



Vulnerability Analysis and Operations (VAO)

Tony Sager

Chief, Vulnerability Analysis & Operations Group

Information Assurance Directorate

National Security Agency

July 2009



What We Do



- ***We Discover and Analyze*** vulnerabilities in...
 - in the core concepts of security
 - in emerging technologies and products
- ***We conduct operations to find vulnerabilities...***
 - in the operational environment (networking, signals, space...);
 - as revealed thru content
- ***We Translate*** vulnerability knowledge...
 - into summaries, trends, root cause.
- ***We Lead*** the Community...
 - in the improvement of security practice;
 - in guidance, training, education, and standards development.



■ ***We're VERY public***

- (Press) FCW/GCN, WTOP, Washington Post, SC Magazine, Information Week, Government Executive, etc.....
- (Presentation) Blackhat/DEFCON, RSA, Lumension 360, IAWS, SC Forum, ITSEF, CISO, SANS
- (Awards) SC Magazine, Fed 100, GovExec, SANS

■ ***We create and give away LOTS of great content***

- VAO Folders
 - 3750+ given out
- Security Configuration Guides
 - 75+ created and posted
 - 7 more in development



Stakeholders in Assurance



Authorities

Suppliers

Buyers

Users

Practitioners



Stakeholders in Assurance



***DoD Policy, OMB, FISMA,
Security Automation Program***

Authorities

***OS Vendors, Tool Vendors,
Compliance Checklists***

Suppliers

Buyers

***Air Force, DoD,
Standard Desktop Load***

Users

***DISA STIGs, NIST Checklists,
Corporate baselines***

Practitioners

***NSA, DISA, NIST, SANS,
Center for Internet Security***



Integrated Analysis & Reporting

Security “Sampling”

**Community events, tools, standards,
reporting, lessons, ...**

**Red
Team**

**Blue
Team**

OPSEC

**COMSEC
Monitoring**

TechSec



Vulnerability "Plumbing"



"CONTENT"

Security Guides
& benchmarks

Red/Blue Reports

Product tests

IT asset info

Security events

Incident reports

"PLUMBING"

CVE

OVAL

CCE

CPE

CVSS

XCCDF

"FIXTURES"

Net Management
tools

Integrated reports

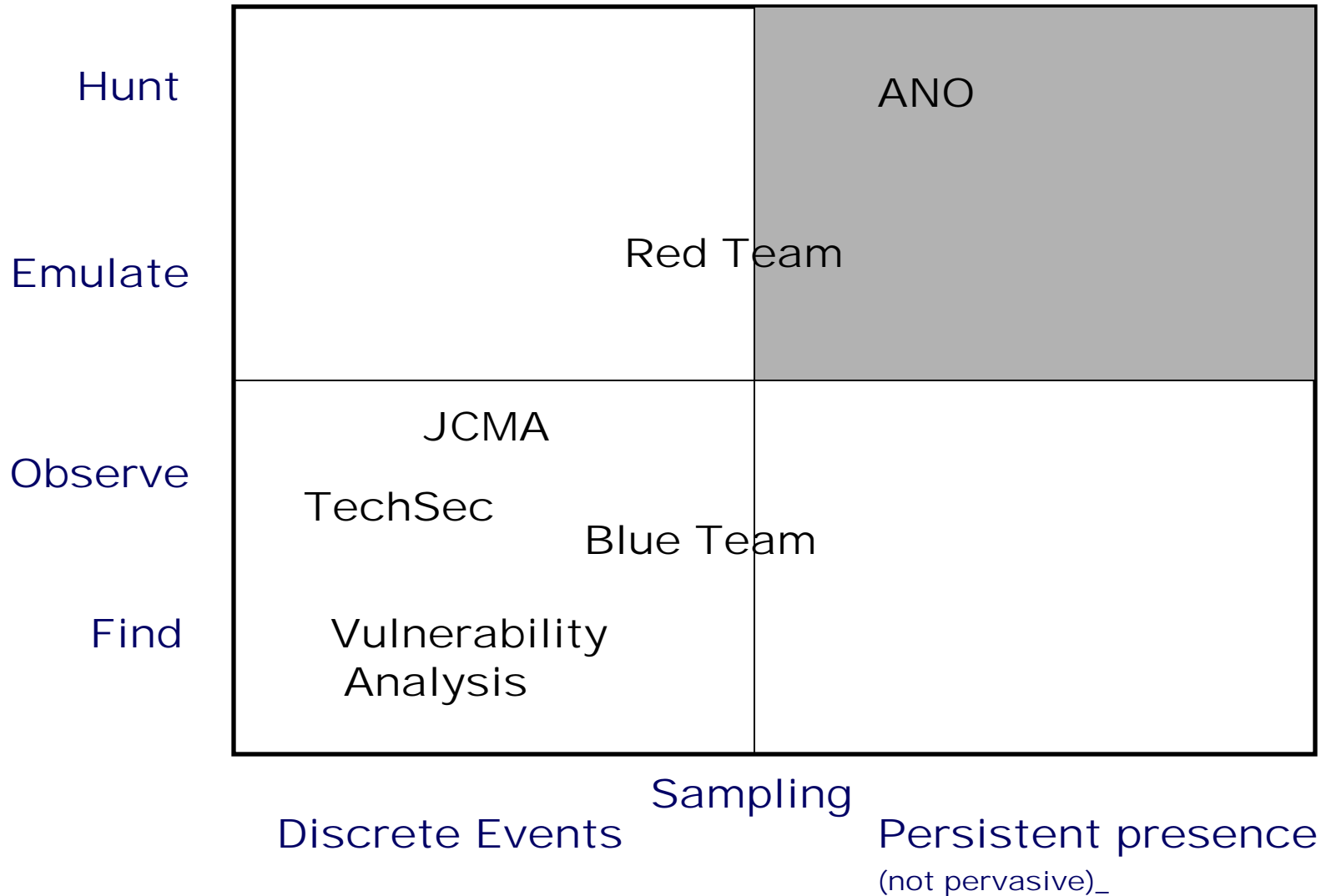
Integrated tools

Policy compliance

Rapid sharing,
assessment,
remediation



Full Spectrum Operations





To learn more...



- ***NSA Security Guidance***
 - <http://www.nsa.gov/snac/>
- ***The National Vulnerability Database, Security Content Automation Protocols, etc.***
 - <http://nvd.nist.gov/home.cfm>
- ***Common Vulnerability & Exposures***
 - <http://cve.mitre.org>
- ***The Center for Internet Security***
 - <http://cisecurity.org>