Infrastructure Defense Inc.

a company built on trust™

Matthew G. Devost

Director of Intelligence Analysis

(703) 914-7113 Voice
(703) 914-7100 Fax
mdevost@idefense.com
http://www.idefense.com

Matthew G. Devost
mdevost@idefense.com

CVAT

Coalition Vulnerability Analysis Team

- First ever international VA Team included US, UK, NATO, Canada, Australia, and New Zealand
- Spawned significant security initiatives within member countries
- Identified as an operational requirement for all Coalition Networks

Technical Lead - CINC DIO Review

- Solutions-based security review

Matthew G. Devost
mdevost@idefense.com

Vulnerability Assessment v. Red Teaming

Vulnerability Assessment

- Review of security posture as part of Risk Management process
- Results reviewed with security department
- Solutions implemented as a result

Red Teaming

- Act as the enemy to exploit vulnerabilities to fullest extent possible
- Give perspective to threat of an information attack

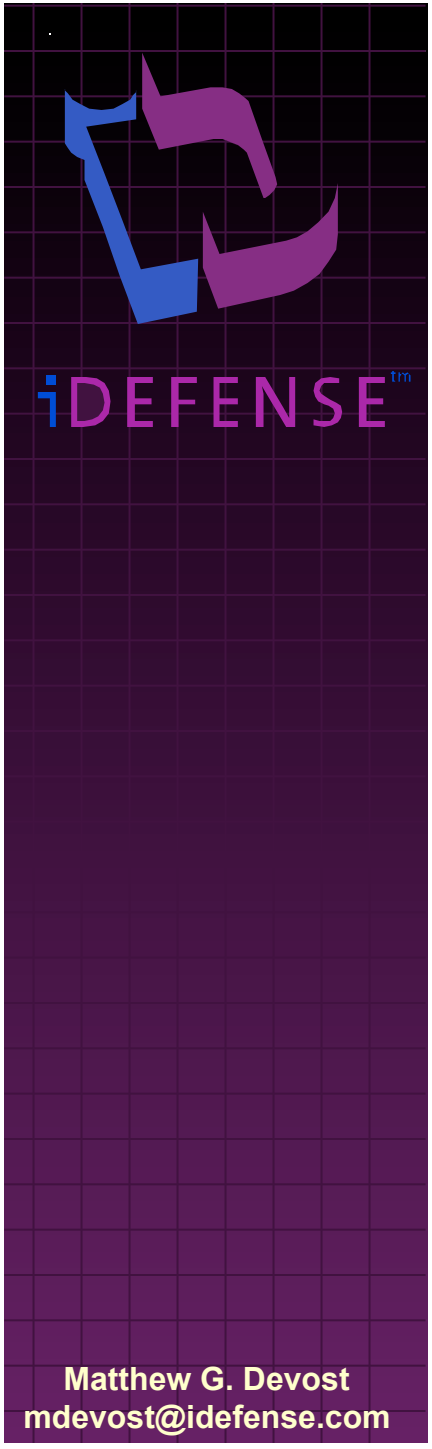
Matthew G. Devost
mdevost@idefense.com

Developing a Common Terminology

Vulnerability Assessment:

- Regular component of security procedures and risk management process
- Evaluate vulnerabilities through VA
- Evaluate safeguards
- Anticipate threat
- Make resource allocation decision

Matthew G. Devost
mdevost@idefense.com

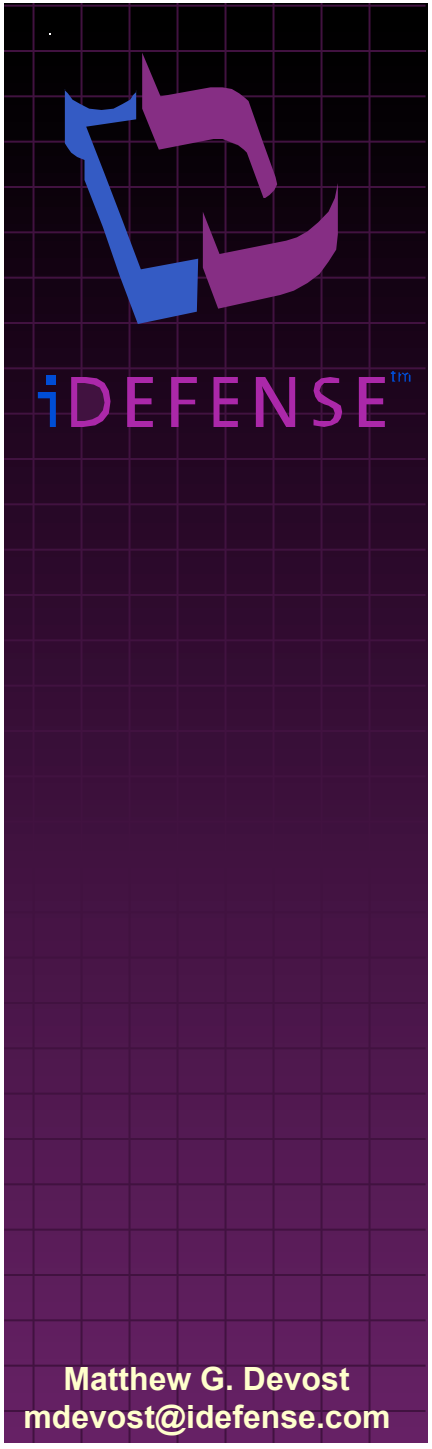


Developing a Common Terminology (II)

Red Teaming:

- Exploitation of vulnerability chains from a threat perspective
- Combine INFOSEC vulnerabilities with physical and personnel (social engineering) vulnerabilities
- Demonstrates the true implication of known vulnerabilities to senior leaders/ management

Matthew G. Devost
mdevost@idefense.com



Vulnerability Assessment An Example

Coalition Vulnerability Assessment Team (CVAT) for Joint Warrior Interoperability Demonstration

Vulnerability assessment reveals low to medium level vulnerabilities

Results and recommendations provided to security managers

Move on to the next system

Matthew G. Devost
mdevost@idefense.com

Red Teaming
An Example

Target same system, but from threat perspective

Scan reveals same low and medium level vulnerabilities…but now…

- **Vulnerability exploited to get registry settings to include usernames**
- **Research open sources to determine password qualifiers**
- **Run password cracking routine with new qualifiers**

Matthew G. Devost
mdevost@idefense.com

Red Teaming
An Example (II)

End Result -

Complete access to Command Center workstation

Time from start to finish - 2.5 hours

Red Team exploits the full vulnerability chain to give threat perspective

Matthew G. Devost
mdevost@idefense.com

"The attackers used tools and techniques readily available on Internet hacker bulletin boards," Minihan said. "Although these attacks were moderately disruptive, the good news is that the vulnerabilities exploited are relatively easily fixed."

- Minihan discussing Solar Sunrise.

Matthew G. Devost
mdevost@idefense.com

Convincing Others of the Benefits of VA

- Required component of Risk Management process within security program
- Most attacks exploit KNOWN vulnerabilities
- COTS and Freeware VA tools assist in checking your systems for known vulnerabilities

"Spending on network security worldwide this year will likely jump 53 percent from last year to $1.85 billion, according to DataQuest Inc. of San Jose, Calif. It is expected to grow to $2.98 billion next year and reach $5.18 billion by 2000."

- Government Computer News - 14 Dec 1999

Matthew G. Devost
mdevost@idefense.com

Convincing Others of the Benefits of VA (II)

Evaluate safeguards based on vulnerabilities addressed

- Determine payoffs for allocation of resources. (Where do you spend your money?)

Effective security is pro-active security. VA is proactive

- OMNCS study on incident costs

Intangibles:

Loss of human life.

Shareholder value

Public perception

Regulatory Compliance

Competitive Advantage

Legal Liability

-Source: OMNCS Report "Business Case Model for Information Security" 1997

Matthew G. Devost
mdevost@idefense.com

Convincing others of the Benefits of Red Teams

Substantiates the importance of vulnerability assessment by exploiting the vulnerability chain of the organization

Recognize the intangible benefits of information security

Useful as an IO Offensive Capability in required situations

Scoping the Red Team Activity

Use Realistic Threat Profile

- True outsider vs. insider
- Capabilities available through open sources
- Validate cross-over assumptions

Don't Play the Blame Game

- Work towards addressing deficiencies and problem areas. Team not responsible for implementing solutions.
- Determine which threats are valid and apply to risk management process

Matthew G. Devost
mdevost@idefense.com

Integrating the Whole Force

Impossible?

- Too many systems, stovepipes and lack of coherent standards
- VA a localized effort
- Red Teams can target the whole force

Integrate Red Teams into Exercises and War Games

Industry - Validate Security Posture with Outside Assessment

Utilize VA as a regular security tool!

Matthew G. Devost
mdevost@idefense.com

Determining the Effectiveness

Red Team Effectiveness

- Extent of success
- Changes reflected in security operations, policy and procedures?

VA Effectiveness

- Integration of results in Risk Management process
- Increased security posture through coordination with security administrators

Matthew G. Devost
mdevost@idefense.com

Conclusions

Vulnerability Assessment and Red Teaming are Vital Components of Information Security/ Critical Infrastructure Protection

Must move towards sharing information regarding vulnerabilities and incidents on a non-attribution basis. This builds trust! (forthcoming paper)

Matthew G. Devost
mdevost@idefense.com

iDEFENSE™

"In a closed briefing before Congress last summer, CIA head George Tenet warned that at least a dozen countries are working on information warfare programs intended to give them the capability to attack another nation's computer systems."

- www.abcnews.com

Matthew G. Devost
mdevost@idefense.com

What does a VA Team Look Like?

Front Row (left to right) USA, Australia, Germany, New Zealand, Canada, Back Row, Turkey, USA

iDEFENSE™

Left to Right

USA

Australia

Canada

New Zealand

USA

Canada

Canada

Matthew G. Devost
mdevost@idefense.com

Backup Slides

An innovation which JWID 97 is pushing hard this year is the use of a Coalition Vulnerability Analysis Team (or **CVAT**). The purpose of the **CVAT** is, through interacting with the demonstrations, to assess and improve the **security** posture and reduce the vulnerabilities of the various C4I systems.

- C4I-Pro News

Matthew G. Devost
mdevost@idefense.com

CVAT Underlying Objectives

Gain CWAN Security Vulnerability Knowledge

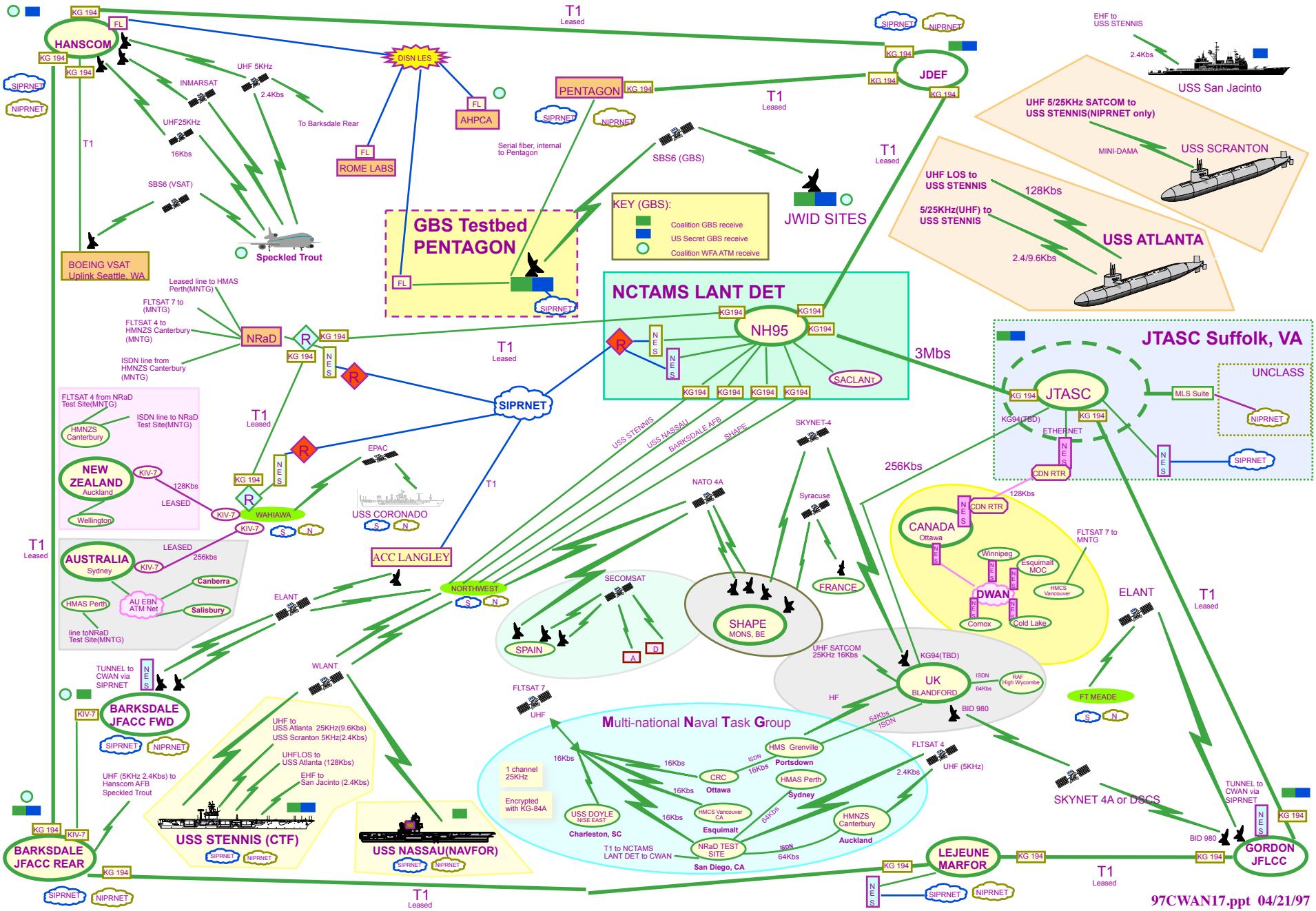
Recommend Security Improvements

Establish Procedures for Conducting Analysis and Sharing Information

Provide Information Operations Demonstration Stimulation

Provide Security Assessments of Demonstrations

JWID97 COALITION WIDE AREA NETWORK



CVAT Resources - Hardware

1 Sun IPX System - CVAT Website

2 Linux Laptops - VA Activities

1 NT Laptop - VA and Intrusion Detection

1 Sun Ultra2 - Network Mapping and VA Activities

1 Windows 98 Laptop - Unclassified reporting and internet access

Matthew G. Devost
mdevost@idefense.com

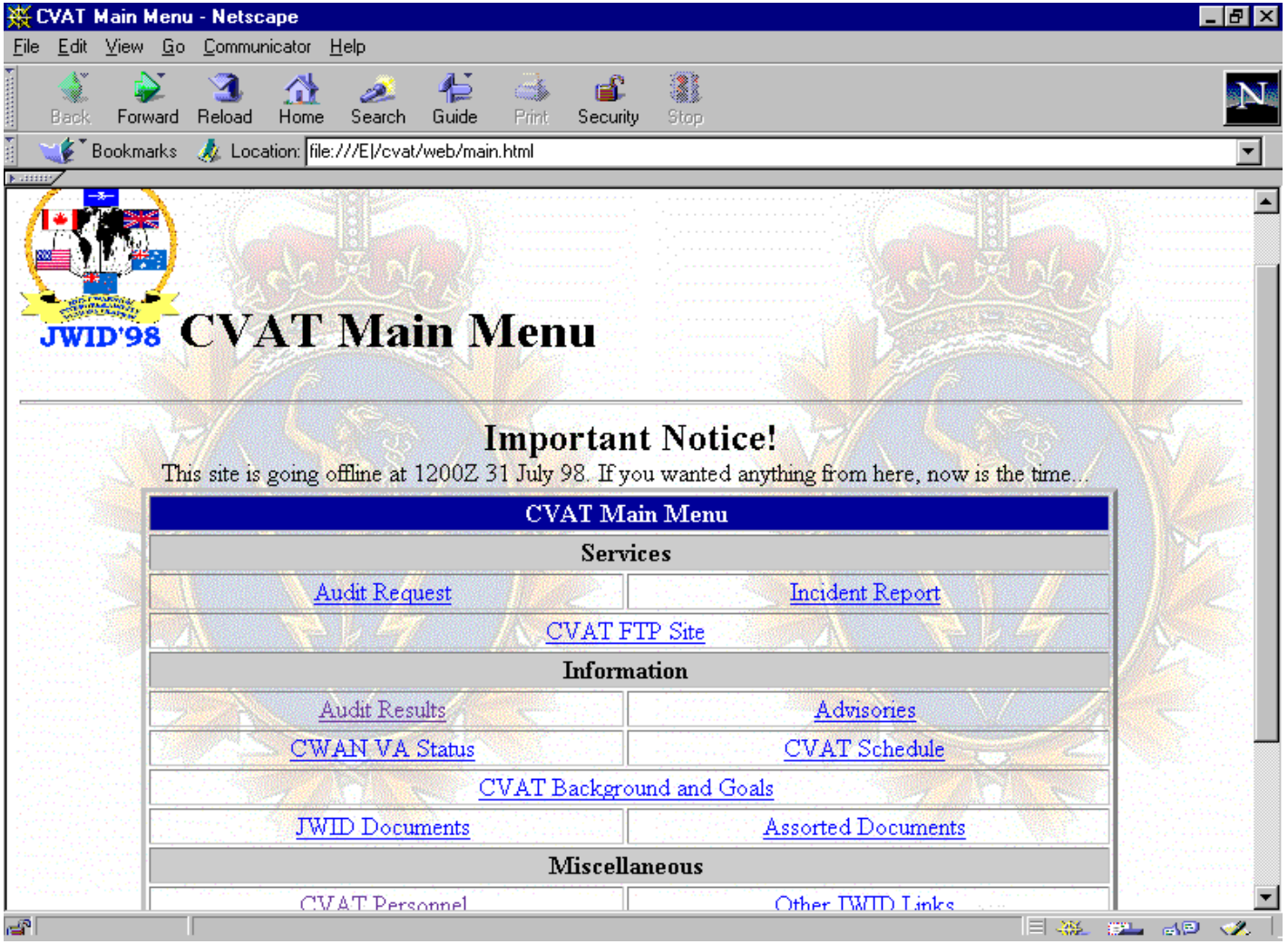
CVAT Resources - Software

Ballista Auditing Tool	VA Software
Internet Security Scanner	VA Software
Axent NetRecon	VA Software
SAINT	VA Software
DISA VTK GOTS	VA Software
TKInedE	Mapping
ISS RealSecure	Intr. Detect.

Combination of commercial off the shelf, GOTS, and Freeware tools establishes a significant VA capability.

Matthew G. Devost
mdevost@idefense.com

CVAT Website

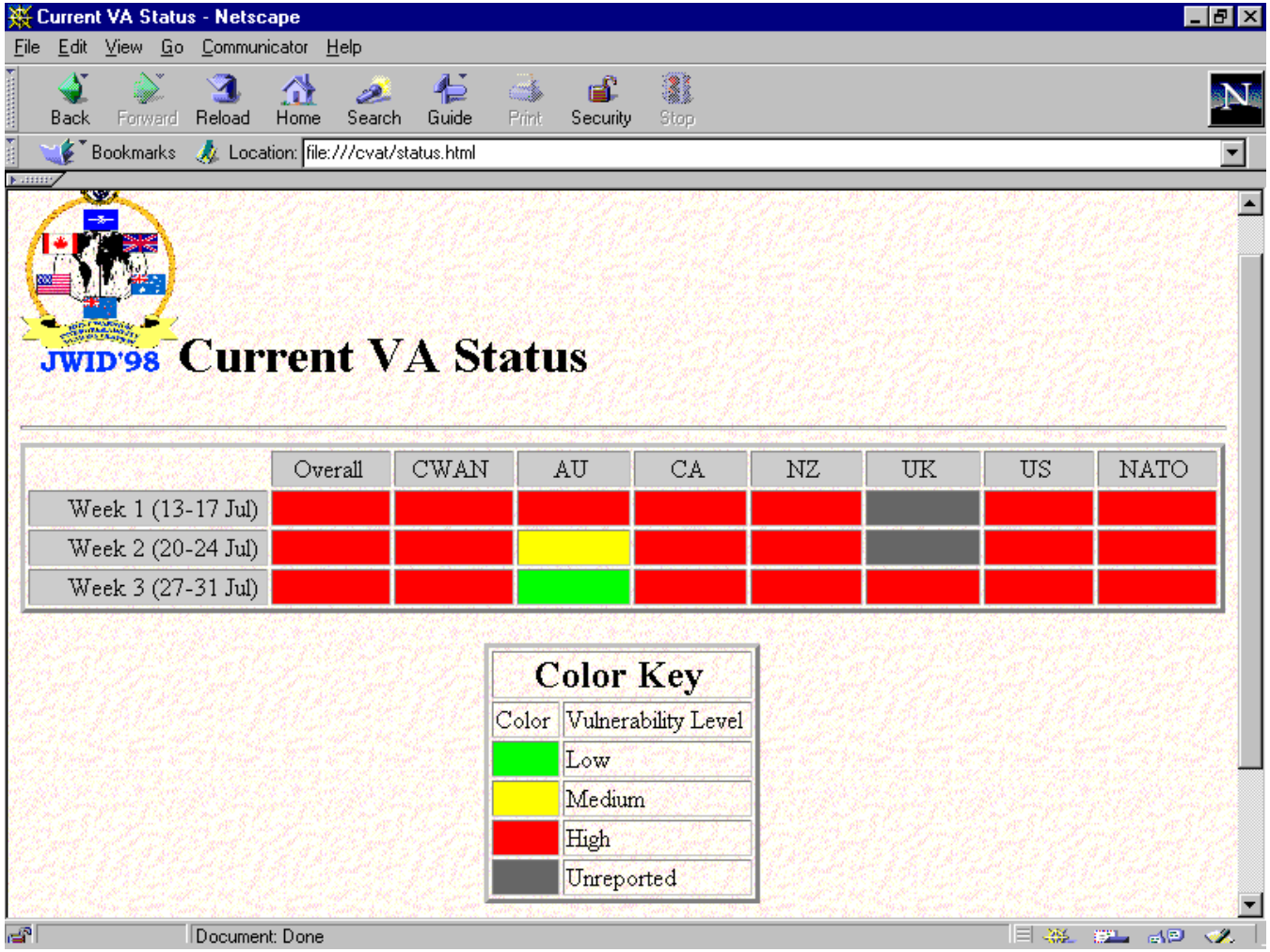


Matthew G. Devost
mdevost@idefense.com

CVAT Website II

iDEFENSE™

Shared Vulnerability Assessment results in a non attribution way. Specific results provided to systems administrators and national representatives only.



Matthew G. Devost
mdevost@idefense.com

No Network too Small or too Large...

Matthew G. Devost
mdevost@idefense.com