Defense Advanced Research Projects Agency

Information Assurance and Survivability Operational Experimentation (OPX)

Phoenix Challenge 2002

Brian Witten

OPX Program Manager

bwitten@darpa.mil

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
22-04-2002	Briefing	xx-xx-2002 to xx-xx-2002

4. TITLE AND SUBTITLE
Information Assurance and Survivability Operational Experimentation (OPX)
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Witten, Brian ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
DARPA
xxxxx, xxxxxxx

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
DARPA
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See report.

15. SUBJECT TERMS
IATAC Collection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	17	email from Booz, Allen & Hamilton (IATAC), (blank) lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/22/2002	Briefing 4/22/2002

4. TITLE AND SUBTITLE
Information Assurance and Survivability Operational Experimentation (OPX)

5. FUNDING NUMBERS

6. AUTHOR(S)
Witten, Brian

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

DARPA

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Advanced Projects Research Agency

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

This briefing was presented during the Phoenix Challenge 2002 Conference and Warfighter Day.

14. SUBJECT TERMS
IATAC Collection, information assurance

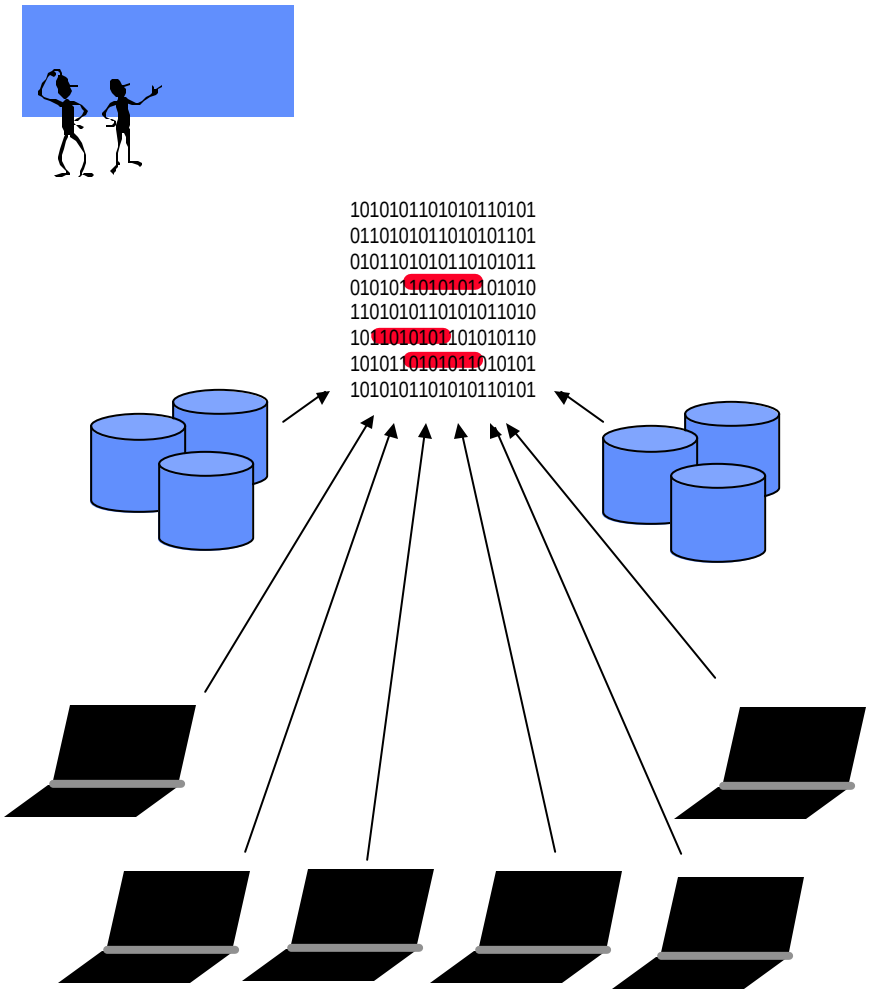
15. NUMBER OF PAGES

16

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Vision



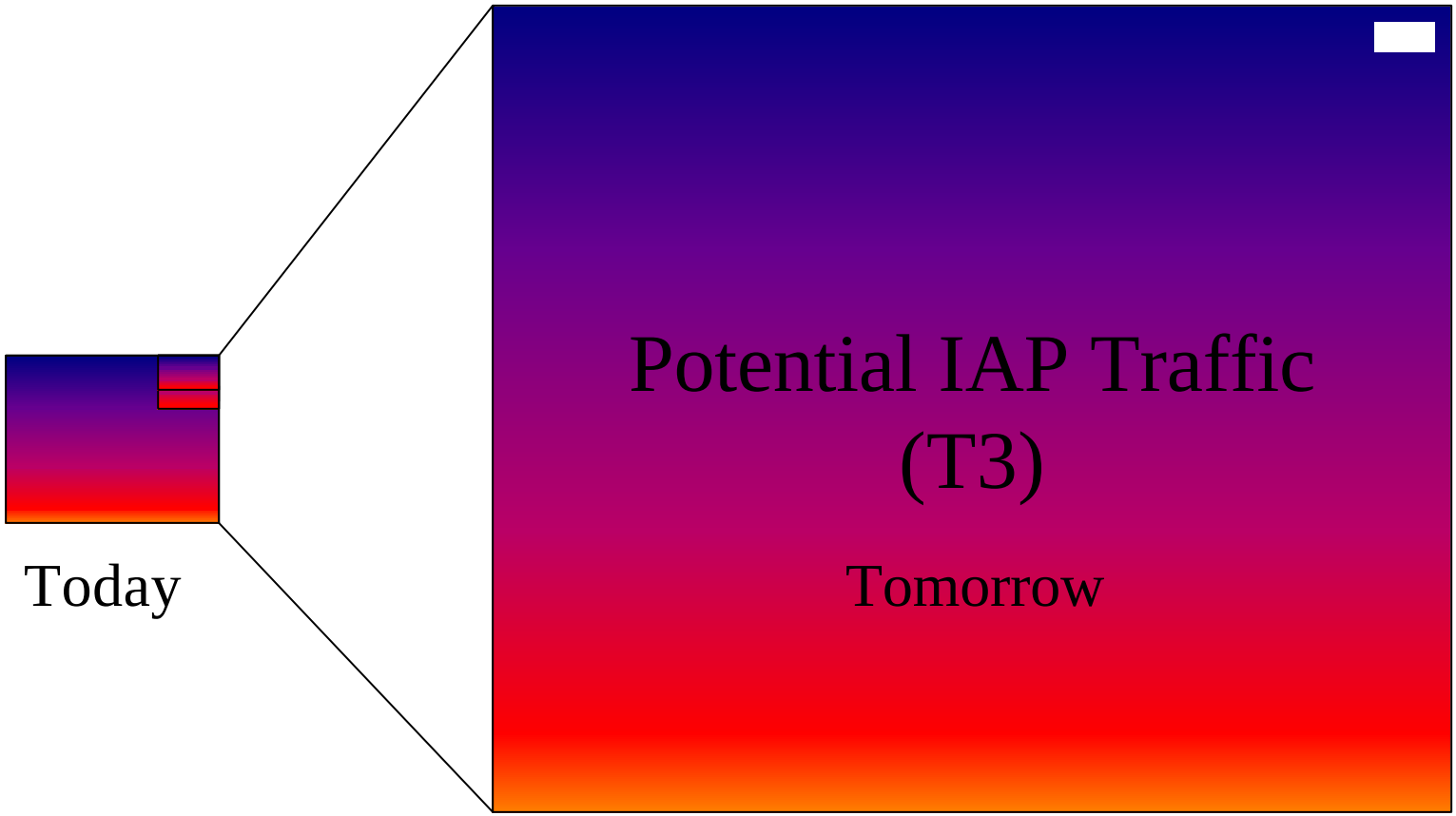
- New Capability:
  Situational Awareness
- Reduce Overload:
  Analyst Workbench
- Protect Centers of Gravity:
  Survivable Servers
- Pervasive Sensors:
  Hardened Clients

Strategy

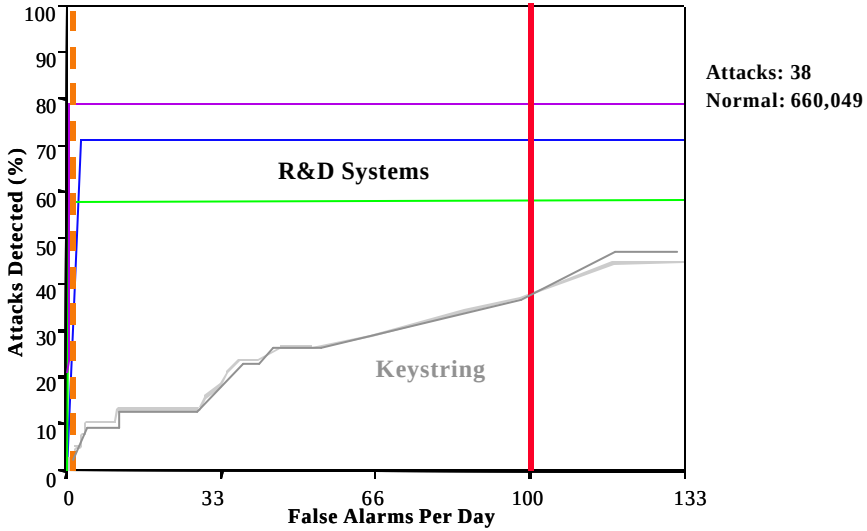
- **Objectives:**
  - Accelerate transition of effective technologies
  - Inform research agenda with operational experience
- **Key Experimentation Risks, Transition Metrics:**
  - Limited operational staff time
  - Impact on operational systems
- **Approach:**
  - Leverage mature research, well tested in lab
  - Field cautiously: walk before we run

The Analyst's Challenge

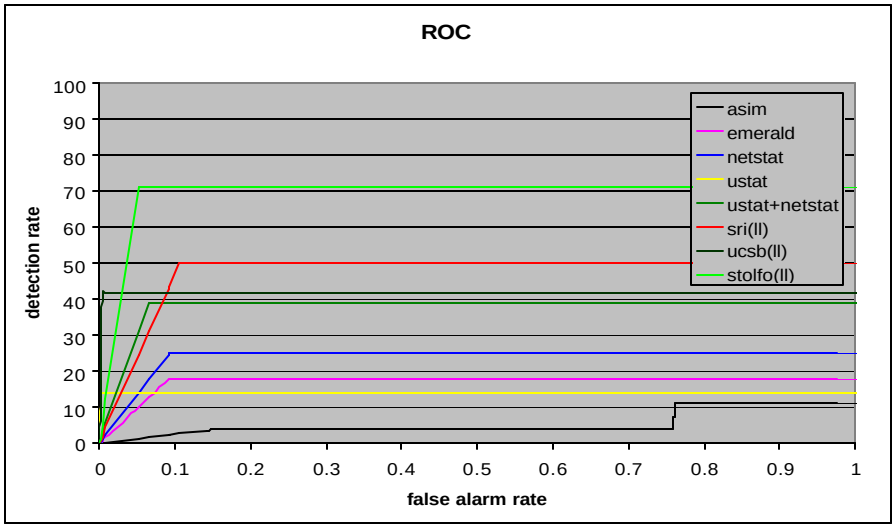
Impact of Transition to T3 volume at Internet Access Points



Intrusion Detection in the Lab



Attacks: 38
Normal: 660,049



DARPA 1998 Results (MIT/LL and AFRL)

- **Operational sensors:**
  - Hundreds of false alarms per attack
  - Actually miss most attacks
- **Research sensors:**
  - Dramatically reduce false alarm rates
  - Substantially improve detection coverage

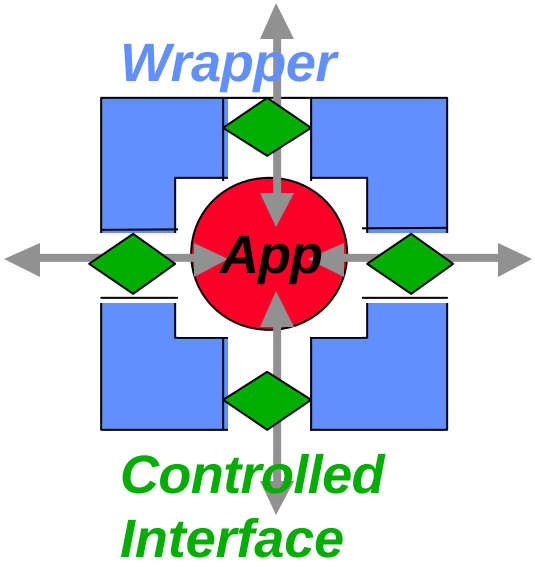
Analyst Workbench

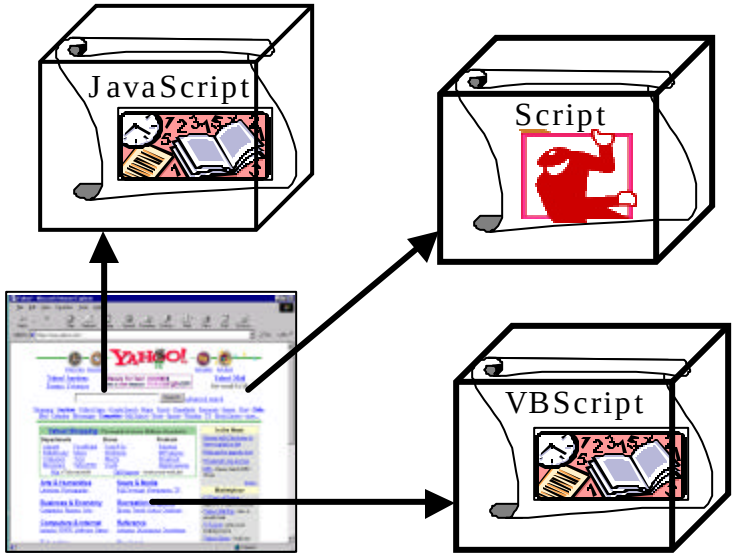
- Analysts currently overwhelmed
  - Flood of data, high false alarm, low detection rates
  - Not… real time, decision quality, always actionable
- DARPA Algorithms
  - Over a dozen lab tested real time algorithms
  - Data mining, anomaly, self organizing, expert systems
- Execution: September 2001 – September 2002

Hardened Client

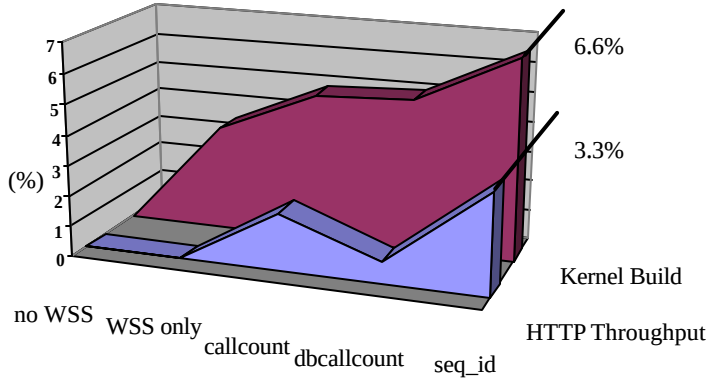
- MARFORPAC Challenge
  - Classic SIPR/NIPR PC problem
  - Compounded by TAD laptop theft
  - Insider threat and unknown viruses
- Proposed Technology
  - Safe e-mail “wrappers” and encrypting file system
  - Autonomic Distributed Firewall
  - PGP Disk & Disk Eraser

Operating System Wrappers





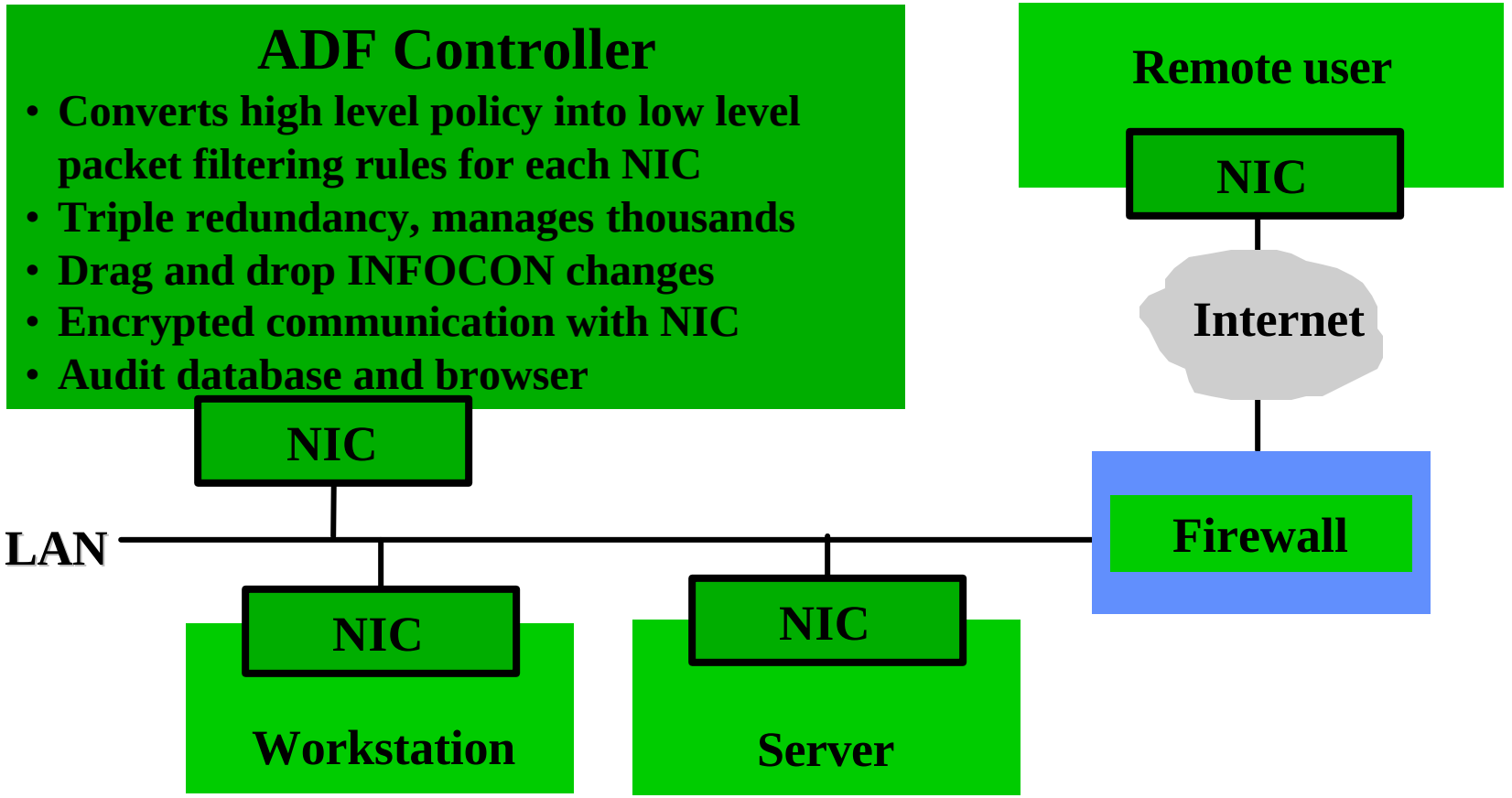
- Trap and stop unknown viruses
- Enable safer use of mobile code
- Performance impact: Low
- Availability: Solaris, Linux, NT, Win2K



Developers: Network Associates, Teknowledge, Cigital, Telcordia

Autonomic Distributed Firewall

- Firewall on Network Interface Card (NIC)
- Hardware based cryptographic accelerator
- Trustworthy control of untrustworthy OS



Made by Secure Computing and 3Com

Research performed under DARPA sponsorship

Hardened Client Timeline

- MARFORPAC Limited Objective Experiment
  - Apply safe e-mail wrappers and encrypting file system
  - MARFORPAC approved internal experiment charter
  - Execution: Late CY2001, RSO&I 02, UFL 02
- Fleet Battle Experiment India (C3F)
  - Execution: Jun 2001 – Autonomic Distributed Firewall (PCI)
- Fleet Battle Experiment Juliet Goals (PACFLT)
  - Complete application of diverse wrappers
  - Autonomic Distributed Firewall (PCMCIA)

Survivable Server

- **Motivating factors:**
  - High-value and commonly targeted center of gravity
  - Need Intrusion Tolerant Systems:

    Ability to confidently execute mission while under attack
  - Reactive defense not adequate
- **Possible technologies:**
  - PASIS: Perpetually Available Survivable Information System

    Leverage fragmentation, redundancy, and scattering
  - SELinux, Immunix, Emerald, NetTop Vmware, Wrappers
- **Execution: 2002**

Situational Awareness

- **Am I under attack ?**
- **What is the nature of the attack ?**
  - Class, mechanism, and source
- **What is mission impact ?**
  - Urgency, damage assessment and control, initial response
- **When did attack start ?**
  - More detailed damage assessment. What have I done wrong ?
- **Who is attacking?**
  - What are they trying to do? What is their next step ?
- **What can I do about it ?**
  - Course of action analysis, collateral damage risk, reversibility

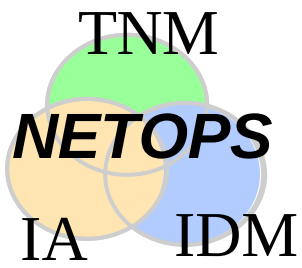
Theater C4I Coordination Center PACOM TCCC

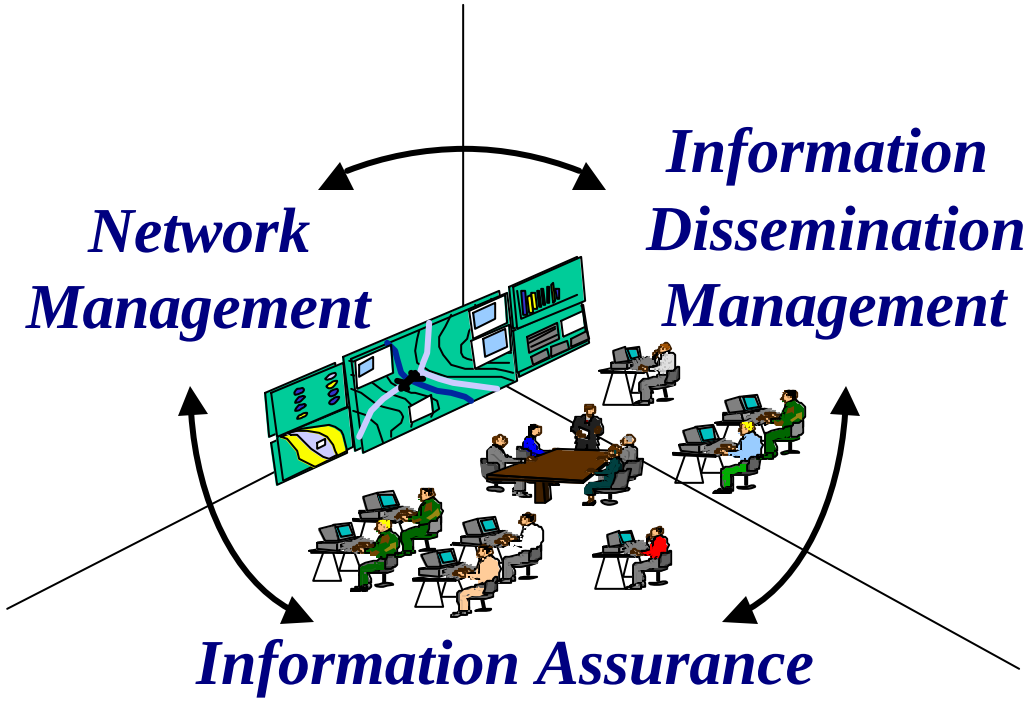
Need

- ***Theater Wide***
- ***Real Time***
- ***Decision Quality***
- ***Actionable Information***

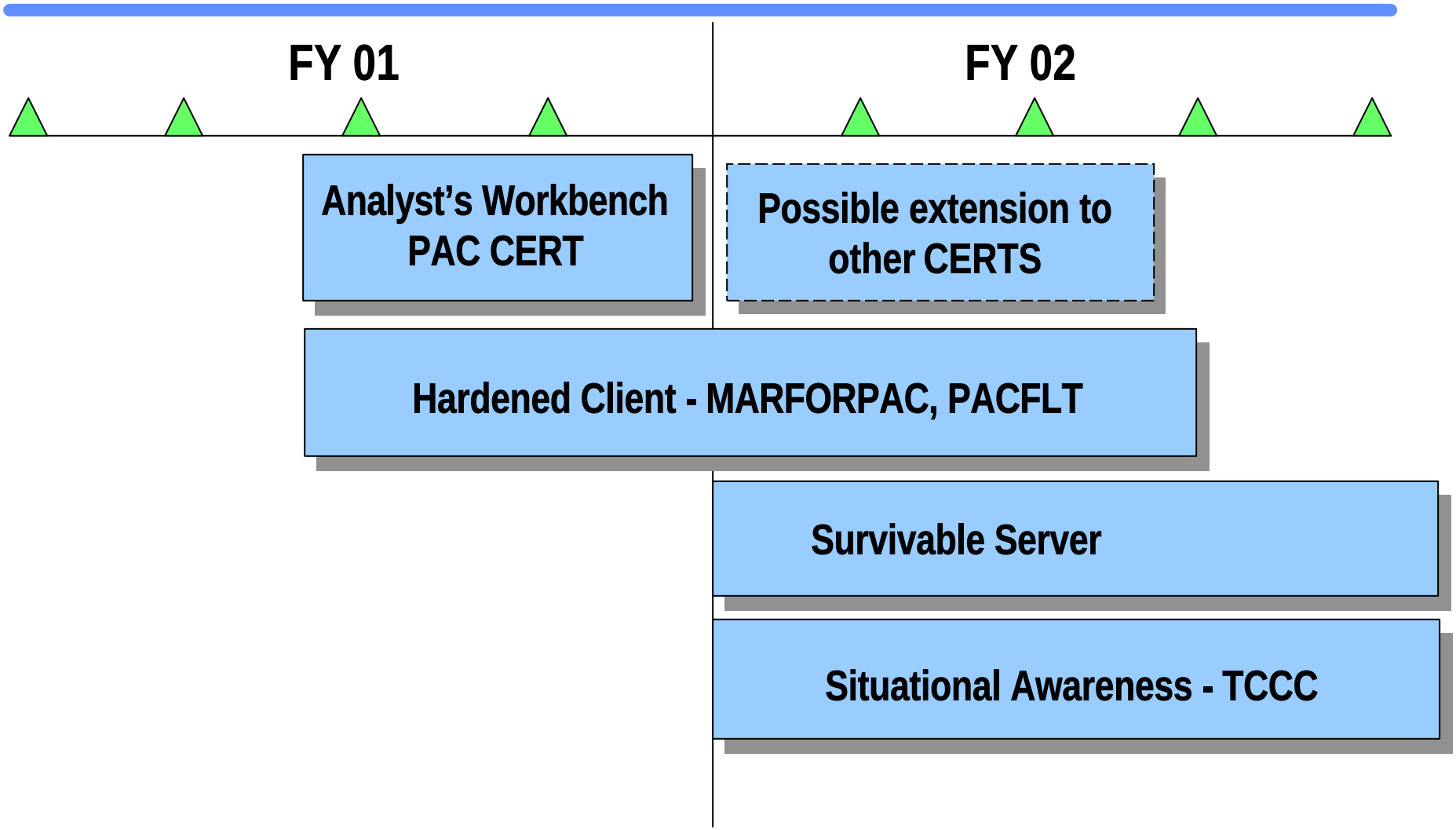
Strategy

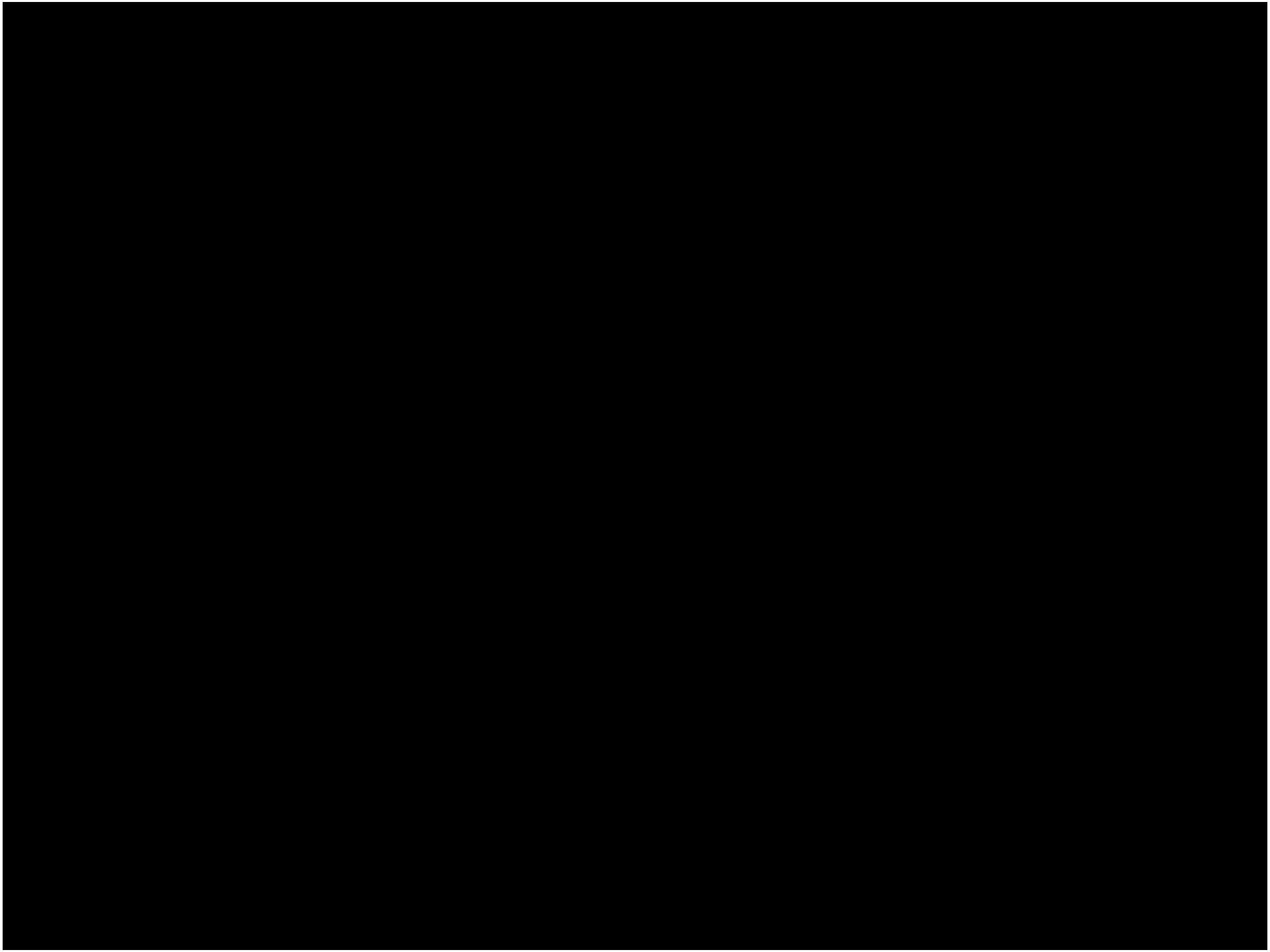
- **Leverage Cyber Panel emerging research**



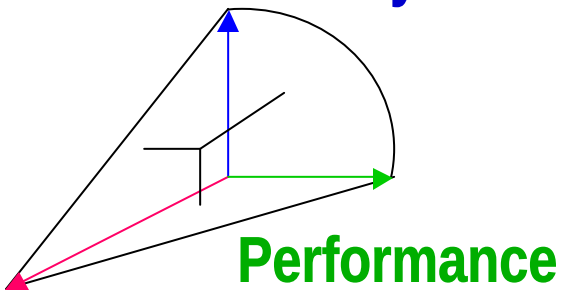


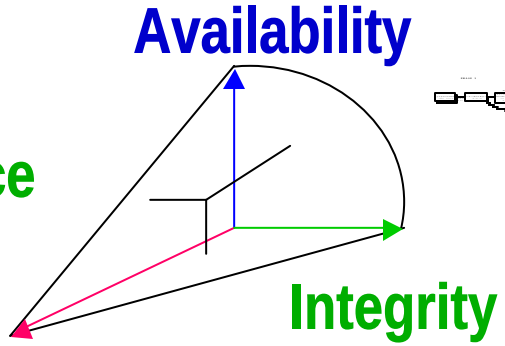
Summary


FY 01
FY 02
Analyst's Workbench
PAC CERT
Possible extension to
other CERTS
Hardened Client - MARFORPAC, PACFLT
Survivable Server
Situational Awareness - TCCC

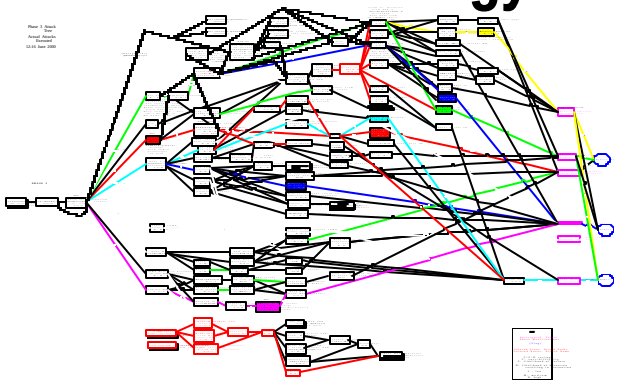


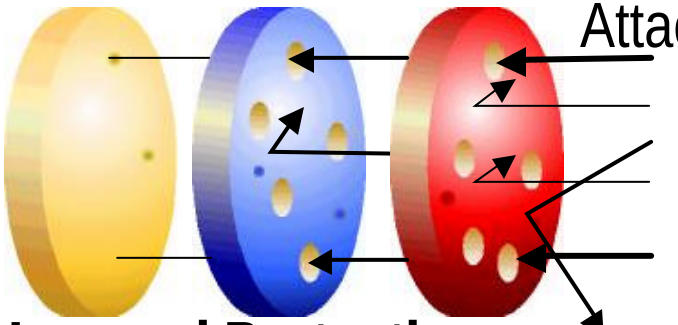
Context



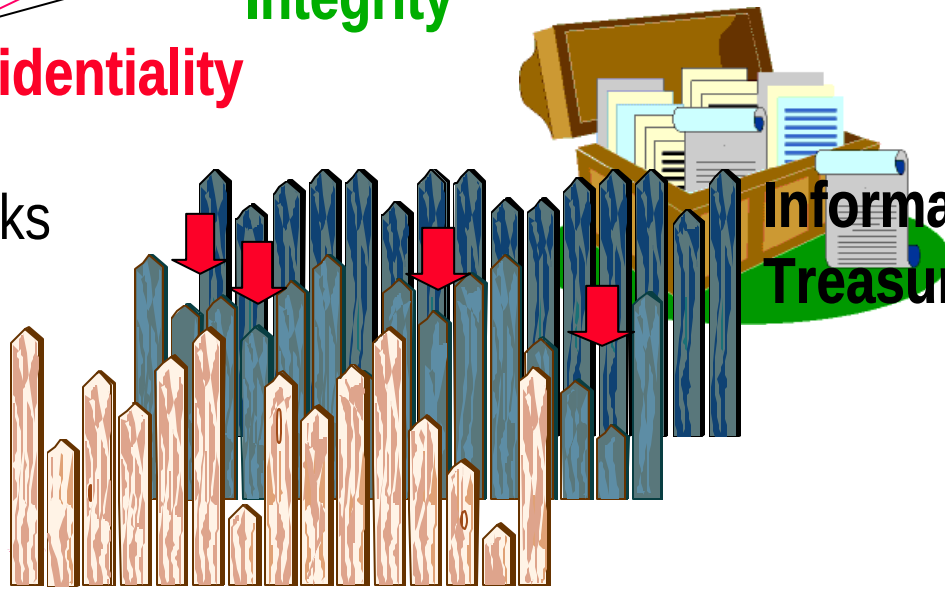


Methodology





Layered Protection
Dynamic Defense



Risk-Balanced Optimizing Strategy