SIAC Information Security

Presented to NY City SPIN

May 11th, 2004

By Michael Lamberg

SIAC

Copyright Notice

Proprietary Notice

This document contains trade secrets of SIAC/NYSE. It is provided to persons and organizations doing business with SIAC/NYSE solely for their use in conducting that business. Disclosure of the contents of this document in whole or in part to any other parties without the prior written consent of SIAC is expressly prohibited.

Brand names and/or Trademarks

Brand names or Products cited in this document may be trade names or trademarks. Where there may be proprietary claims to such trademarks or trade names, the name has been used with a initial capital. Regardless of the capitalization used, all such use has been in a editorial fashion without any intent to convey endorsement whatsoever of the product or trademark claimant. SIAC expresses no judgement as to the validity or legal status of any such proprietary claims.

Engineering Services Disclaimer

Information contained in this document is believed to be accurate. However SIAC does not guarantee the completeness or accuracy of any of the published information. This work is published with the understanding that SIAC is supplying information, but not attempting to render engineering or other professional services. If such services are required the assistance of the appropriate professional should be sought.

What is Security?

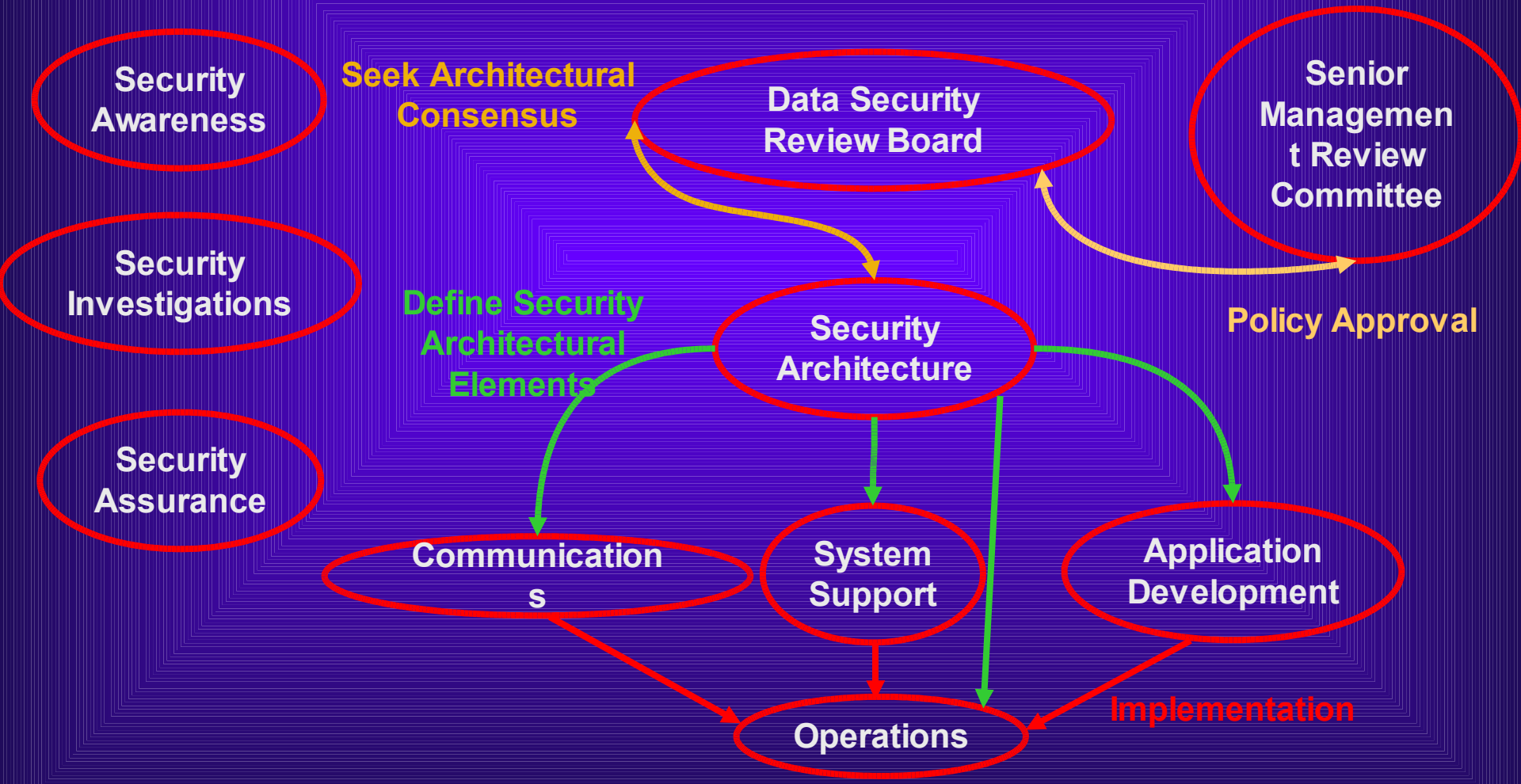
- To recognize and neutralize a threat using both proactive and reactive mechanisms
- *Security Mantra*
  - Secure what is reasonable and monitor everything else

SIAC

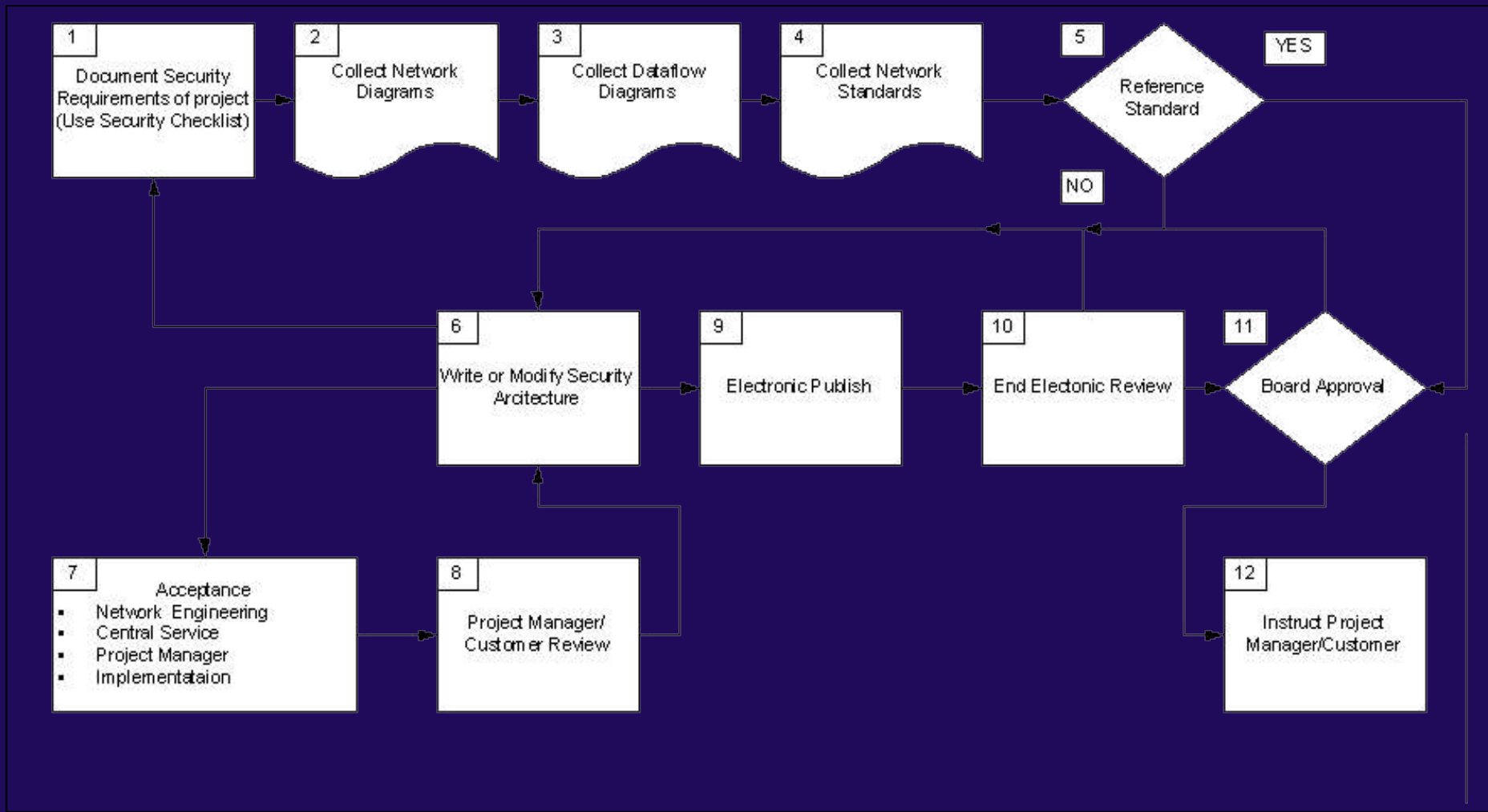
Corporate Information Security Department

- Policies, Guidelines, and Standards
- Information Security Awareness
- Security Architecture
- Data Security Review Board
- Security Technical Services
- Investigations and Forensics
- Industry Participation
- Research and Development

Major Components



Security Review Process



Policies

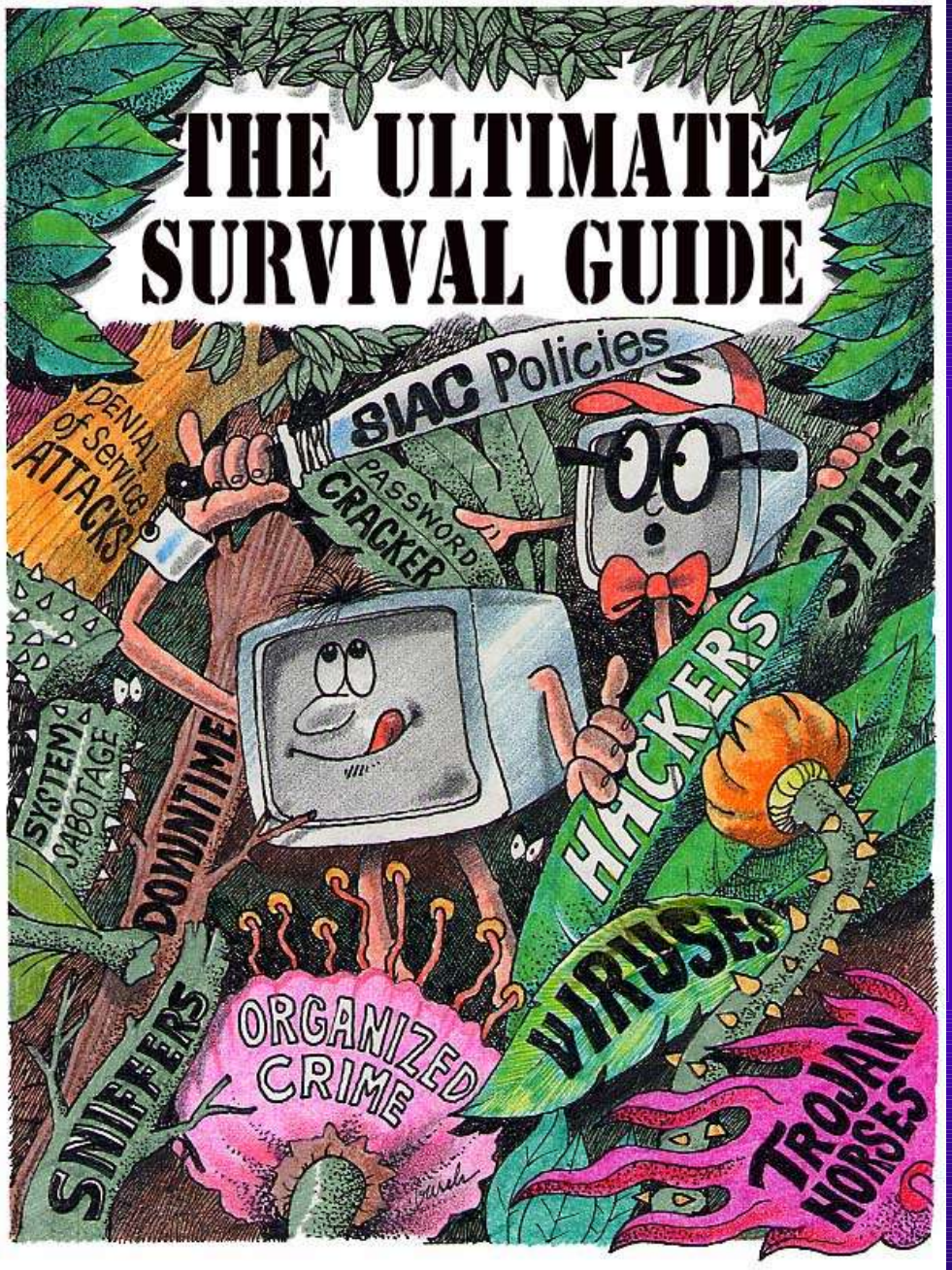
- New Information Security Policies rolled out on March 1, 2002
- Currently in use by the DSRB in reviewing projects
- Provide the focus of CISD's 2002 Security Awareness program
  - Training made mandatory

Standards

- Supporting documents for Policy implementation
  - Provide more specific guidance
- Mandatory Standards
  - Processes or practices that apply to SIAC as a whole
- Model Standards
  - Standards which may vary by business unit
  - CISD presents an example Standard representing best practices
  - Business units may adopt as is
  - Business units may write their own and submit to CISD for approval

Educational Challenges

- Large amount of material to introduce
- Policies are **BORING**
- InfoSec concerns are often in competition with other business needs


THE ULTIMATE SURVIVAL GUIDE
SIAC Policies
DENIAL of Service ATTACKS
PASSWORD CRACKER
SPIES
HACKERS
SYSTEM SABOTAGE
DOWNTIME
VIRUSES
SNIFFERS
ORGANIZED CRIME
TROJAN HORSES
TO SIAC INFORMATION SECURITY POLICIES!

Awareness Programs

- Info Security Calendar
- Awareness Days
- Web site – infosec.siac.com
- Information distribution
- Training for new and existing staff
  - Classes held on Secure Programming

Corporate Information Security

Search

Home | Applications | Hewlett Packard | IDS | Linux | Mainframes | Microsoft | Sun Microsystems | Others || Contact Us

Archive

Bulletins

Policies & Standards

Resources

Security

Upcoming Events Calendar

Good Morning
January 13, 2004

Worth Your While

2004 InfoSec Calendar
CERT Summary CS-2003-04
The Honeynet Project
PROFILES: Women of Vision
20 Women Luminaries
Use of the Common Vulnerabilities and Exposures...
Infosec Mailing List

E-zines

CyberNotes #2003-26
InfoSec News Volume 6.11 (November 2003)
InfoSec NewsWire Volume 4.1
SANS Newsbites Volume 6.1
Security Alert Consensus Volume 03.01
ISS Security Alert Summary #AS04-02

[more . . .]

Vulnerabilities

FS-ISAC Notices for January 13, 2004

Red Hat Updated CVS Packages Fix Minor Security Issue
Potential buffer overflow in xdrmem_getbytes() (rev.10)
Potential security vulnerability in rpc.yppasswdd (rev.2)
Potential buffer overflow in XDR library (rev.5)
Potential buffer overflows in DNS resolver libraries (rev.16)
Debian fsp Buffer Overflow Vulnerability
Debian 'nd' WebDAV command line Buffer Overflow...
HP 'ypxfrd' daemon Vulnerability
Potential Vulnerabilities in Apache HTTP Server (rev.2)
Potential vulnerability in ypxfrd
Multiple stack-based buffer overflows in mod_alias and mod_rewrite modules for Apache versions prior to 1.3.29.

[more . . .]

Viruses

	Virus Name	Infected Files* (McAfee.com)
1.	VBS/Redlof@M	194,971
2.	Exploit-URLSpoof	93,030
3.	W32/Pate.b	37,452
4.	W32/Dumaru.a@MM	25,348
5.	Adware-Lop	23,785
6.	IGetNet	21,074
7.	Adware-Gator	19,271
8.	MIRC/Generic	17,216
9.	W32/Nofear.c@MM	15,696
10.	Exploit-ByteVerify	15,594

*Worldwide / Past 24 hours

	Virus Name	Infected Files* (NYSE)	Infected Files* (SIAC)
1.	WORM_SWEN.A	-	22
2.	WORM_KLEZ.H	22	9
3.	HTML_CITIFRAUD.A	4	5
4.	WORM_SOBER.C	4	-
5.	VBS_INTERNAL.H	-	3
6.	PE_MAGISTR.B	1	1
7.	JS_KAKWORM.A	1	-
8.	WORM_GIBE.B	-	1

*January 1-12

Check this out! Check DAT out !!

View By: Location | Track: Infected computers | Select Map: Worldwide | Time Period: Past 24 hours

Top 10 - Worldwide

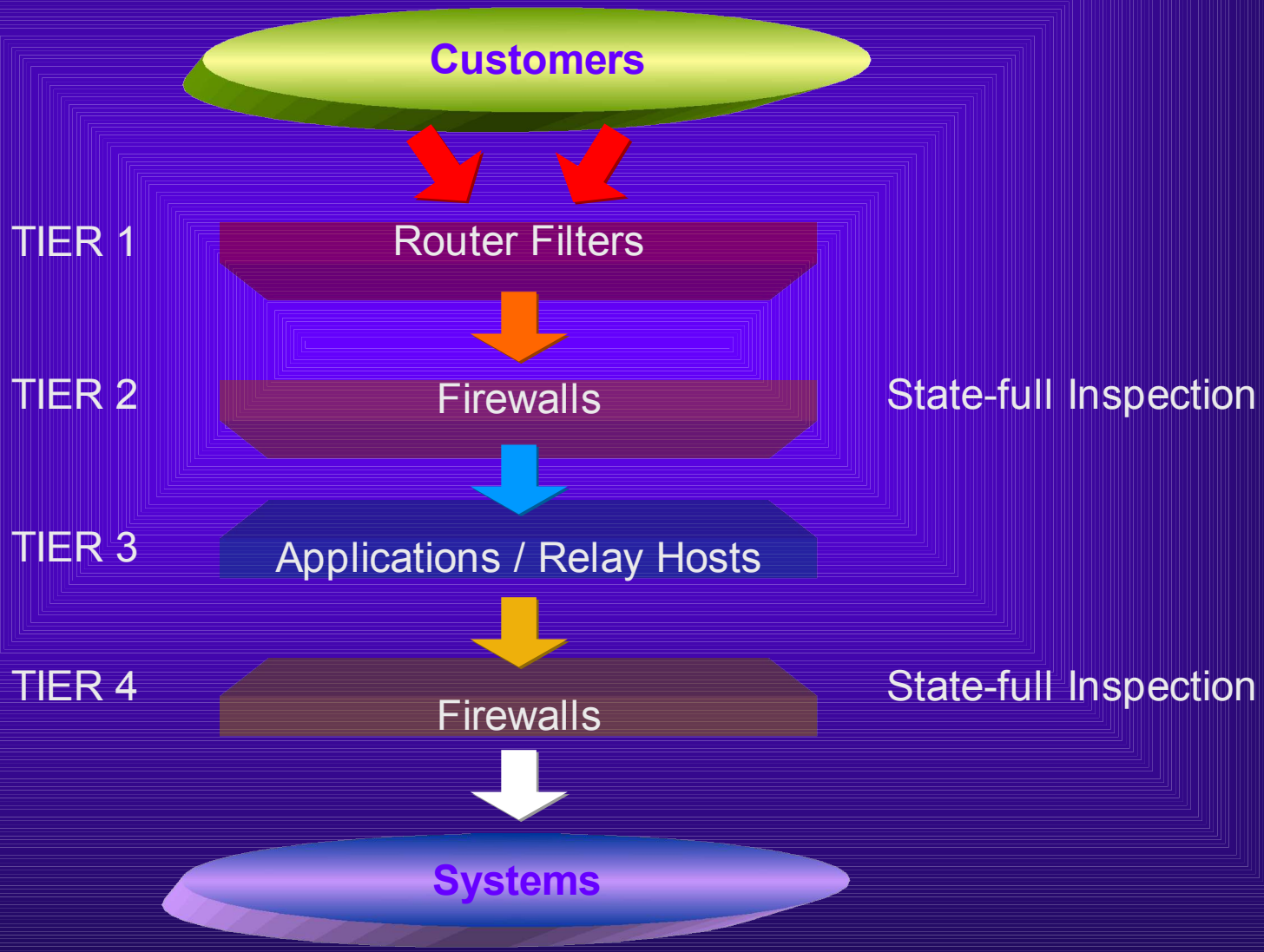
1.	WORM_LOVGATE.G	30,059
2.	PE_VALLA.A	9,028
3.	PE_ELKERN.D	8,657
4.	PE_NIMDA.A-O	3,079
5.	TROJ_MAGICON.A	2,792
6.	PE_FUNLOVE.4099	1,516

Information Security Technology

- **Proactive** Mechanisms
  - CAP (defense in depth)
    - Firewalls, Relay hosts
  - DMZ
- **Reactive** Mechanisms
  - Collective Intelligence
  - Intrusion Detection

SIAC

Layered Networking Approach



Security Assessment & Testing

- Continuous Assessment
  - Daily Scans of the perimeter
- Pre and Post Deployment Assessments
- Utilize a combination of tools
  - SIAC developed tools: “BorderPatrol”
  - Third Party Tools: “Foundstone Managed Service”
  - Automated tools: Nessus, ISS, WebInspect

Corporate IDS Strategy

- Transition to COTS solution
- Improved configuration/signature management
- Development of environment specific signatures

FS ISAC

Ops Staff

DHS

AntiVirus Vendors

I4

3rd party analysis

SIAC Information Security Posture

Secret Service

Internet Monitoring

FBI

Legend

FS-ISAC: Financial Services Info Sharing and Coordination

I4: International Information Integrity Institute

DHS: Department of Homeland Security

SIAC

Additional Areas of Focus

- Incident Escalation Drills and Metrics
- Tabletop Exercises
- Evaluate Risk Assessment Models