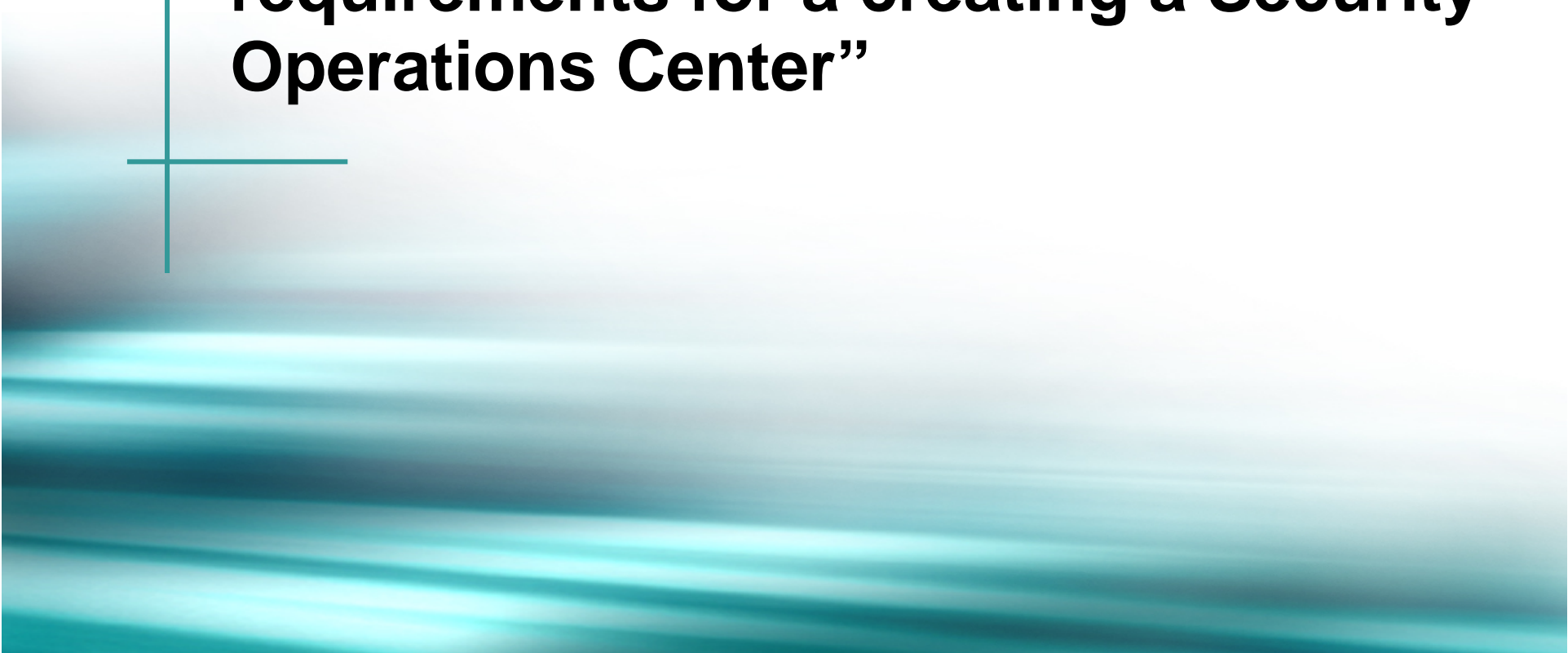




Creating a Security Operations Center (SOC)

Objectives

Cisco.com



“Understand the fundamental requirements for creating a Security Operations Center”

Agenda

Cisco.com

- **What is a SOC?**
- **Principles of a SOC**
- **Why build a SOC?**
- **Build your SOC Team**
- **SOC Team Skills**
- **Build the Communications Channels to your Peers and Customers**
- **Build Communications Channel to your Vendors**
- **Building the Tool Kit**

What is a SOC?



A lot of confusion - based on FUD

Cisco.com

- **Competitors – especially Managed Security Service Provider (MSSP) competitors – are using “SOC” as a tool to generate business.**
- **Yet, what is a “Security Operations Center” all about?**
 - Network Security?**
 - Customer Security?**
 - Facilities Security?**
 - Site Security?**
 - Rapid Reaction and Response?**
 - Emergency Response (Fire, Earthquake, etc.)?**
 - Lost Prevention and Response (loose a laptop lately)?**

What is a SOC?

- It all depends what you want to achieve.
- For our discussion, we will be addressing:
 - SP Operations Security on all the infrastructure necessary to protect their production business.
 - SP Operations Security to protect their customers.
 - SP Operations Security as a service sold or provided to their customers.
- What it is not:
 - We will not be talking about the INFOSEC Role which protects the IT resources which *support* their business.

Cisco's Recommendation

Cisco.com

- **Three Security Operations Teams are needed in a SP:**
 1. **Network Operations Center (NOC):** Running and Managing the network.
 2. **Security Operations Center (SOC):** Protecting, Securing, and Responding to Incidents.
 3. **INFOSEC:** Protecting the IT resources in the company.

Principles of a SP's SOC



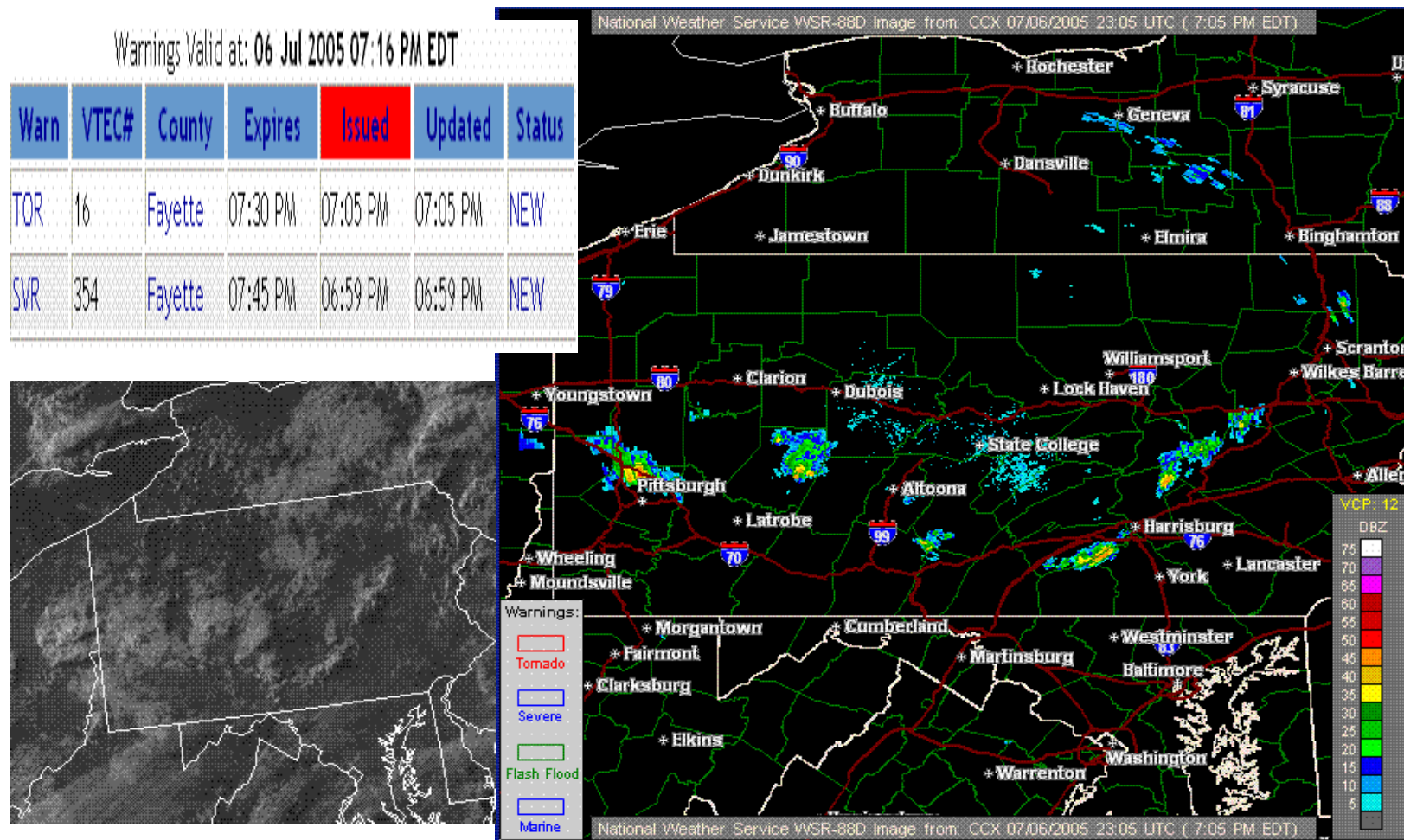
Core Principles of a SP SOC (in work)

Cisco.com

1. Complete *Situational Awareness* of the entire SP business.
2. Command and Control over the entire network *while the network is under stress*.
3. Multiple, Redundant, and Exercised *Inter-Organizational* and *Extra-Organizational* Community Channels.
4. Tested Tools, Procedures, and Practices which the SOC uses to do it's job.
5. Incident Management/Trouble Ticketing Tools to insure that the chaos does not allow anything to fall through the cracks.

What is Situational Awareness?

Cisco.com



Situational Awareness Sources

Cisco.com



Everything is interlinked and Inter-dependent. Vehicle maintenance is as important to *security* as any other part of the system.

Concept of the CIC and C4I

Cisco.com

- **Command Information Center (CIC)** is the center of a high risk environment.
- It is the central control point of the battlefield.
- It is governed by the doctrine of C4I, Command, Control Communication, Computerization, and Intelligence.
- Today's CIC for a network is called a NOC/SOC.



Why Build a SOC?



Data Overload

Cisco.com

Syslogs

Packet Capture

SNMP

IDS

Identity Management

Netflow

Firewall Logs

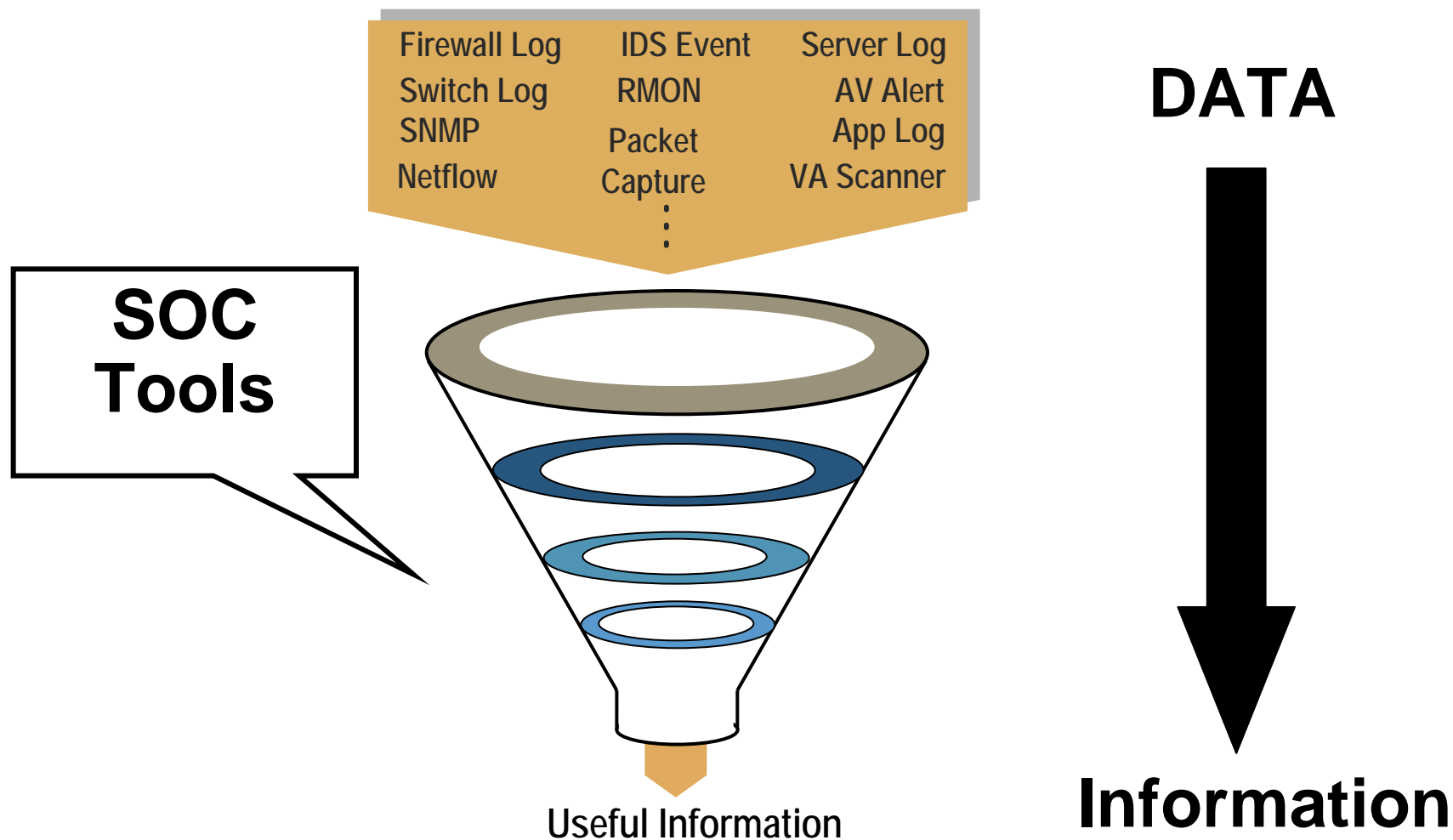
RMON

Backscatter

Anti-Virus Logs

Correlation

Cisco.com



Questions

- **In the face of such overwhelming odds, how can you ensure that your vital business assets and operations are protected?**
- **How do you guarantee privacy for your employees, partners, vendors and customers?**
- **How do you implement security policies?**
- **How do you get a handle on the vast amounts of data and on the incompatible technologies and devices that, while standing guard, generate an entire new set of challenges?**
- **How do you maintain accountability and corporate governance within the organization?**

What Do SPs Need to Do?

Cisco.com

Security incidents are a normal part of an SP's operations!



The Preparation Problem

Cisco.com

- **The problem - Most SP NOCs:**

Do not have security plans

Do not have security procedures

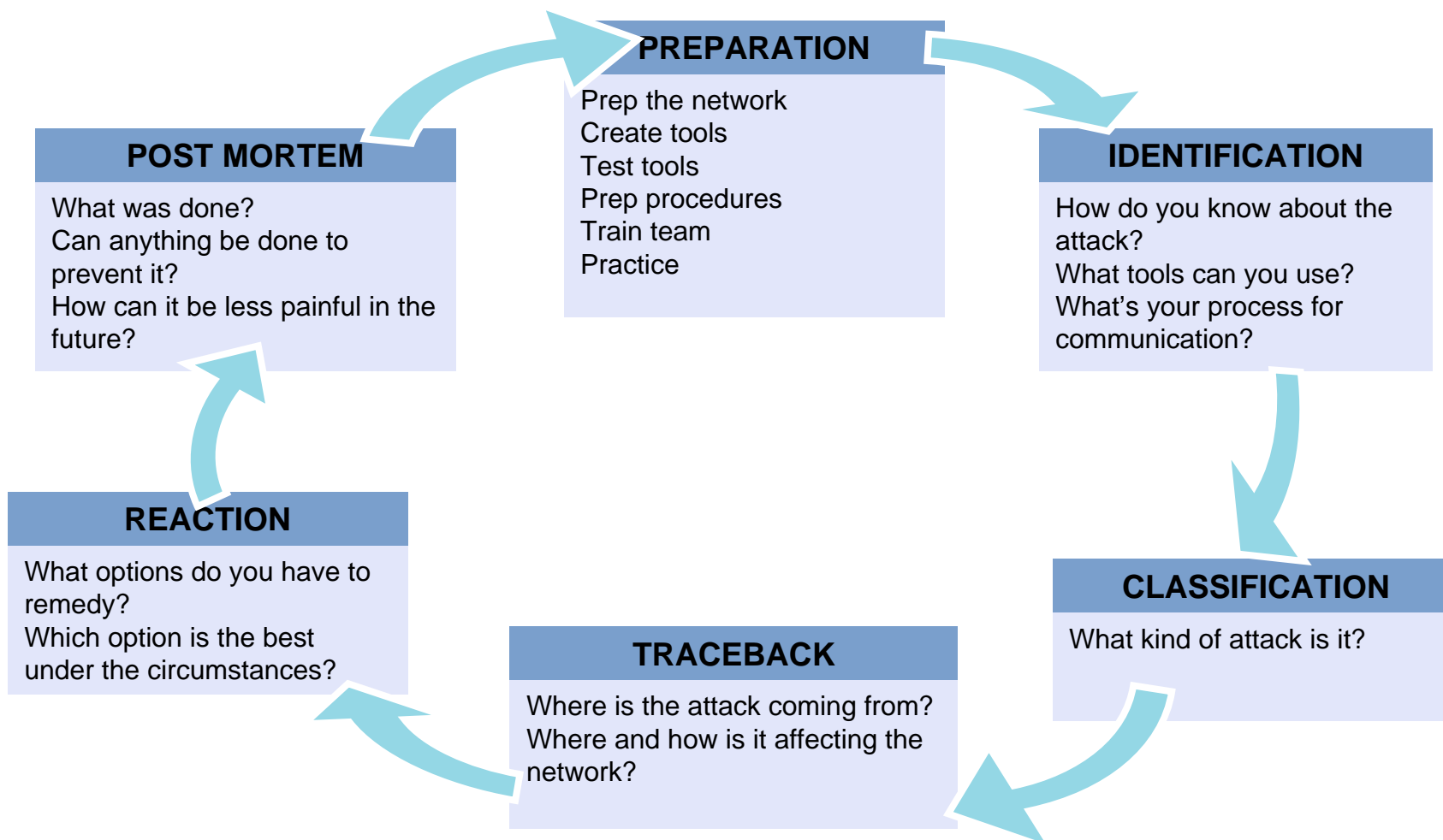
Do not train in the tools or procedures

OJT (on the job training)—learn as it happens



Six Phases of Incident Response

Cisco.com



Functions

- **Risk Management**
- **Security Information Management System (SIMS)**
- **Vulnerability Scanning (tactical scanning, targeted scanning and differential scanning)**
- **Sniffing/Data Forensics**
- **Command Console (Intrusion Prevention System, Intrusion Detection System, IT-Sec Dashboard)**
- **Top-Talkers Reporting and Response**
- **Centrally Managed AV/FW/IDS**
- **Patch Management**
- **Asset Tracking and Recovery**
- **Anomaly Detection**

Actions of SOC

- **Performs real-time monitoring and management of firewalls, intrusion detection systems, intrusion prevention systems, virtual private networks, patch management, asset management and other security products**
- **Enhances the institution's information security posture through continuous monitoring and management, expert analysis of log data, and immediate response to potential security threats**
- **Provides rapid resolution of security problems from the security operations center**
- **Offers the institution a real-time view of the enterprise security posture**
- **Ensures optimal protection of mission-critical assets by providing analysis and commentary needed to adjust defenses against emerging attacks**
- **Protects companies technology investments**

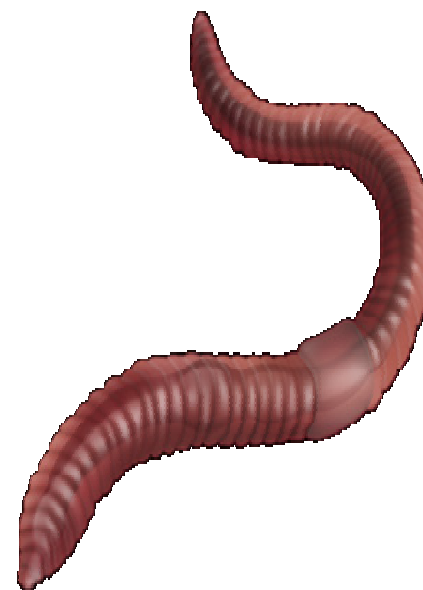
Consequences of No Action

- **SLAMMER Illustrated the difference between those SP who were prepared and those who were not.**

NOC/Sec-Ops Teams that had the most rudimentary procedures in place (i.e. a internal contact list) where able to start their anti-Slammer action with the first 6 hours.

Those who did not, started after 6 hours – with the effects network wide.

- **Q. Are you ready for the next Turbo Worm?**
- **Q. Are you ready for the next Internet wide incident?**



Build and Prepare your Security Operations Teams



Tips

- **Hire experienced, certified people**
- **Document and verify processes**
- **Maintain latest infrastructure information**
- **Establish SLAs with customers and peers**
- **Test the continuity of operations regularly**
- **Maintain vendor support contracts**
- **Leverage analysis tools**
- **Create incentives for analyst development**
- **Plan and prepare for incident response**
- **Evaluate and measure for process improvement**

SP's SOC Team

Cisco.com

- **Every SP needs a SOC**
- **Anyone who has worked or run a SOC has their own list of what should be in a SOC**
 - Make your own wish list**
 - Talk to colleagues and get their list**
 - Then try to make it happen**
- **No SOC is a perfect SOC—the result is always a ratio of time, money, skills, facilities, and manpower**

SP's OPSEC Team

- **An SP's OPerational SECurity Team can be:**
 - A NOC Escalation Team**
 - A sister to the NOC – reporting to Operations**
 - Integrated Team with the NOC**
- **The OPSEC Team is a critical component of the day to day operations of a large IP Transit provider.**

SP's OPSEC Team – Separate?

Cisco.com

- **Traditionally, the security, InfoSec, or Information Assurance (IA) team has been totally separate from the network/systems operations organization.**

The BCP in the industry to insure audit separation.

Audit gains has the consequence of in-efficient working relationship with the operations organization.

- **With today's DDOS attacks, BOTnets, and Turbo Worms, separation and poor working relationships bog down the resolution time – impacting the services to the customers.**

SP's/ISP's SOC Team and INFOSEC Team

Cisco.com

- **Some SPs have adopted the model of two teams:**
 - OPSEC integrated into network/system operations**
 - InfoSec in a separate reporting chain**
- **OPSEC team is tactical—Taking care of the daily security incidents**
- **INFOSEC team is strategic—Working on long term solutions, audits, and other items that are not time critical**

An SP's Incident Response Team

Cisco.com

- **SPs need an Incident Response Team**
- **The SP's Incident Response Team can be from one person to many people – depending on the size of the ISP.**

Dedicated Team

Virtual Team

NOC Double Coverage

- **Usually connected to the SP's NOC/SOC**

Processes

Cisco.com

- Write down the process you use to mitigate a security incident on your network
- Do you have a consistent methodology? Or, do you just start poking around?
- How can you evolve a mitigation methodology in your organization?



SOC Team Skill Requirements



SOC Team Skill Requirements

Cisco.com


- **SOC Team needs to know**
 - Everything a SP's Backbone Engineer knows**
 - Everything a SP's Network Management Engineers knows**
 - Everything a SP's Hosting/Content Engineer knows**
 - Everything a SP's Postmaster knows**
 - Everything a SP's DNS/DHCP/Addressing Engineer knows**
 - Everything a CERT Engineer knows**
 - Everything a Enterprise Security Engineer knows**
- **In essence – you are looking for super engineers who are a hybrid SP Backbone and Security Engineer**

Why?

- **An SP's SOC/OPSEC team needs**
 - Access to every device in the network.**
 - Total access to the network's control plane**
 - Authority, maturity, and trust to make on the spot decisions which impact the entire network.**

Communications





“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”

Barry Raveendran Greene

Preparation as Empowerment

Cisco.com

- **It is imperative that an SP's operations team prepare by empowering them for action.**

Contacts for all ISPs who you inter-connect (peers, customers, and upstreams)

Contacts for all vendor's product security reaction teams.

Document your policies. Will you help your customers? Will you classify the attacks? Will you traceback the attacks? Will you drop the attacks on your infrastructure?

Important Points

Cisco.com

- **Create your company's Computer Emergency Response Team**
- **Know your peers (neighboring CERTs), build relationships**
- **Get on NSP-SEC mailing list and on iNOC Phone**
- **Know Cisco PSIRT**

Use psirt@cisco.com, security-alert@cisco.com to contact us.

Subscribe to cust-security-announce@cisco.com for alerts.

- **Be prepared ! Define what to do & whom to contact for various incidents.**

Step #1 – Take Care of Your Responsibilities

Cisco.com

- **Before knocking on doors to collect information on others, it is best that you take the time to insure you are fulfilling your responsibilities to facilitate communications.**
- **Make sure you have all the E-mail, phones, pagers, and web pages complete.**
- **Make sure you have procedures in place to answer and communicate.**

OPSEC Communications

Cisco.com

- **Operations teams have a responsibility to communicate with**
 - All peers, IXPs, and transit providers**
 - Teams inside their organization**
 - Customers connected to their network**
 - Other ISPs in the community**
- **E-mail and Web pages are the most common forms of communication**
- **Pagers and hand phones are secondary communication tools**

OPSEC Communications

Cisco.com

Q. Does noc@someisp.net work?

Q. Does security@someisp.net work?

Q. Do you have an Operations and Security Web site with:

Contact information

Network policies (i.e. RFC 1998+++)

Security policies and contact information

Q. Have you registered you NOC information at one of the NOC Coordination Pages?

<http://puck.nether.net/netops/nocs.cgi>

SOC's Public Mailboxes

Cisco.com

- RFC 2142 defines E-mail Aliases all ISPs should have for customer – ISP and ISP – ISP communication
- Operations addresses are intended to provide recourse for customers, providers and others who are experiencing difficulties with the organization's Internet service.

MAILBOX	AREA	USAGE
-----	-----	-----
ABUSE	Customer Relations	Inappropriate public behavior
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries

/Security Web Page

Cisco.com

- **New Industry Practices insist that every IT company has a /security web page. This page would include:**
 - Incident Response contacts for the company.**
 - 7*24 contact information**
 - Pointers to best common practices**
 - Pointer to company's public security policies**
 - Etc.**
- **See www.cisco.com/security as an example.**

Emergency Customer Contact List

Cisco.com

- **E-mail alias and Web pages to communicate to your customer**

Critical during an Internet wide incident

Can be pushed to sales to maintain the contact list

Operations should have 7*24 access to the customer contact list

Remember to exercise the contact list (looking for bounces)

Exercising the Customer Contact List

Cisco.com

- **Use Internet warning to look for bounces before a crisis**

Dear Customers,

You are receiving this email because you have subscribed to one or more services with Infoserve. We have received a virus alert from security authorities and we believe that you should be informed (please see information below). If you do not wish to be included in future information service, please click "Reply" and type "Remove from subscription" in the subject field.

We have received warning from security authorities on a new virus, W32.Sobig.E@mm. W32.Sobig.E@mm is a new variant of the W32.Sobig worm. It is a mass-mailing worm sends itself to all the email addresses, purporting to have been sent by Yahoo (support@yahoo.com) or obtained email address from the infected machine. The worm finds the addresses in the files with the following extensions: .wab .dbx .htm .html .eml .txt

You should regularly update your antivirus definition files to ensure that you are up-to-date with the latest protection.

For more information, please follow the following links:

Information from Computer Associates: <http://www3.ca.com/solutions/collateral.asp?CT=27081&CID=46275>

Information from F-Secure: http://www.europe.f-secure.com/v-descs/sobig_e.shtml

Information from McAfee: http://vil.mcafee.com/dispVirus.asp?virus_k=100429

Information from Norman: http://www.norman.com/virus_info/w32_sobig_e_mm.shtml

Information from Sophos: http://www.norman.com/virus_info/w32_sobig_e_mm.shtml

Information from Symantec: <http://www.symantec.com/avcenter/venc/data/w32.sobig.e@mm.html>

Information from Trend Micro: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.E

Remember to Communicate

Cisco.com

- **Make sure there is someone behind all the E-mail aliases**
- **It is of no use to have a mean for people to communicate with your when you have no one behind the alias/phone/pager/web page to communicate back**
- **Many aliases are **unmanned**—with E-mail going into limbo**

CERTs (Computer Emergency Response Teams)

Cisco.com

- **Origin: The Internet Worm, 1988**
- **Creation of “The” CERT-CC (co-ordination center)**

Carnegie Mellon University, Pittsburgh

<http://www.cert.org/>

- **The names vary:**

IRT (Incident Response Team)

CSIRT (Computer security incident response team)

... and various other acronyms

- **Start with the following URLs:**

www.cert.org

www.first.org

How to Work with CERTs

Cisco.com

- **Confidentiality**
- **Use signed and encrypted communication**
Use PGP, S/MIME or GPG, have your key signed !
- **CERTs coordinate with other CERTs and ISPs**
- **CERTs provide assistance, help, advice**
- **They do not do your work!**

Coordination

Cisco.com

- **FIRST:**
Forum of Incident Response Teams
<http://www.first.org>
- **NSP-SEC**
- **I-NOC Phone**

Collecting Information from Peers

Cisco.com

- **Do you have the following information for every peer and transit provider you interconnect with?**

E-mail to NOC, abuse, and security teams

Work phone numbers to NOC, abuse, and security teams

Cell Phone numbers to key members of the NOC, abuse, and security teams

URLs to NOC, abuse, and security team pages

All the RFC 1998+++ remote-triggered communities

Questions

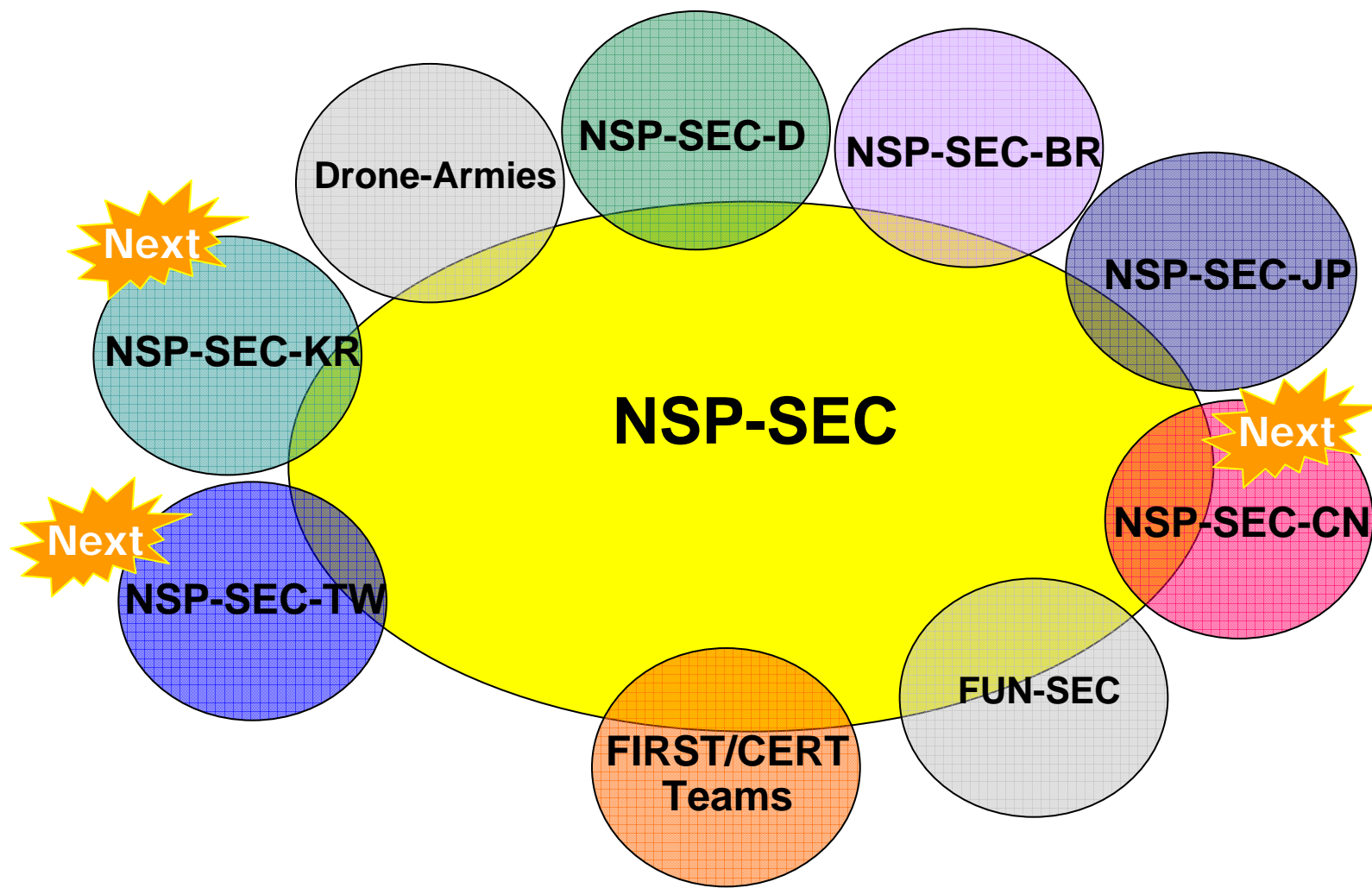
- Q. Do you have the NOC and Security Contacts for every ISP you are peered?**
- Q. Do you test the contact information every month (E-mail, Phone, Pager)?**
- Q. Have you agreed on the format for the information you will exchange?**
- Q. Do you have a customer security policy so your customers know what to expect from your Security Team?**

Community Communications



Miscreant Mitigation Communities

Cisco.com



NSP-SEC

“The nsp-security [NSP-SEC] forum is a volunteer incident response mailing list, which coordinates the interaction between ISPs and NSPs in near real-time and tracks exploits and compromised systems as well as mitigates the effects of those exploits on ISP networks. The list has helped mitigate attacks and will continue to do so.”

<http://puck.nether.net/mailman/listinfo/nsp-security>

NSP-SEC

Cisco.com

- **NSP-SEC—Closed security operations alias for engineers actively working with NSPs/ISPs to mitigate security incidents**
- **Multiple layers of sanity checking the applicability and trust levels of individuals**
- **Not meant to be perfect—just better than what we had before**

<http://puck.nether.net/mailman/listinfo/nsp-security>

Who can be on NSP-SEC ?

- **Do you work for some type of IP transit provider, huge multi-homed content provider, or service provider?**
- **Does your job include Operational Security?**
- **Are you willing to offer free services, data, forensic, and other monitoring data to the NSP community?**
- **Do you have authorization to actively mitigate incidents in your network? Do you actually log into a router and do something to mitigate an attack or call someone to task them to do the work?**
- **Do you have the time for a real-time NSP mitigation forum?**

What Can You Do to Help?

Cisco.com

- **Inform your SP, ISP, NSP, and Co-Location peers. Let them know that NSP-SEC exist:**

<http://puck.nether.net/mailman/listinfo/nsp-security>

- **NSP-SEC is looking for two or three engineers from each ISP who has the authority to configure routers and handle security incidents**

NSP-SEC: Daily DDOS Mitigation Work

Cisco.com

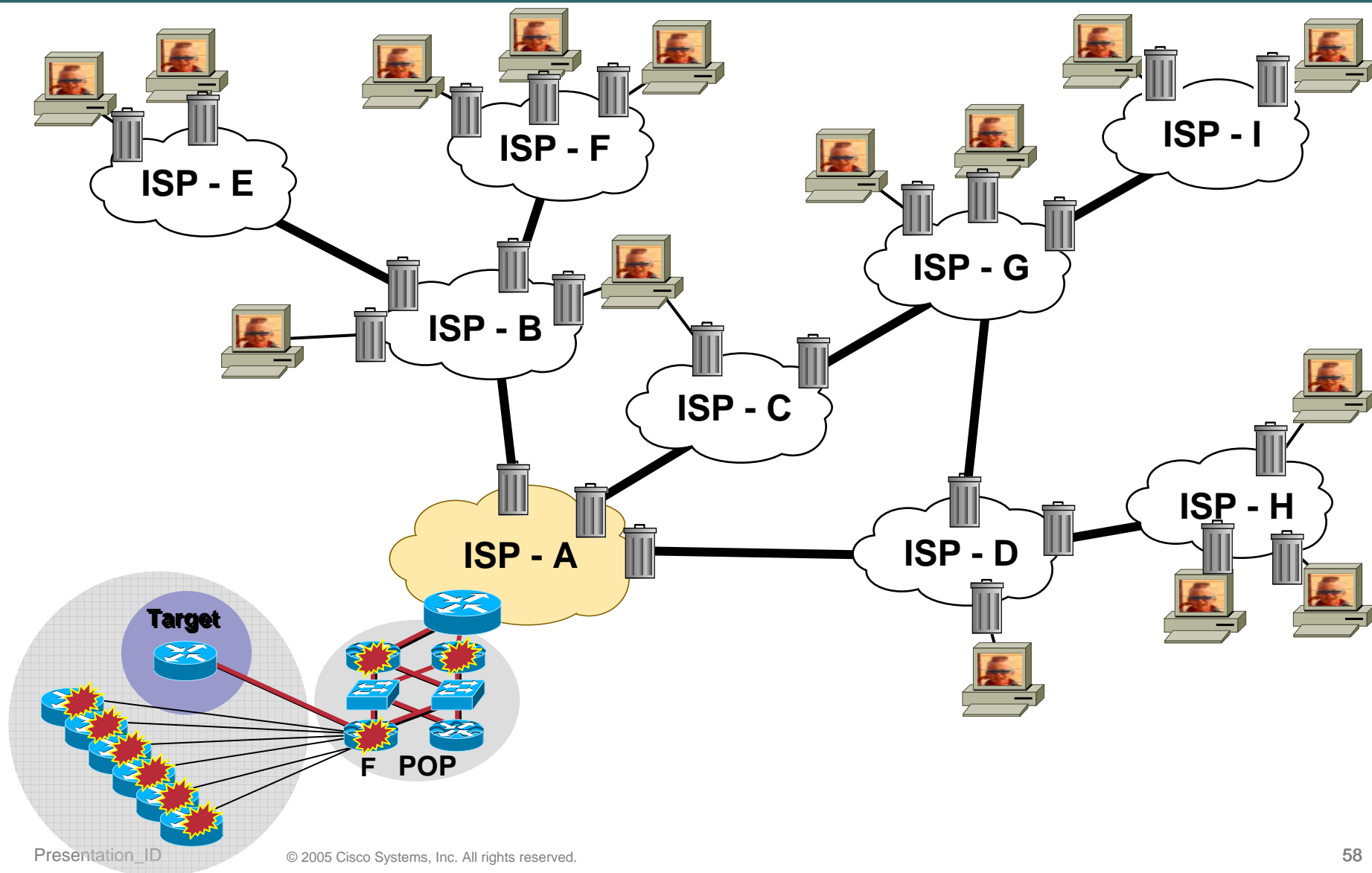
I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.

Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.

I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

NSP-SEC = Inter-Provider Mitigation

Cisco.com



NSP-SEC's Role During Slammer

Cisco.com

- **The ISPs were the first to notice something was happening**

Circuits saturated, routers spiking, BGP sessions flapped, and customers complained

- **NSP-SEC was the first reporter of the worm. CERT/FIRST Teams got their alert from NSP-SEC**
- **NSP-SEC members were the ones who dump the packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm**

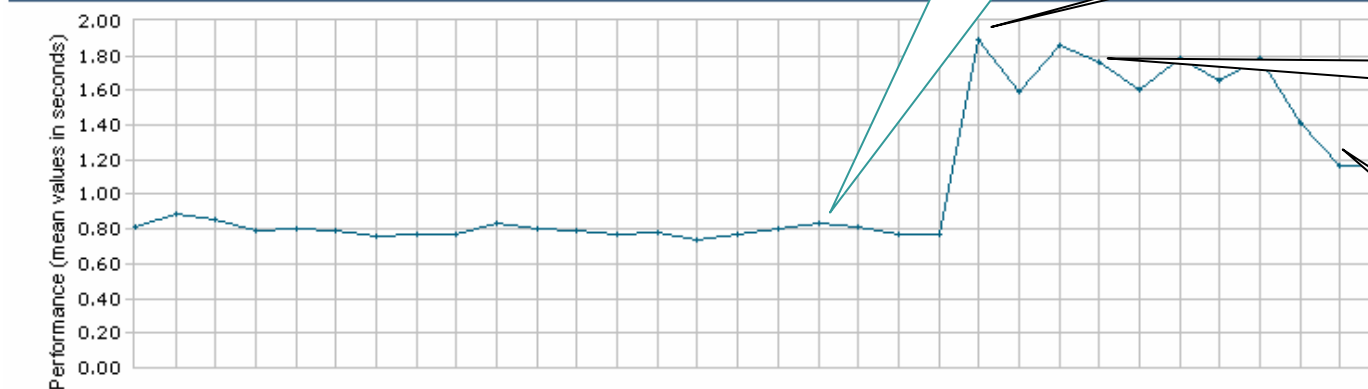
Impact of NSP-SEC's Containment

Cisco.com

KEYNOTE

MyKeynote

Web Site Performance and Availability by Time - Trimmed

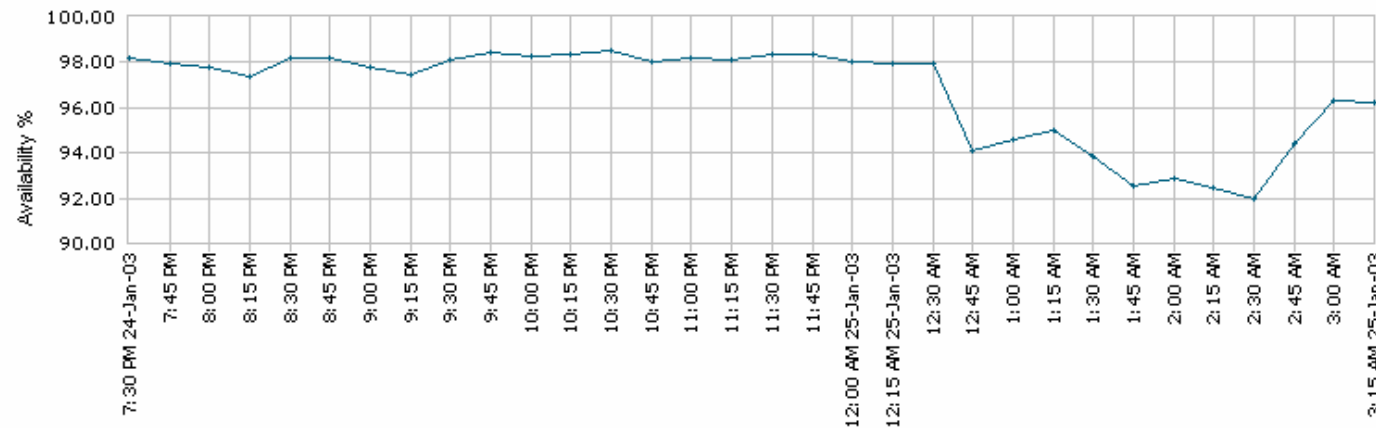


Real Impact

First Seen

Containment Starts

Containment Takes Effect



4:00 a.m. PST
Containment
In the Skitter
Core



iNOC Phone: The next wave of inter-NOC Communication

iNOC DBA – Why ?

- **ISPs need to coordinate for attacks. They need to talk.**
- **It is not easy to reach the right contact. The engineer you are trying to reach will not likely pick up the phone.**
- **Solution: Dedicated NOC Hotline System**
INOC-DBA: *Inter-NOC Dial-by-ASN*

What is the problem?

- **ISPs needed to talk to each other in the middle of the attack.**
- **Top Engineers inside ISPs often do not pick up the phone and/or screen calls so they can get work done. If the line is an outside line, they do not pick up.**
- **Potential solution – create a dedicated NOC Hotline system. When the *NOC Hotline* rings, you know it is one of the NOC Engineer's peers.**

iNOC DBA Hotline

Cisco.com

- The iNOC Hotline is used to get directly to peers.
- Numbering system based on the Internet:
ASnumber:phone
109:100 is Barry's house.
- SIP Based VoIP system, managed by Packet Clearing House (www.pch.net), and sponsored by Cisco.
- www.pch.net/inoc-dba



How to Participate

Cisco.com

- **With your own phones:**

PCH needs your MAC address, contact info, ASNs, and extension number.

- **With PCH phones:**

PCH need your contact and shipping address, ASNs, and extension number.

How is iNOC being used today?

Cisco.com

- **Used during attacks like Slammer (Barry was using his iNOC phone at home to talk to ISPs in the early hours of Slammer).**
- **D-GIX in Stockholm bought 60 phones for their members (ISP's around Stockholm)**
- **People have started carrying around their SIP phones when traveling**
- **Many DNS Root Servers are using the iNOC Hotline for their phone communication.**
- **General Engineering consultation – ISP Engineers working on inter-ISP issues.**

More Information

Cisco.com

- **General information:**
<http://www.pch.net/inoc-dba/>
- **Mailing-list archive:**
<http://www.pch.net/resources/discussion/inoc-dba/archive/>
- **Who's participating:**
<http://www.pch.net/inoc-dba/directory/>

Exchanges	Carriers		Associations	
LINX	SD-NAP	UUnet	AT&T	ARIN
PAIX	LAIIX	Sprint	SBC	APNIC
Equinix	NSP-IXP2		C&W	AOL/T-WRIPE/NCC
AMS-IX	NOTA	Genuity	RCN	ICANN
MAEs	OIX	Verio/NTT	TDS	ISC



Build the Communications Channels to your Vendors

Over Dependence on Vendors – Danger!

Cisco.com

- **Operators who use their Vendors as Tier 2 and higher support endanger their network to security risk.**

Vendors are partners with an operator. They should not maintain and troubleshoot the entire network.

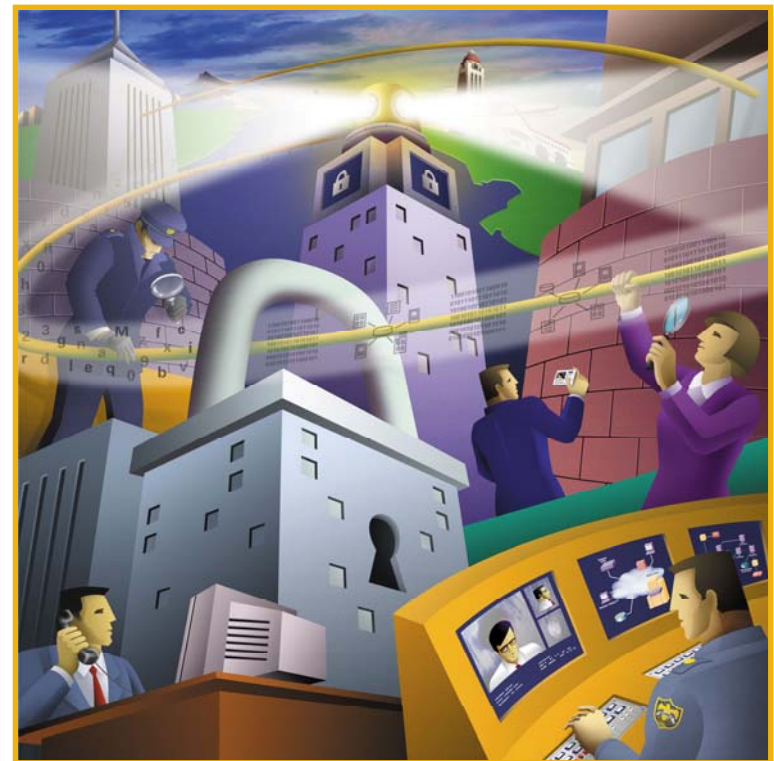
Way too many operators today see a problem on a router and then call the vendor to fix it.

This is not working with Turbo Worms.

Hardware Vendor's Responsibilities

Cisco.com

- The roll of the hardware vendor is to support the network's objectives. Hence, there is a very synergistic relationship between the ISP and the hardware vendor to insure the network is resistant to security compromises



What you should expect from your vendor?

Cisco.com

- **Expect 7x24 Tech Support (paid service)**
- **You should not expect your vendor to run your network.**

Hardware Vendor's Responsibilities

Cisco.com



- **Cisco System's example:**

Operations people working directly with the ISPs

Emergency reaction teams (i.e. PSIRT)

Developers working with customers and IETF on new features

Security consultants working with customers on attacks, audits, and prosecution

Individuals tracking the hacker/phracker communities

Consultants working with governments/law enforcement officials

The Cisco PSIRT

Cisco.com

- **P**roduct **S**ecurity **I**ncident **R**esponse **T**eam
- Handling of **Cisco** product vulnerabilities
- Customers report **security** problems with Cisco products to PSIRT (not to TAC)
- The PSIRT:
 - ... assists in finding immediate workarounds
 - ... works with engineering to fix vulnerabilities
 - ... escalates within Cisco if necessary
 - ... helps customer in fixing the problem
- PSIRT is one of two Cisco FIRST Teams (our internal InfoSec is the second FIRST Team)

Tools and Techniques



More Questions

Cisco.com

- **Have you taken the proactive step to be Prepared?**

- Build and Prepare OpSEC team**

- Securing the router**

- Securing the routing protocols**

- Route filtering**

- Black hole filtering**

- Sink Hole routers/networks**

- Packet filtering**

- Securing the network**

- Default routes, ISPs, and security**

Phase 1 - Preparation

- Preparation is critical!

You know your *customers* are going to be attacked

It is not a matter of **if** but **how often and how hard**

The Internet is not a nice place anymore!

Think **battle plans**

- Militaries know the value of planning, practice, drilling and simulation

Those that are prepared will be victorious.

The Preparation Problem

CEO, “Customer X just called and said they’ve been DOSed for the past 12 hours. What are we doing about it?”

Operations Chief, “We’re working on it.”

CEO, “How long before it is fixed?”

Operations Chief, “We’re working on it.”

CEO, “What exactly are we doing about it?”

Operations Chief, “We’re working on it.”

CEO, “Do you know how to get the customer up and running?”

Operations Chief, “It is all Cisco’s fault – they should fix the *DOS problem*.”

Prepare: Tools and Techniques

Cisco.com

- **Prepare your Tools!**

Do you have all your SNMP tools deployed?

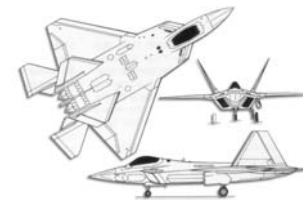
Do you have all your SYSLOG tools deployed?

Do you have your ACLs created?

Do you have your scripts created?

Have you built and tested your *Sink Hole* and *Backscatter* tools?

Etc.

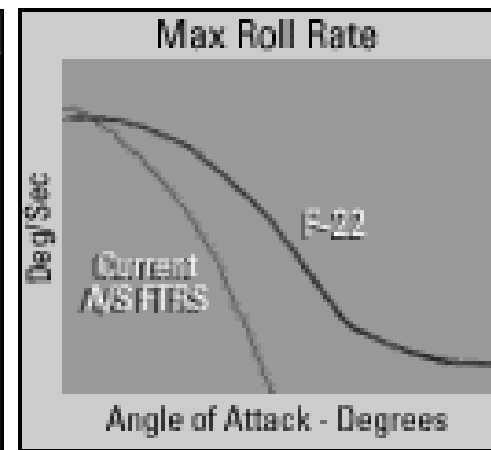
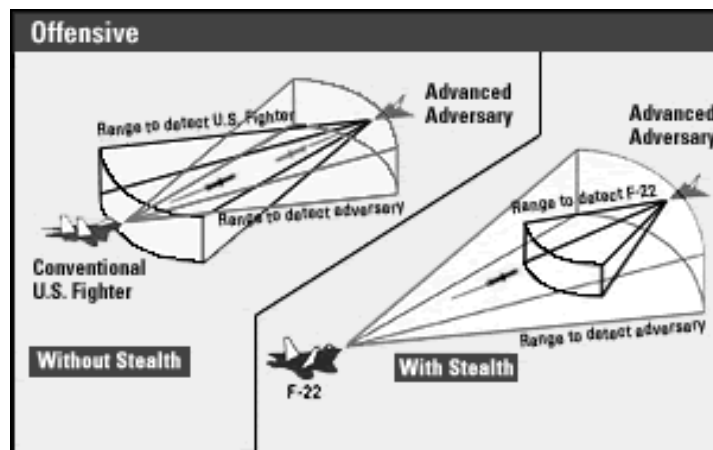


Are you pushing the *envelop*?

- **Know your Equipment and Infrastructure:**

Know the Performance Envelop of all your equipment (routers, switches, workstation, etc). You need to know what your equipment is really capable of doing. If you cannot do it your self, make is a purchasing requirement.

Know the capabilities of your network. If possible, test it. Surprises are not kind during a security incident.



Are you pushing the *envelop*? *Get Real!*

Cisco.com

- Operator, “I tired to push my aircraft to 70,000 ft and it stalled.”
- Vendor, “But the aircraft was only designed for a 50,000 ft ceiling.”
- Operator, “I need it to go to 70,000 ft, so you should make that happen.”
- Vendor, “But that is not going to happen, 50K ft is the only thing it can do. You knew that when you bought it.”
- Operator, “Your equipment sucks if you cannot exceed you design specs.”

Network Size and Complexity

Cisco.com

- **Are these traffic patterns normal for our network?**
- **What is using up all of our bandwidth?**
- **Angry customers are calling - what happened?**
- **Why can't we reach that server, network or AS?**
- **Has another provider hijacked our routes?**
- **Should we buy more transit or peer directly?**
- **Should we change these BGP attributes or policies?**

Preparation (1)

- **Preparation: All the work the ISP does to prepare the network, create the tools, test the tools, develop the procedures, train the team, and practice.**

#1 Most critical phase of how a ISP responds to a security incident.

Big difference between ISPs who have prepared and those who have done nothing.

What can you do?

- 1. Ask lots of security questions. Cisco is not holding anything back, we just have way too much information for any one person to process.**
- 2. Follow-up on security questions. Your Cisco contacts may have to dig for the answers. Don't let them get distracted.**

Tools – Top 4

Cisco.com

1. **SNMP**
2. **Syslog**
3. **Netflow**
4. **Sinkhole/HoneyNet**

Interesting Un-Tapped Tools

Cisco.com

- **DNS Logs**
- **BGP Logs (RIPE Database)**
- **DShield/MyNetWatchman**
- **IPSLA**

CISCO SYSTEMS

