Information Assurance Update

29 Jan 99

Overview

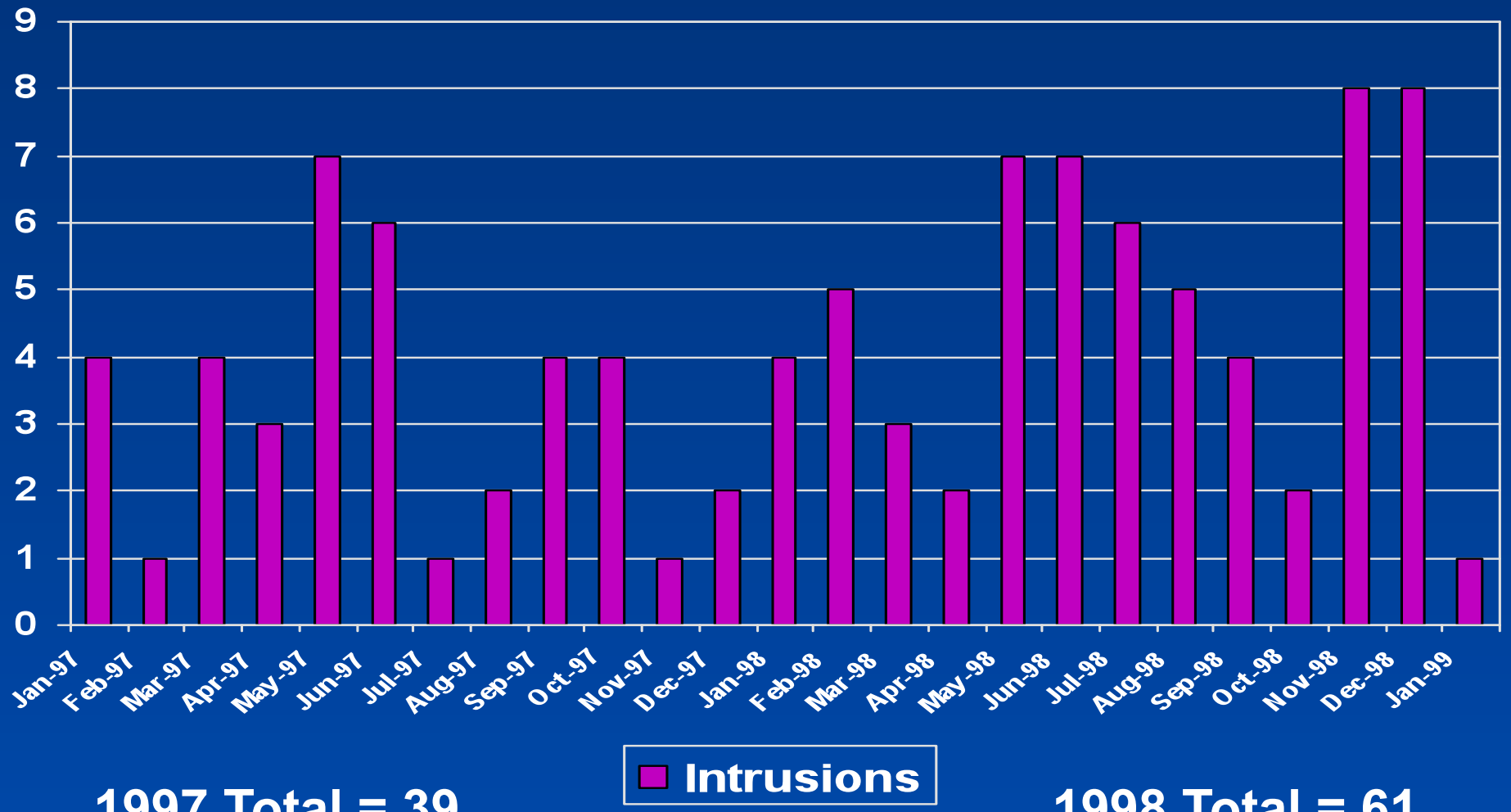
- Information Assurance (IA) Metrics
- Tightening Our Defenses
- Audits
- IG Special Interest Item
- IA Manpower
- Training & Certification
- Information Assurance Awareness Month
- Worldwide Web Security
- Defense Research Engineering Network (DREN)
- Public Key Infrastructure (PKI)

Metrics

- Intrusions
- Advisory Compliance

Intrusion Summary

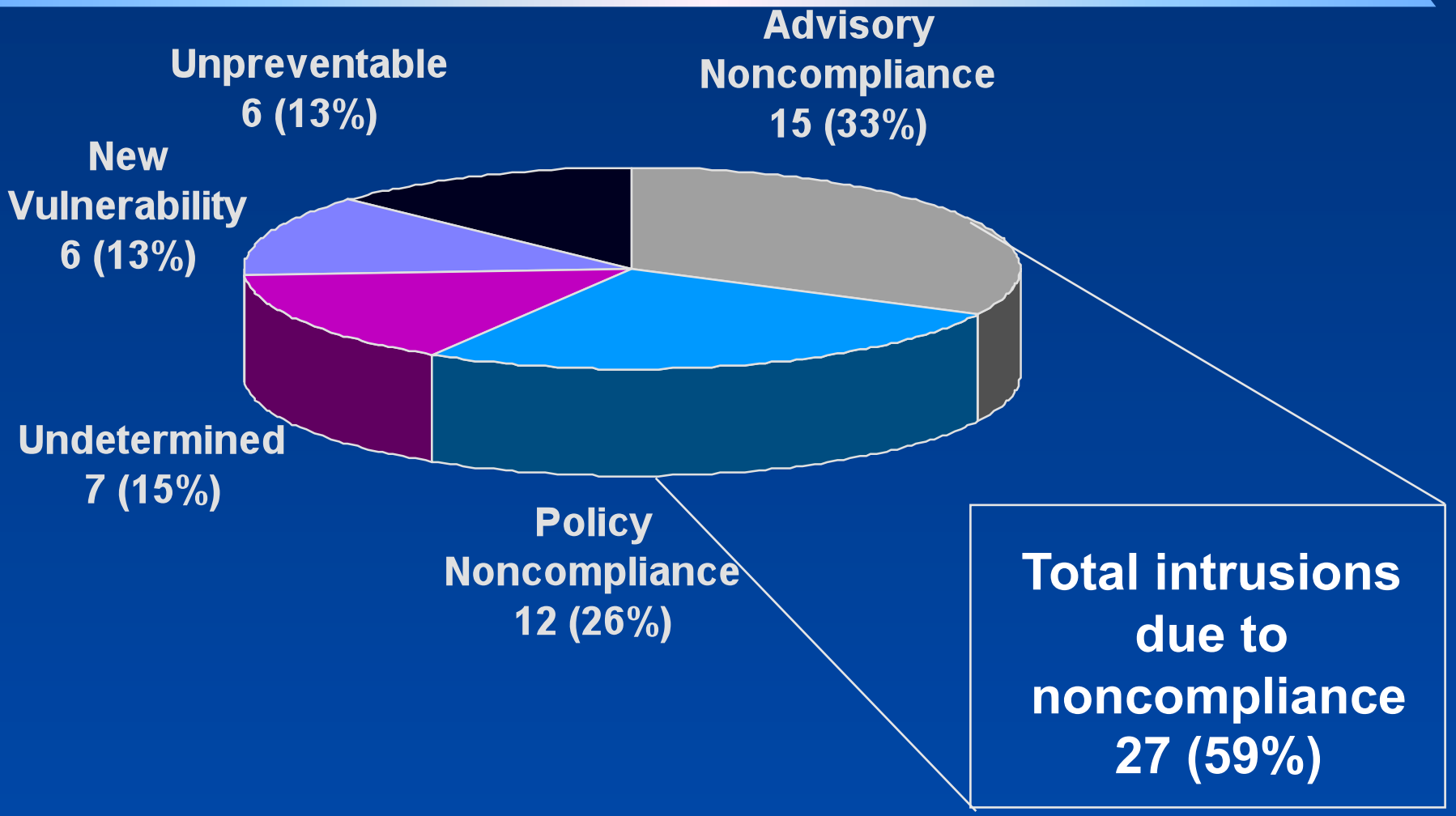
Unauthorized User or Root-level Access
Jan 97 - Jan 99



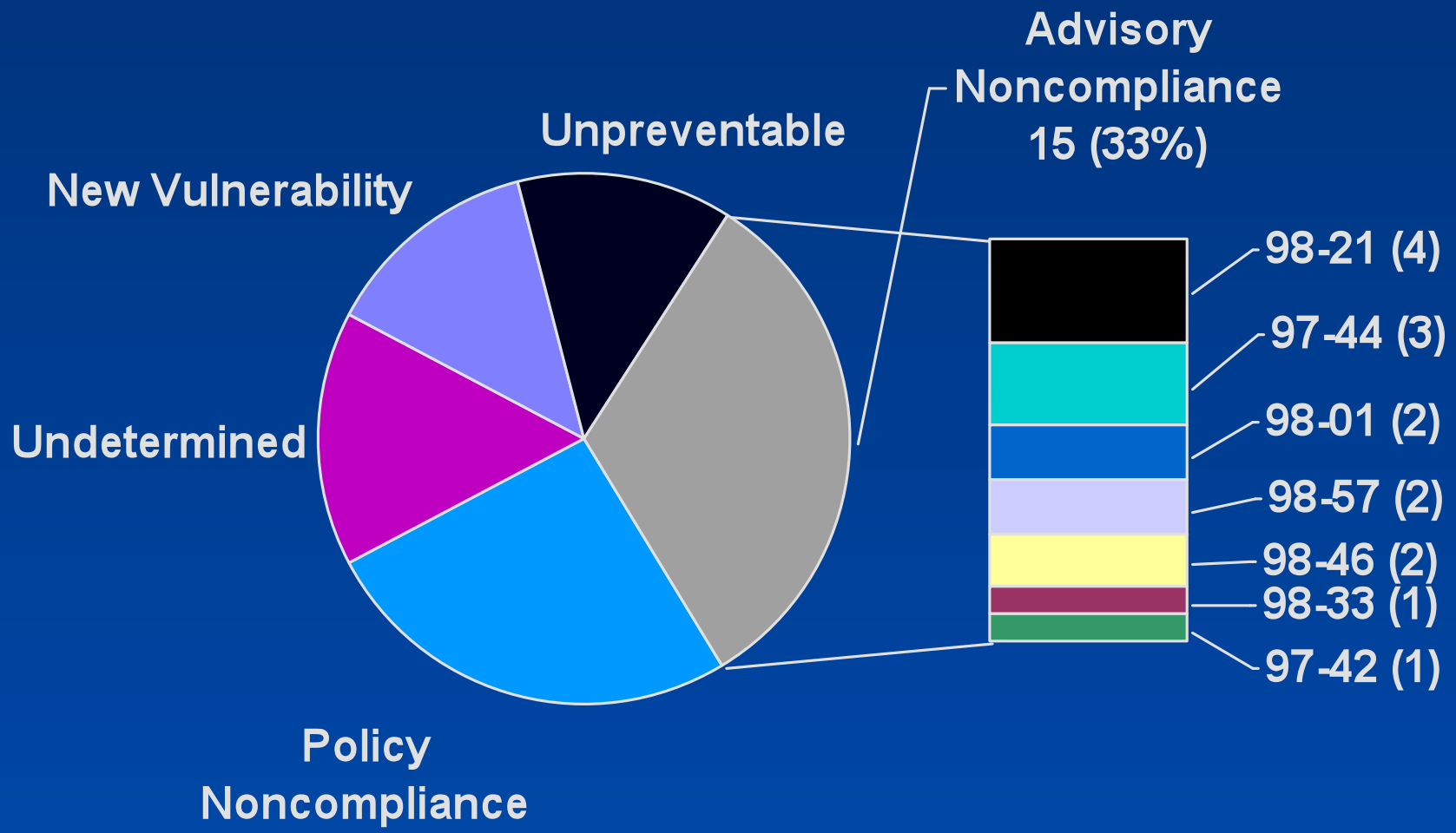
1997 Total = 39

1998 Total = 61

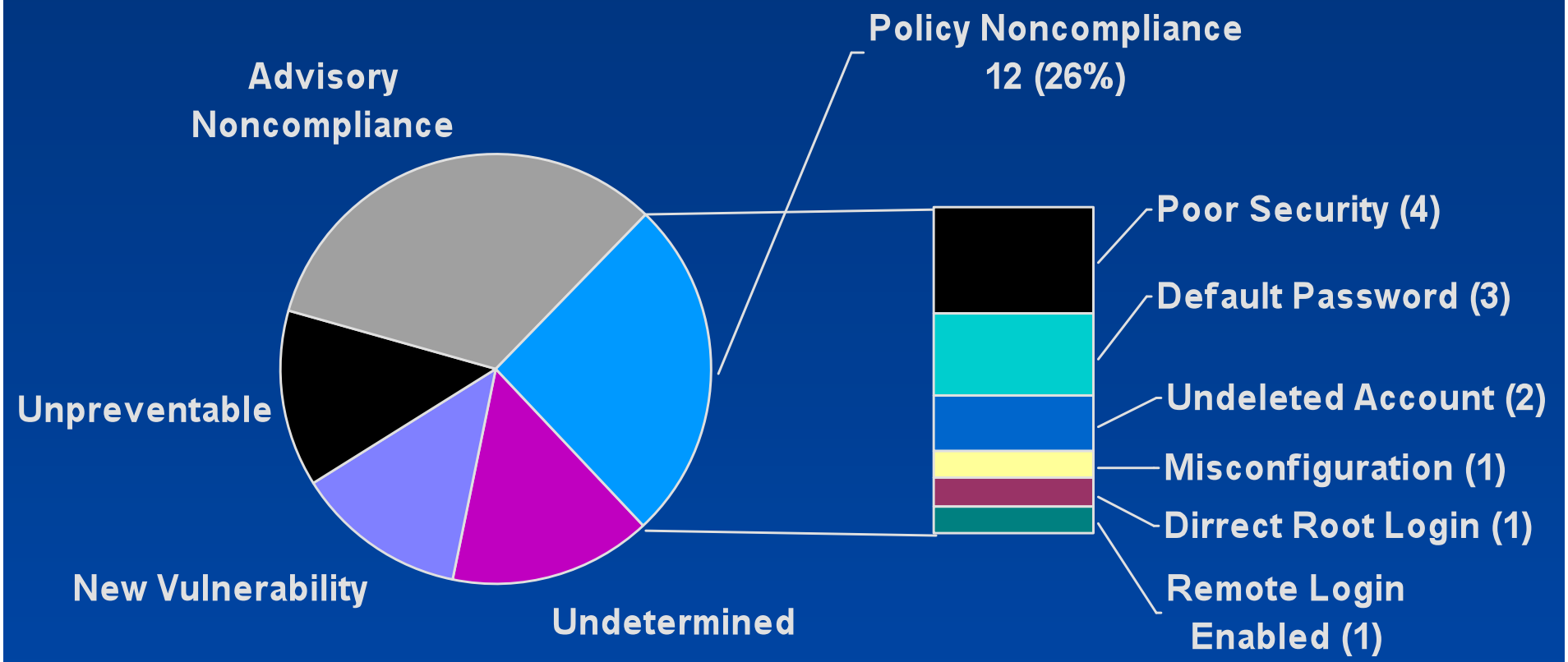
Root Intrusions
CY98 - 46 Total



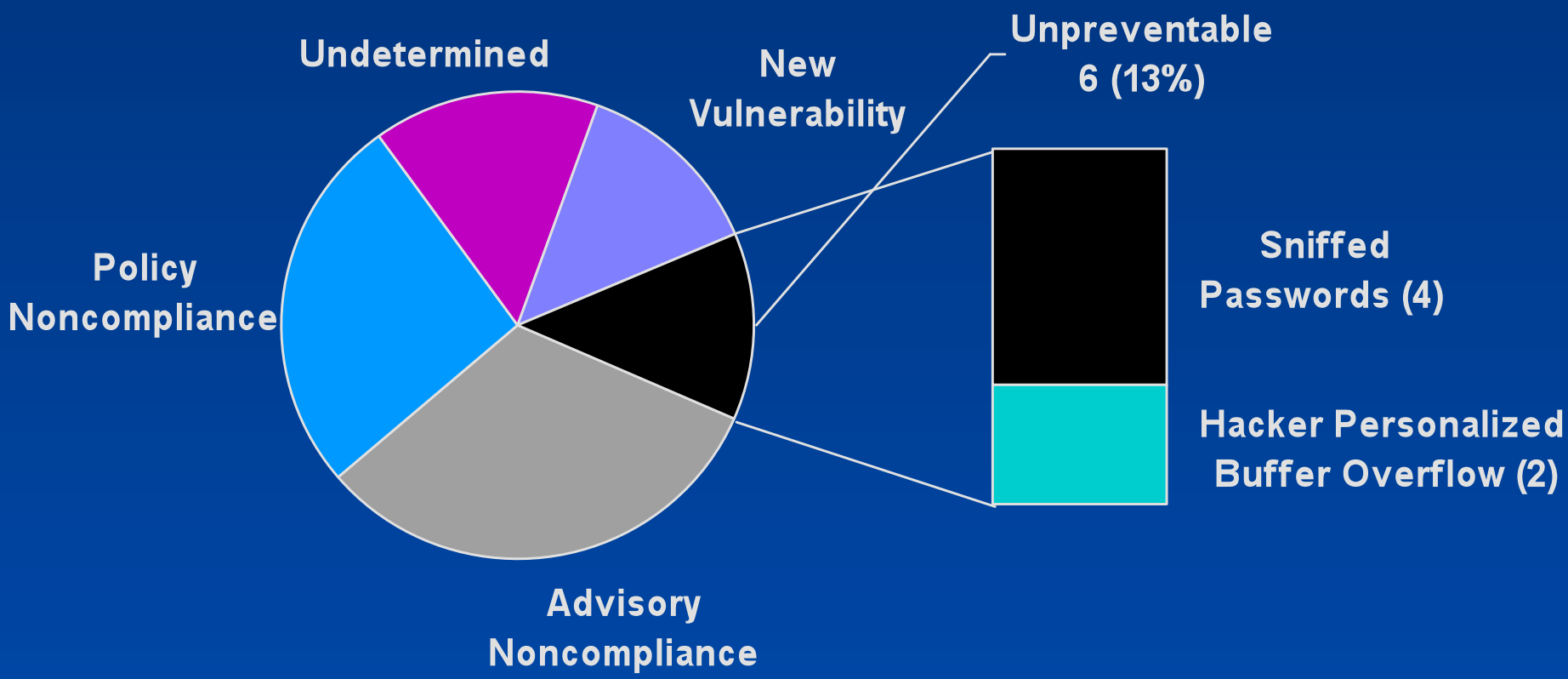
Advisory Noncompliance



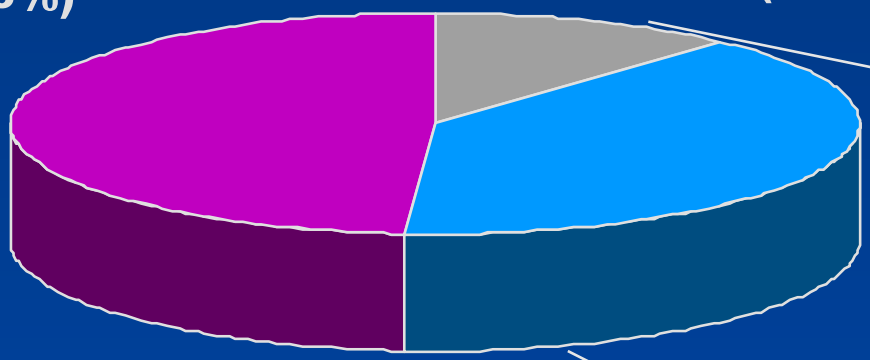
Policy Noncompliance



Unpreventable

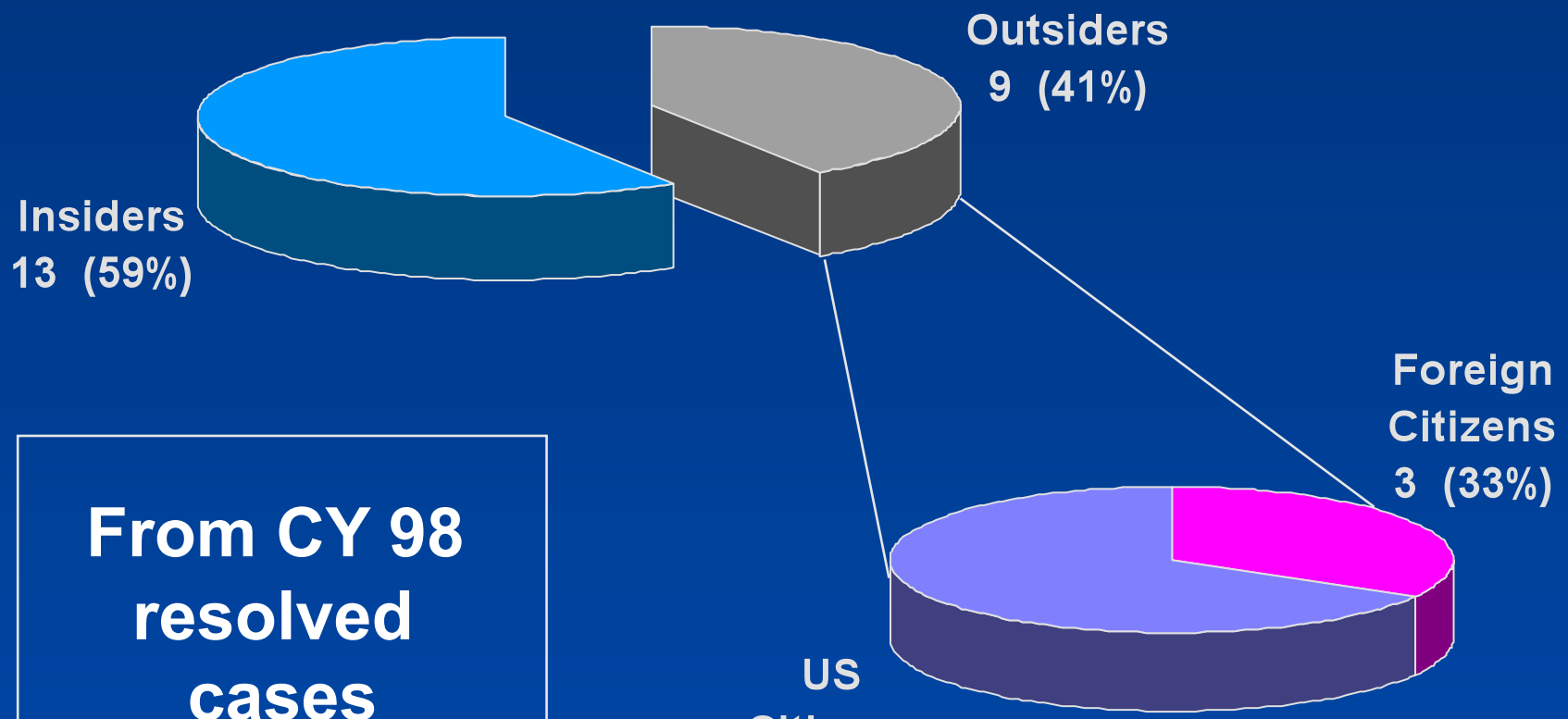


AFOSI Computer Investigations - CY98



22 cases resolved (52%) out of 43 total

Hackers
Insiders vs. Outsiders



From CY 98 resolved cases (22 total)

AFCERT Advisory Compliance Message Report Card - 1998

MAJCOM	98-01	98-02	98-04	98-05	98-06	98-07	98-08	98-09
ACC	●	●	●	●	●	●	●	●
AETC	●	●	●	●	●	●	●	●
AFMC	●	●	●	●	●	●	●	●
AFSPC	●	●	●	●	●	●	●	●
AFPC	●	●	●	●	●	●	●	●
AFPCA	●	●	●	●	●	●	●	●
AFRC	●	●	●	●	●	●	●	●
AFSOC	●	●	●	●	●	●	●	●
AMC	●	●	●	●	●	●	●	●
ANG	●	●	●	●	●	●	●	●
PACAF	●	●	●	●	●	●	●	●
USAFA	●	●	●	●	●	●	●	●
USAFE	●	●	●	●	●	●	●	●
11th WG	●	●	●	●	●	●	●	●

98-03 Retracted & replaced with 98-04

● = Compliant ● = Responded with exceptions ✸ = Intrusion

AFCERT Advisory Compliance Message Report Card - 1999

MAJCOM	99-01	99-02
ACC	●	●
AETC	●	●
AFMC	●	●
AFSPC	●	●
AFPC	●	●
AFPCA	●	●
AFRC	●	●
AFSOC	●	●
AMC	●	●
ANG	●	●
PACAF	●	●
USAFA	●	●
USAFE	●	●
11th WG	●	●

● = Compliant ● = Responded with exceptions

● = Compliance due 29 Jan ● = Compliance due 12 Feb

FOR OFFICIAL USE ONLY

Romania to Randolph
Root Level Access

Detection Date:	24 Jan 99
Location :	Randolph AFB
Unit:	AFPC/DPAP
System's Purpose:	AFPC Officer Assignments Web Page
Degree of Access:	Root Level
How Access Was Gained:	Web server was running the software product "Front Page" that allows web pages to be modified over the Internet
Insider/Outsider:	Outsider
Mission Impact:	Minimum-Hacker replaced official web page info with hacker message- access was limited to information available to the public
Known Vulnerability:	Yes
Corrective Action:	System disconnected from the network and backed up for further analysis
System Routed through AFNCC:	No
IAVA Issued:	No
ACM Issued:	No
AFCERT Advisory Issued:	Yes (Advisory 97-60)
CITS/BIP Installed:	Yes
AFOSI Investigation:	No, but notified

Improving the Process

- Revised process for issuing compliance messages - 15 Feb
- Process to cover centrally managed systems - 15 Feb
- On-line tracking mechanism developed
- Begin verification process using OLS tools - 1 Mar

Policy

Verifi tion

Compliance

Tightening Our Defenses

- Route networks through NCCs
  - MAJCOMs report data beginning 15 Feb
- Operational Reporting
  - AFMAN 10-206 (OPREP-3) - 15 Feb 99
  - AFMAN 10-201 (SORTS) - Mar 99
  - 1st CSAF SORTS Report - 1 May 99

Audits

- **Audits**
  - 7 in progress; no new draft or final reports since last briefing
  - 1 follow-on in progress
  - 1 final report with follow-up recommendation
  - 13 projected in next 18 months
- **Findings**
  - Vulnerabilities continue
  - Non-compliance with policies
  - Advisory Compliance Message process difficult for bases to follow
  - Difficult to determine if advisory applies to specific system
  - Poor readability of solution set

IG Special Interest Item on IA

- Look at compliance with policy, directives, procedures
- Direction from IGI - reframe, redo, 5-10 objective questions
- Work into inspection cycle
  - Mar 99 - Mar 00
  - 25% of AF

IA Manpower

- NCC manpower standard last applied in Dec 96
  - 1500 additional authorizations awarded
    - 500 in FY99
    - 250 each year FY00-FY03
- Will request XP review IA manpower in Network Control Centers and IA offices

Training & Certification

- Users - IA training & certification using IA CBT
- System administrators & maintainers - training & certification using IA CBT, skill-level CBTs, classroom instruction
- DoD mandate - J6K requesting suspense change

Category	Current	Requested
Classified system users	31 Jan 99	31 Mar 99
Classified system administrators & maintainers	31 Jan 99	31 Dec 99 Level 1 only
Unclassified system users,	31 Dec 00	31 Dec 00
Unclassified system administrators, & maintainers	31 Dec 00	31 Dec 00 Level 1 only

3rd Annual IA Awareness Month Feb 99

- CSAF message & NOTAM
- AF Web site hosted by AFCA
- AF/SC articles
- Activities
  - Train users & network professionals
  - Scrub publicly accessible Web sites
  - Verify compliance
    - Passwords
    - Virus scans
    - Patches installed

Theme:

A Risk Accepted by One is a Risk Imposed on All

IA Awareness Month SAM Activities

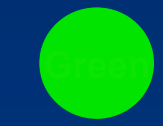
- SAM Town Meetings
  - AF OSI Forensics Lab - 2 Feb
  - Office of Criminal Investigation Computer Crimes Division - 4 Feb
  - AFOSI Hacker Tracking - 26 Feb
- Computer Security booth in Pentagon 1-5 Feb (2nd floor, corridor 9-10)
- Web site http://www.sam.pentagon.mil/DS/AFIAAM

Web Security

Tasks from DEPSECDEF Memo

OPR	TASK	DATE DUE
Services	1. Scrub web sites	24 Nov 98
OSD	2. Formulate policy	24 Nov 98
Services	3. Perform security review	23 Mar 99
OSD/ Services	4. Develop training program	23 Mar 99
OSD/ Services	5. Plan to use Reserves to conduct assessments	23 Mar 99

Task 3
Security Review



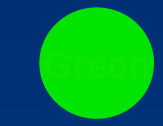
Task:
- Ensure comprehensive, multi-disciplinary security assessment is conducted for AF web sites

OPR:
- AF/SC through MAJCOMs/DRUs

Due date:
- 23 Mar 99

Status:
- Part of IA Awareness Month
- Complete review required NLT 23 Mar 99 per draft AF memo

Task 4
Training Program



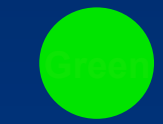
Task:
- Develop training program to address information security on web

OPR:
- AF/SC (lead), OPS, INTEL, information security, legal, PA, FOIA, privacy act

Due date:
- 23 Mar 99

Status:
- Workgroup Managers - initial training
- Web server administrators/workgroup managers (in-depth training)
- Developing comprehensive training plan to include PA & AQ communities

Task 5
Reserve Component



Task: Explore Reserve Component role in web site assessments

OPR: AF Reserve Affairs

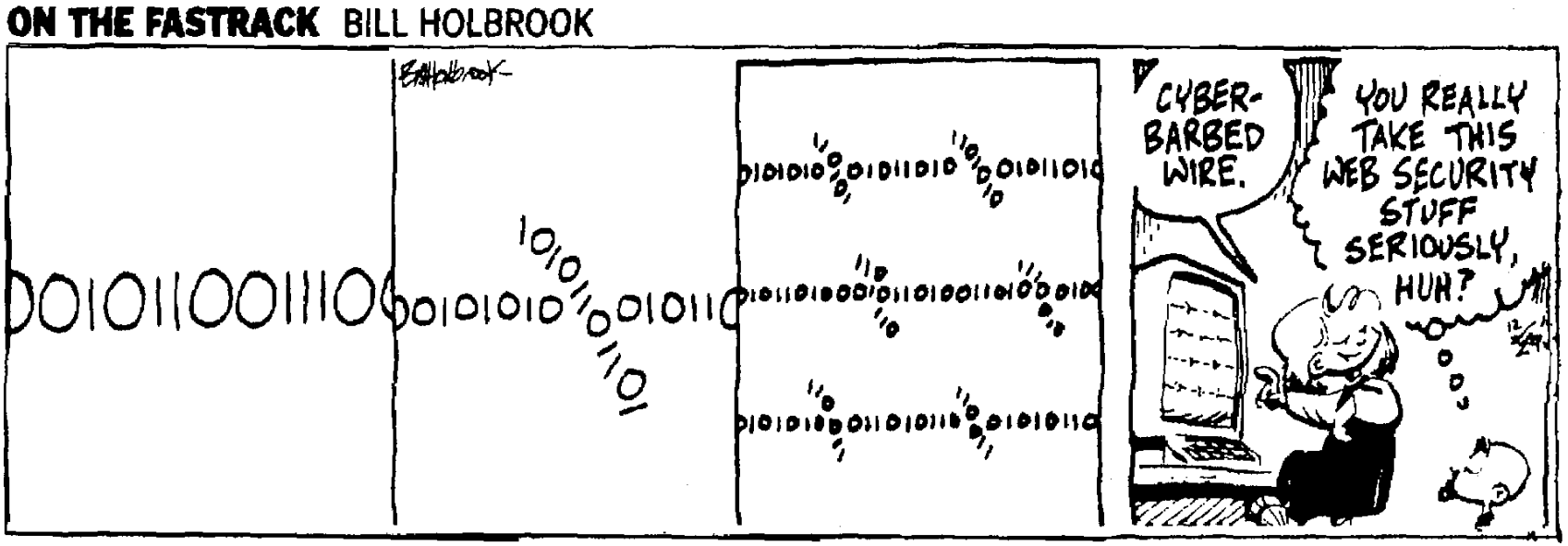
Due date: 23 Mar 99

Status:
- USAF/RE concurred with OSD Joint Web Risk Assessment Cell CONOPs - will provide 2 bodies
- USAF CONOPs in review
- Establish Reserve presence at MAJCOM NOSCs

Web Security Way Ahead

- Team with OSD:
  - Clarify
    - "Sensitive" information
    - Aggregation (OPSEC) concerns
  - Identify automated tool set
  - Develop training plan
- Team with AFRC:
  - Develop CONOPS
  - Establish IA mission
- Update to DEPSECDEF 3 Feb 99

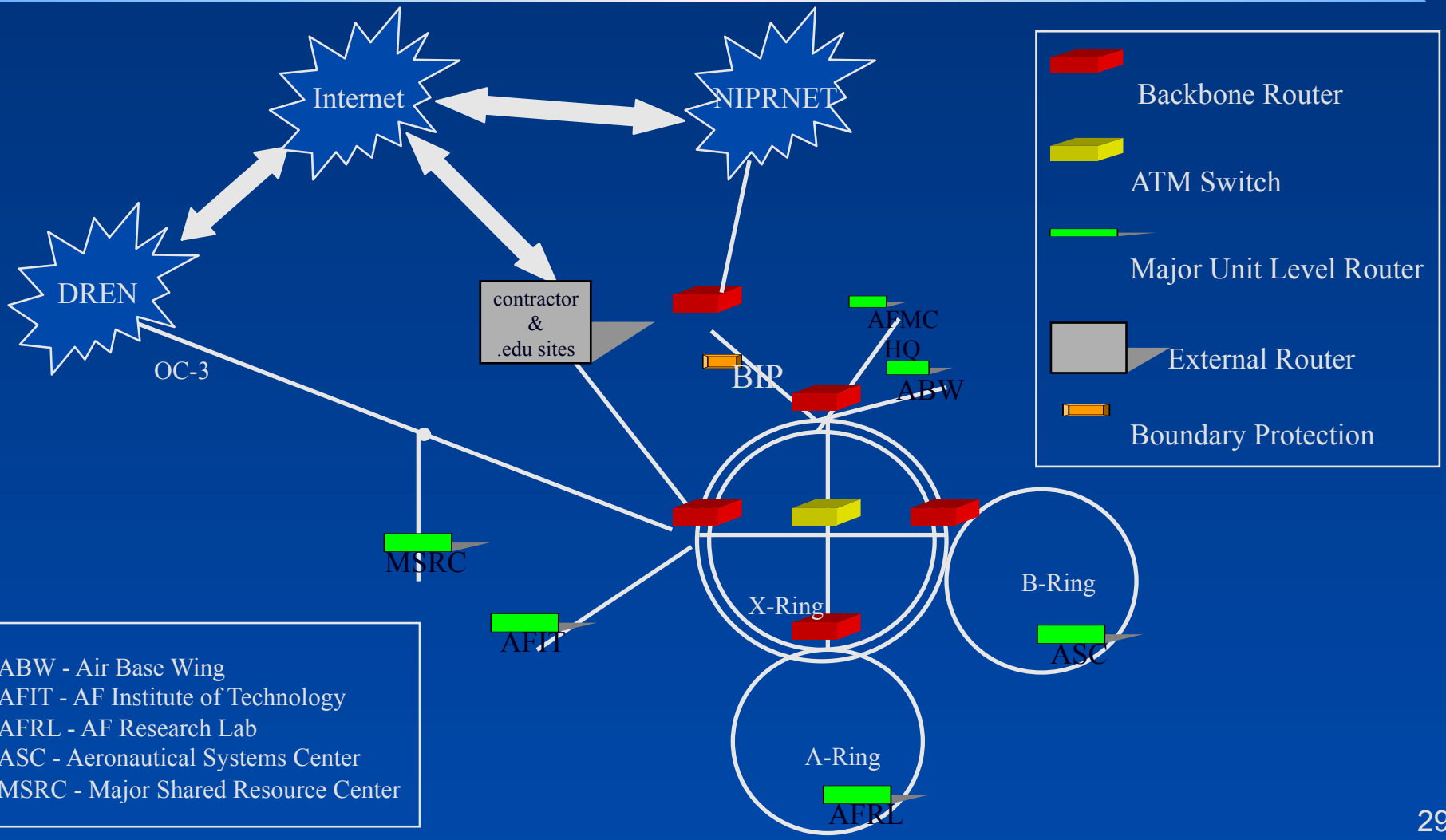
On The Light Side



Defense Research Engineering Network (DREN)

- Under cognizance of Director of Defense Research and Engineering
- Purpose - link DoD scientists and engineers to high-performance computing centers and each other
- Provides WAN services at bandwidths commensurate with user requirements
- Currently 63 DoD sites (14 AF sites)

DREN Past Topology

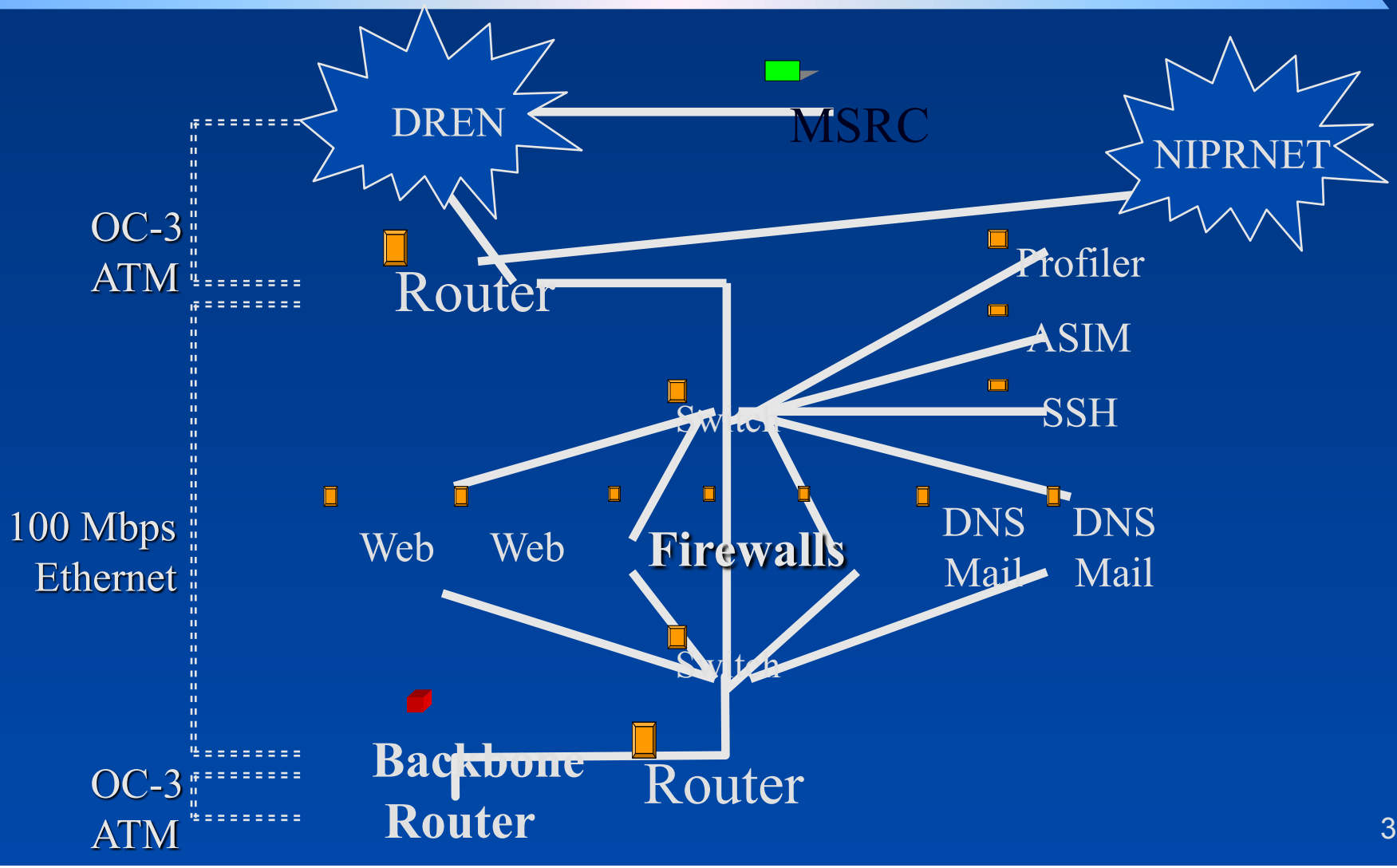


ABW - Air Base Wing
AFIT - AF Institute of Technology
AFRL - AF Research Lab
ASC - Aeronautical Systems Center
MSRC - Major Shared Resource Center

DREN Solution

- Problem: DoD sites connected to the DREN were vulnerable to attack
- AFCA teamed with WPAFB to develop solution
  - Initial 90% solution completed by 23 Dec 98
  - Place remaining backdoor connections through NCC by 30 Apr 99
  - Solution sent to remaining AF sites by 30 Jan 99
- Costs
  - $450K for WPAFB (AMC funded)
  - $2.9M for remaining 13 AF sites (unfunded)

DREN Projected Topology



Public Key Infrastructure (PKI)

- PKI underpins DEPSECDEF mandate to move to electronic commerce and paperless contracting

- PKI ensures:
  - Sender is the originator
  - Receiver is the intended recipient
  - Information is not intercepted
  - Data integrity is not compromised

What We've Done

- Established DoD PKI as Air Force standard
  - Uses industry standard certificates for Web and application encryption and digital signatures
  - Easy to migrate existing programs (assignment system) utilizing other brands
- Participation in DoD pilot programs
- High assurance PKI via Fortezza for DMS
- Teamed with business managers (electronic commerce) to incorporate digital signatures

PKI Funding

2000 POM, PE 33112, Base Information Infrastructure

(M)	00	01	02	03	04	05	Total
3080	5.0	14.0	5.0	4.4	4.5	4.6	37.5
3400	11.0	16.1	32.4	17.4	17.7	18.0	112.6

3080: Registration (certificate & directory) servers
Local registration workstations
Smart card tokens and peripheral upgrade for active duty, civilian, guard and reserve personnel

3400: Registration support personnel for all bases
Legacy software integration
Support help desk

PKI Program Schedule

	99	00	01	02	03	04	05
Field Registration Components		Mar-Dec 00				Mar 04-Mar 05	
Field Smart Cards and Readers			Jun 01----------				----------Sep 05
Train Local Registration Authority Personnel	Jul 99----------						----------Sep 05
Provide PKI Help Desk Personnel		Jan 00----------					----------Sep 05
Ad Hoc Register	Jan 99----------		----------Jun 01				
Register all USAF thru Local Registration Authority		Mar 00----------					----------Sep 05

Questions?

Backups

Root Intrusions Vulnerabilities Exploited

- **Advisory Noncompliance**
  - Domain Name Server (DNS) Buffer Overflow 98-21 & 98-24 (4)
  - Internet Message Access Protocol (IMAP) 97-44 (3)
  - Initial Sun Remote Procedure Call (SUNRPC) Probe 97-42 (1)
  - Netbus 98-57 (2)
  - Status Daemon (STATD) Buffer Overflow 98-01 (2)
  - ToolTalk 98-46 (2)
  - Unix File System (UFS) Restore 98-33 (1)
- **Policy Noncompliance**
  - Internet Information Server (IIS) Web Misconfiguration (1)
  - Default Password (3)
  - Poor Security (4)
  - Undeleted Account (2)
  - Direct Root Login (1)
  - Remote Login Enabled (1)

Root Intrusions Vulnerabilities Exploited

- New Vulnerability
  - Domain Name Server (DNS) Buffer Overflow 98-21 & 98-24 (1)
  - Netbus 98-57 (3)
  - Mount Daemon (LINUX) 99-01 (1)
  - X11/XConsole Buffer Overflow (1)
- Unpreventable
  - Sniffed Passwords (4)
  - “DF” (Hacker Personalized) Buffer Overflow (2)

Advisory Compliance Messages (ACM) - 1998

ACM 98-01	12 Jun	Remote Buffer Overflow
ACM 98-02	27 Aug	Malicious Code
ACM 98-04	6 Sep	Server Software
ACM 98-05	11 Sep	Multi-purpose Internet Mail Extension (MIME)-Aware Clients
ACM 98-06	23 Sep	Stack Overflow in Tooltalk
ACM 98-07	16 Oct	CISCO Internetworking Operation System (IOS) Vulnerability
ACM 98-08	18 Nov	Silicon Graphics, Inc. (SGI) Buffer Overflow
ACM 98-09	18 Nov	Internet Message Access Protocol (IMAP) & Post Office Protocol (POP)

Advisory Compliance Messages (ACM) - 1999

ACM 99-01	29 Jan	Remotely Exploitable Buffer Overflow Vulnerability in MOUNTD
ACM 99-02	12 Feb	Trojanized Version of TCP Wrappers

Compliance Process
(In place 27 May '98)