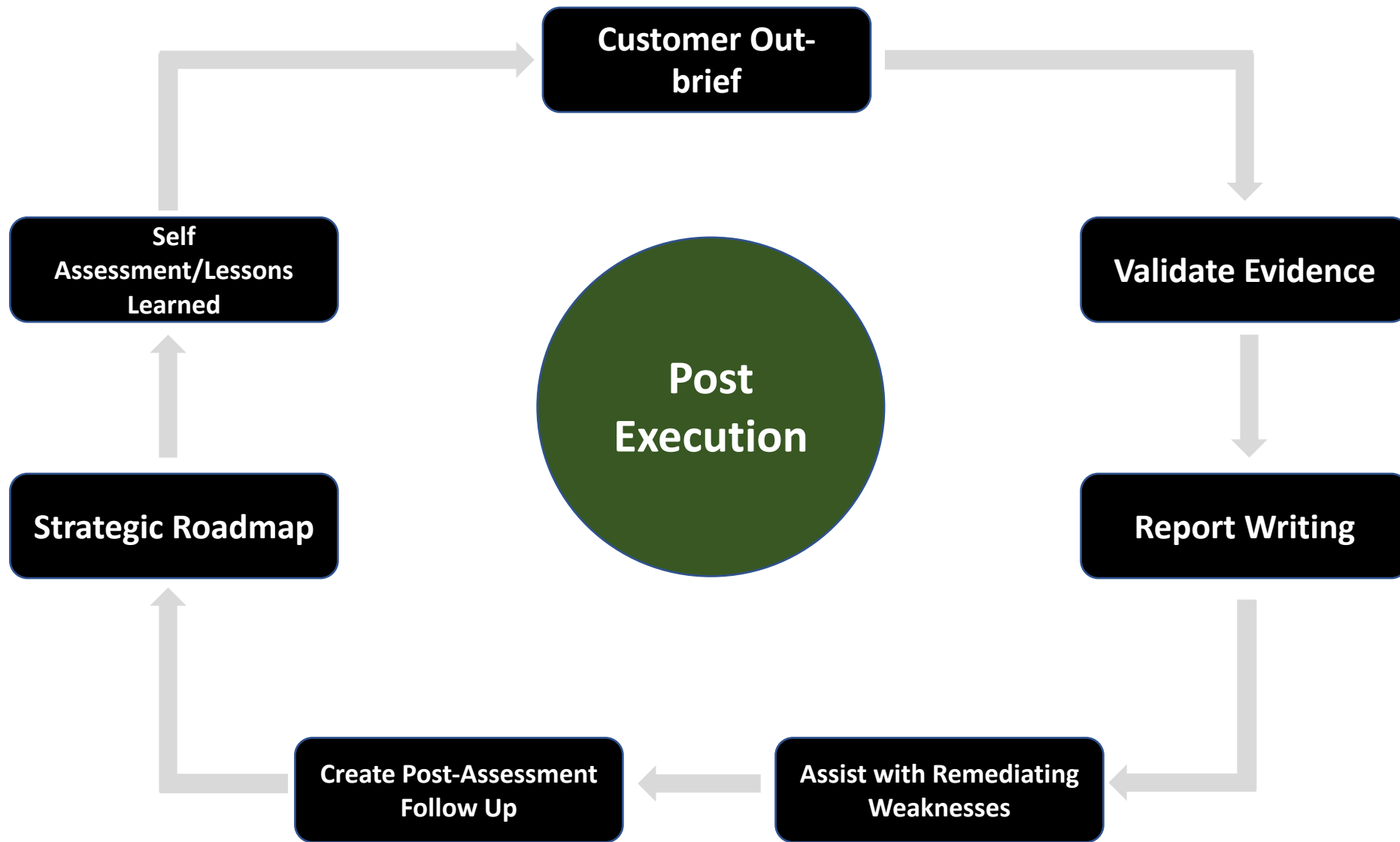
1110 Glebe Rd. Arlington, VA 22201

Prepared by

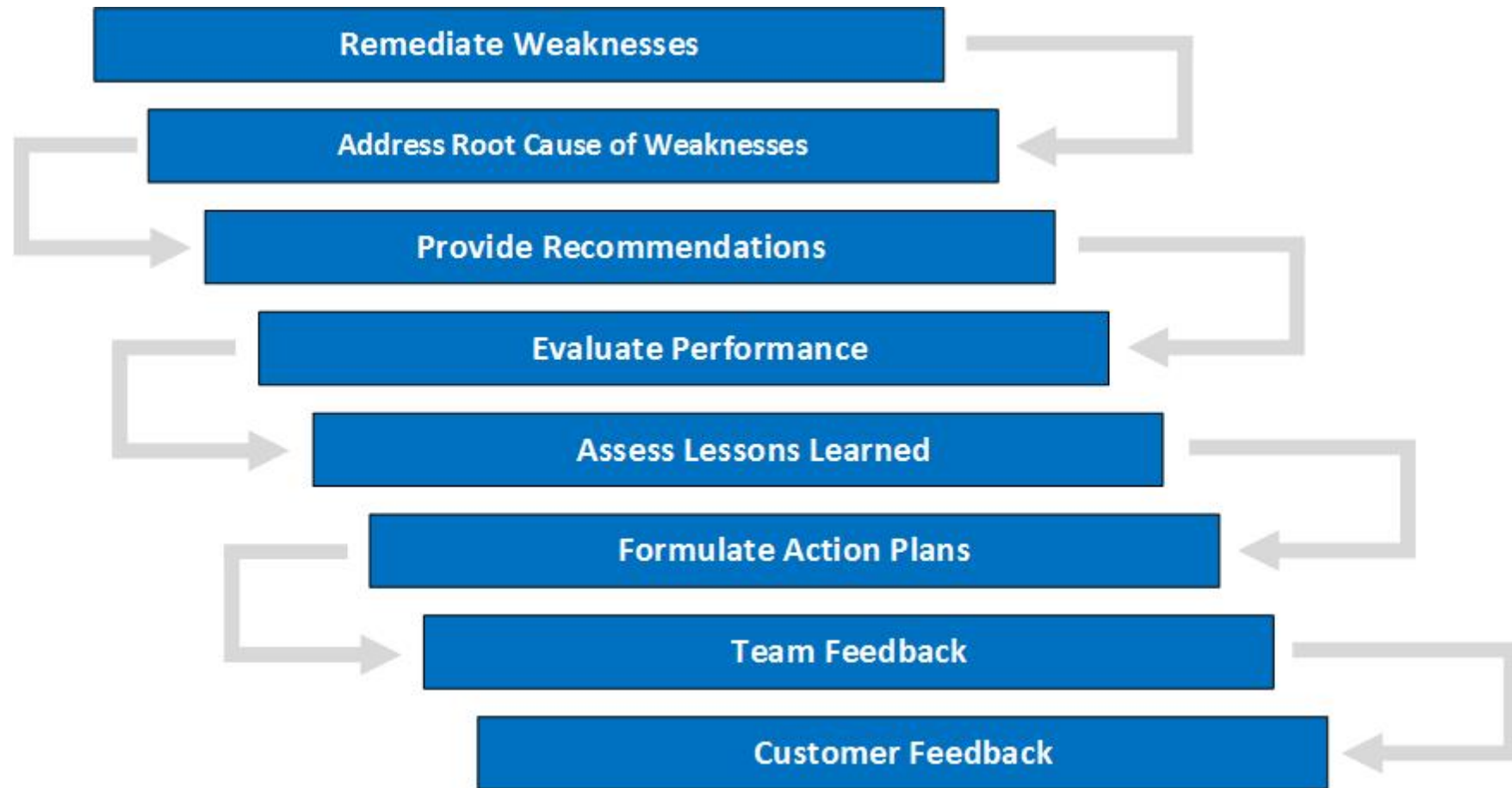
National Cybersecurity Assessment and Technical Services (NCATS)

September 30, 2014





Concluding and Reporting



Penetration Testing Guidelines and Frameworks

- NCATS Training and Qualification (TAQ)
- National Institute of Standards (NIST) 800-115
- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTIMM)
- Information Systems Security Assessment Framework (ISSAF)
- Open Web Application Security Project (OWASP)

NCATS Training and Qualification DRQP


The NCATS team provides a robust training and qualification (TAQ) program to federal departments and agencies encompassing the methodologies, processes, policies and procedures employed by the NCATS Risk and Vulnerability Assessment (RVA) program to conduct vulnerability scanning and penetration testing. As part of the training, candidates are required to complete the following activities:

- Candidate registration
- Sign and return registration documents
- Candidate pre-qualification evaluation


DHS-validated teams share non-attributional summary data and findings with NCATS in order to create trending across the federal government on systemic weakness and effective countermeasures

[2] Training

- Attend virtual classroom training

| Training Practicums | |
|--|--|
| <p>NCATS developed a series of technical, hands-on practicums to enhance an individual's technical skills in relation to the expertise necessary to conduct an RVA. Individuals are then evaluated against this set of technical training criteria during qualification.</p> |  |

ties on the

| Skills Range | |
|---|--|
| <p>NCATS built a virtual lab where candidates will apply their technical expertise through the RVA methodology in a simulated, corporate environment. Individuals and teams will be evaluated and tested on their ability to identify vulnerabilities, exploit attack</p> |  |

NCATS_INFO@hq.dhs.gov

[4] Activation

- Notification of surge force activation
- Commence assessment activities

Questions?