Managed Security Services

Der Weg,
wie die Verantwortung getragen werden kann!

Christoph Altherr
System Engineer – Security

Agenda

- Enterprise Security Threats & Challenges
- Cisco Remote Management Services Overview
- Cisco Security Remote Management Services
- Operational Approach Based on ITIL Framework
- Cisco IPS Signature Management Service
- Conclusion – Why Cisco!

Enterprise Security Threats & Challenges
Increasing the Business Impact of IT

Business Objectives

1

Increasing Revenues and Opportunity

Reacting in real time to customer and market demands
Driving innovative products and services to market faster

2

Increasing Business Resiliency and Agility

Greater flexibility to use resources where and when needed
Greater ability to interact with customers and partners as appropriate

3

Improving Customer Relationships

Strengthening trust and confidence
Building long-term business partner relationships

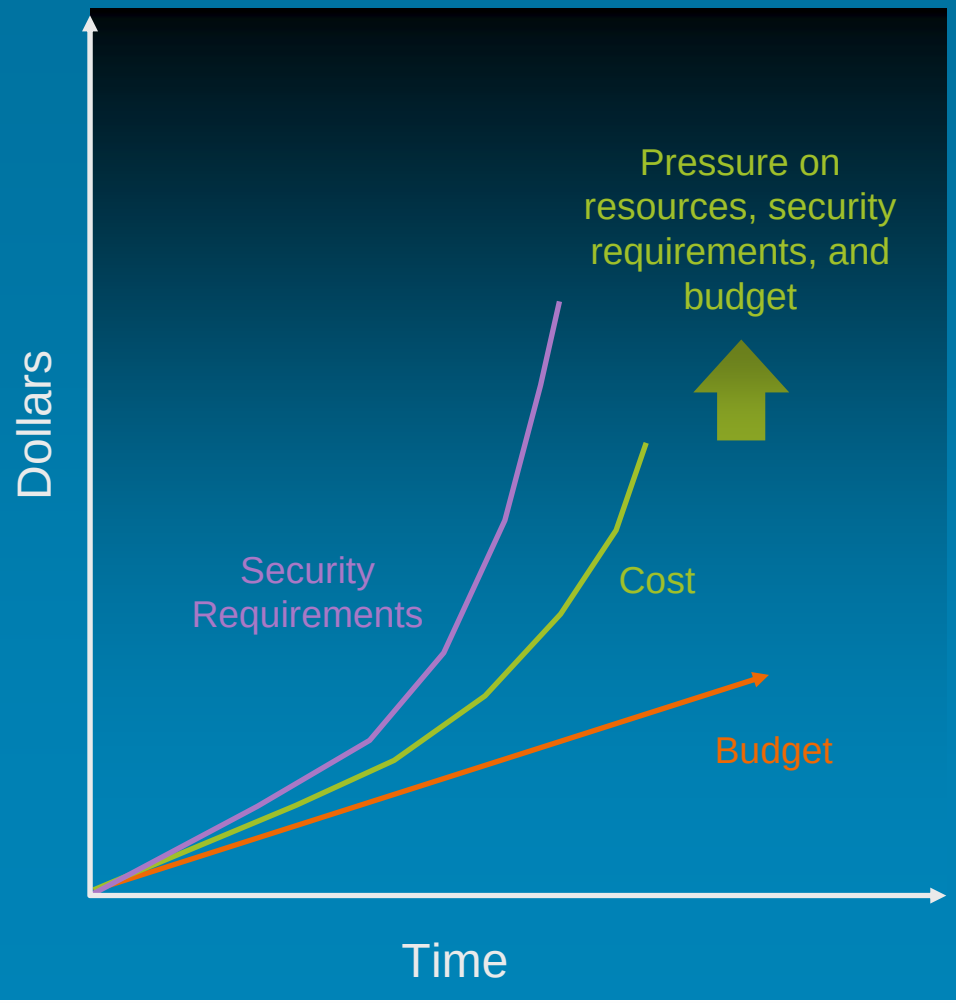
4

Increasing Productivity, Efficiency While Reducing Costs

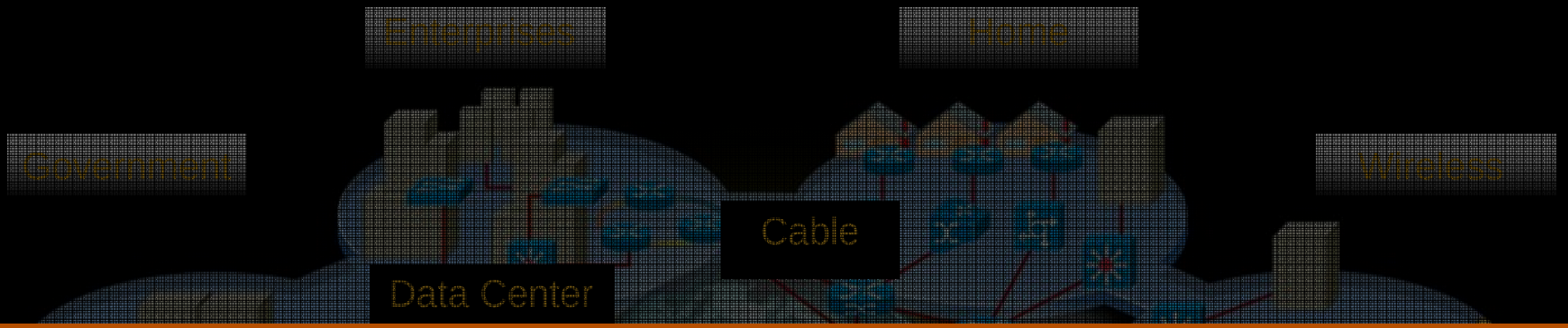
Greater process efficiency, monitoring and reporting on activity
Reduce the escalating costs of IT, achieving ROI expectations

Enterprise Security Threats & Challenges
Chief Security / Information Officer Challenge

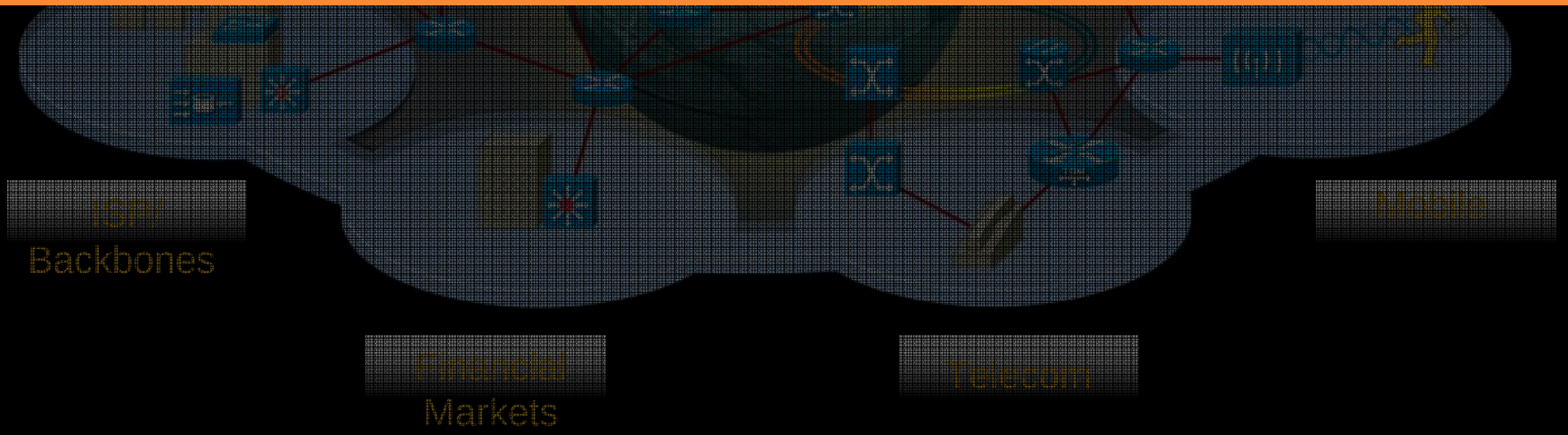
- Protect the business from security threats
- Improve security staff productivity
- Reduce total cost of ownership for network



Enterprise Security Threats & Challenges
Constantly Evolving Network Driven by Innovation

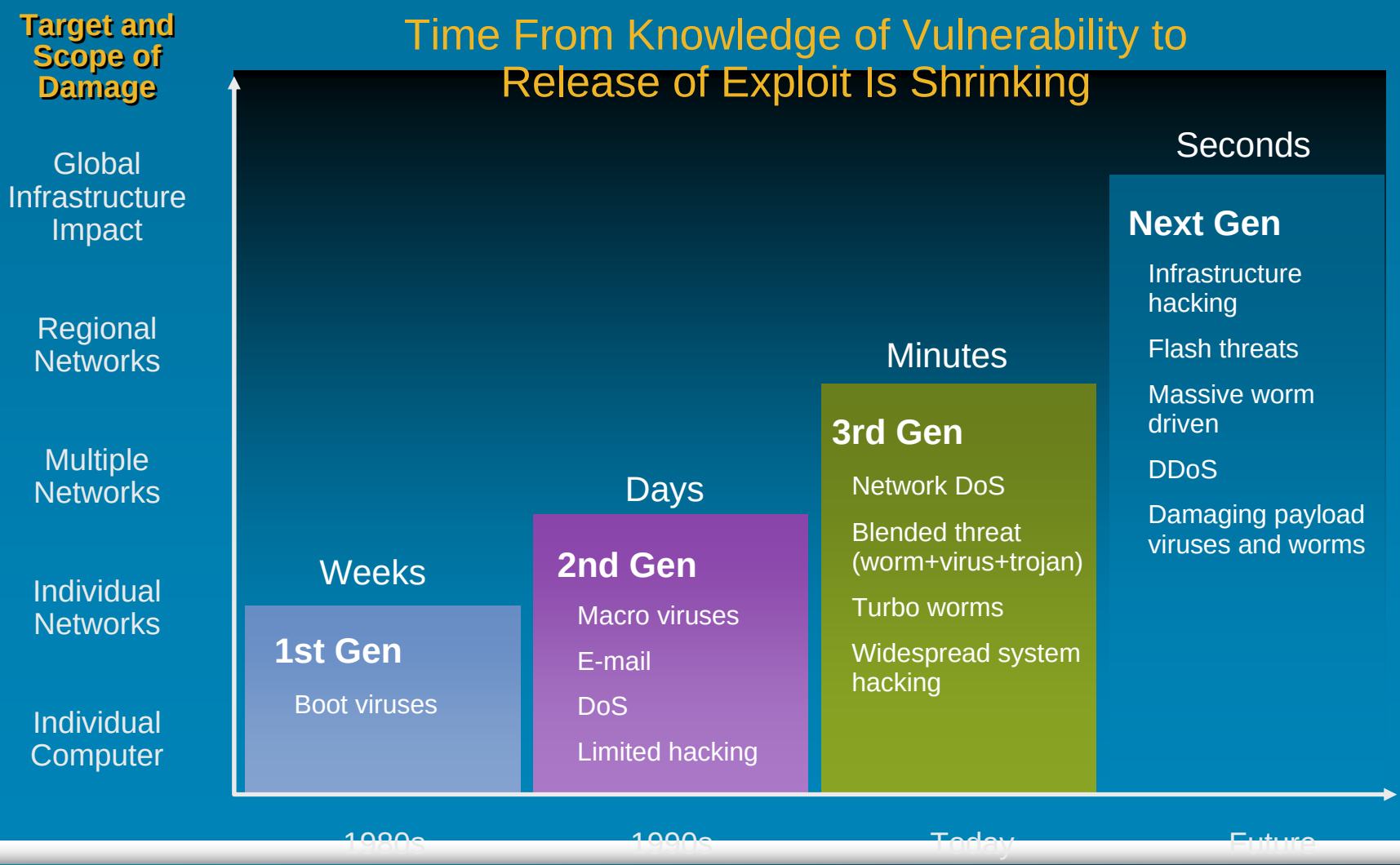


Everything Is a Point of Attack
Everything Must Be Defended



Network Is Global and Interconnected

Enterprise Security Threats & Challenges
Evolution of Security Challenges

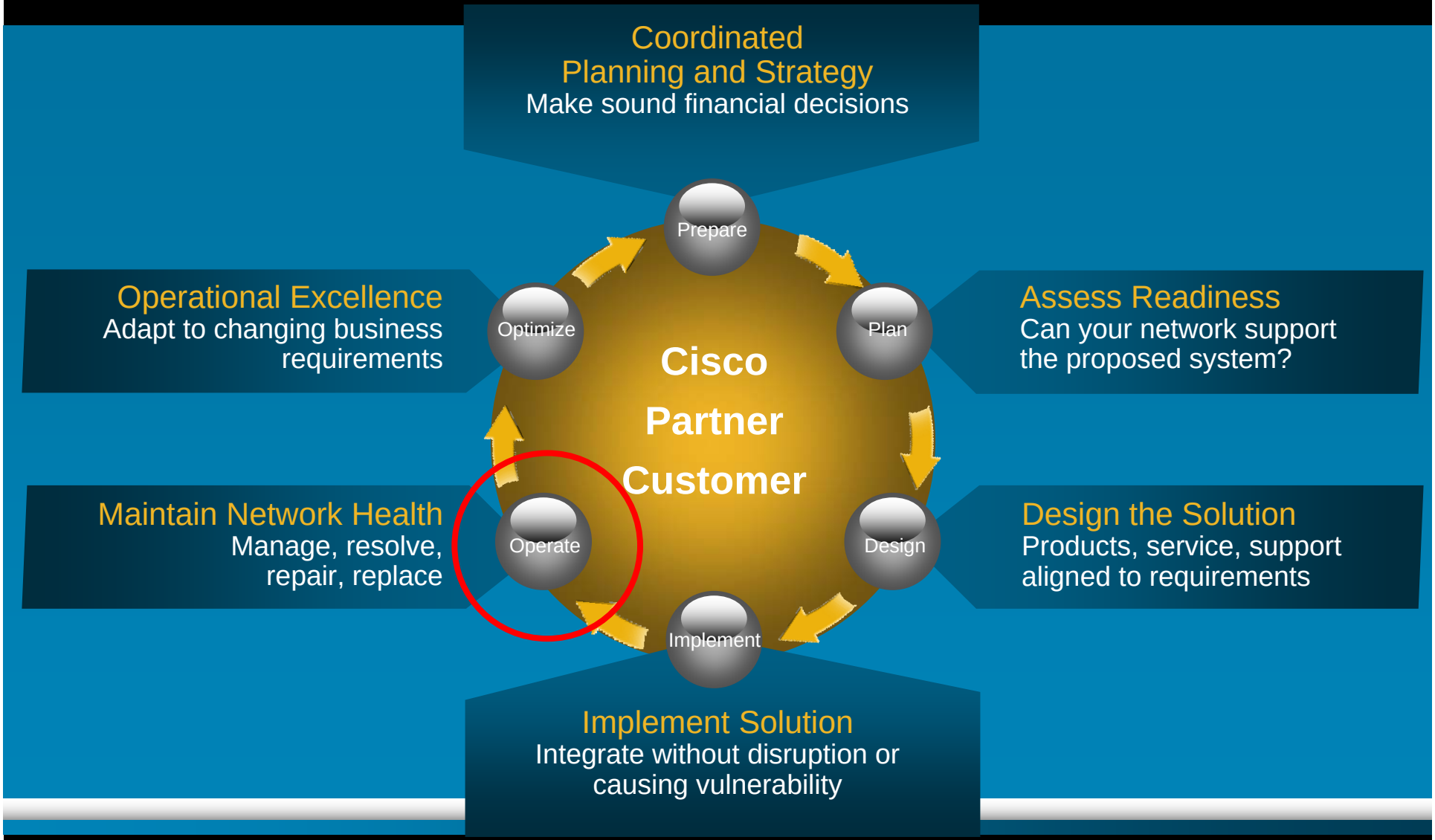


Agenda

- Enterprise Security Threats & Challenges
- Cisco Remote Management Services Overview
- Cisco Security Remote Management Services
- Operational Approach Based on ITIL Framework
- Cisco IPS Signature Management Service
- Conclusion – Why Cisco!

Cisco Remote Management Services Overview

Cisco: Lifecycle Approach to Security Services



Cisco Remote Management Services Overview
Enterprise Support Options

	Outsourcing	Out-Tasking	Do it Yourself
What	3rd party performs all network security functions	3rd party performs day-to-day management on selected network security components	Customer performs all functions
How	▪ Outsource entire network security function	▪ Typical: Monitoring, MACD, incident resolution, device updates ▪ Optional: optimization, system upgrades	▪ Buy/integrate tools ▪ Develop skills and organization ▪ Develop processes and knowledge base
Benefits	▪ Focus on competitive differentiation ▪ Reduces network security staffing costs	▪ Competitive differentiation ▪ 24x7 access to security expertise ▪ Agility	▪ Control own destiny ▪ Leverage existing resources
Pitfalls	▪ Loss of control ▪ Expensive (migration and governance costs) ▪ Risk in migration ▪ Loss of agility	▪ Governance overhead ▪ Possible lack of control ▪ Vendor skill depth	▪ Expensive, time-consuming ▪ Integration issues ▪ Ongoing skills training

Cisco Remote Management Services Overview
Remote Management Services Organization

- Deliver Cisco Remote Management Services
- Singular focus with a proven track record
  - Experience in Remote Management Services—Security, Foundation Technology, and Unified Communications
  - Currently delivering Security Remote Management Services for VPN, Access Control, and Intrusion Prevention
  - Highest customer loyalty levels within ROS
- Security services expertise
  - Security capabilities built on Cisco Security Operations Center
  - Approximately 3000 security devices under management
  - Collect, analyze, remediate, and report on over 1.5 million network, security, and performance events every 5 minutes




People | Process | Tools | Knowledge

CSI4

I don't think we need the text I put in red
What is SOC? should spell out
Text in green is my change
These will revert back to white once you approve
Charlene

Cisco Remote Management Services Overview
Services Portfolio – Cisco Brand and CBR

Security

- Access Control Management
- Intrusion Management
- VPN Management
- IPS Signature Management
- Collaborative RMS

Unified Communications

- Remote Management
  - Call Manger
  - Unity

TelePresence

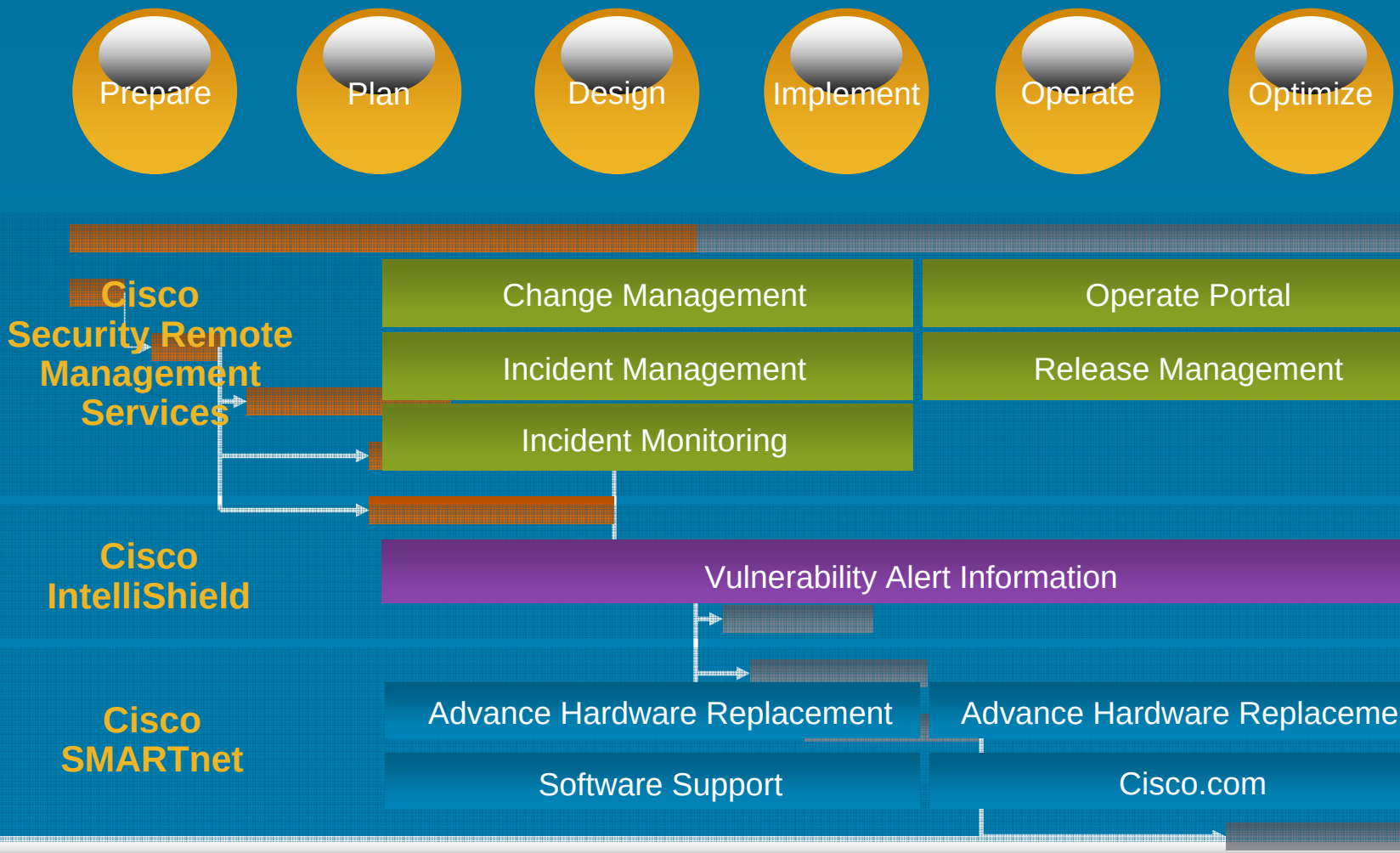
- Select Operate
- Remote Assistance

Agenda

- Enterprise Security Threats & Challenges
- Cisco Remote Management Services Overview
- Cisco Security Remote Management Services
- Operational Approach Based on ITIL Framework
- Cisco IPS Signature Management Service
- Conclusion – Why Cisco!

Cisco Security Remote Management Services

The Cisco Services for Security Portfolio



CSI5 Is there a reason why Advance Hardware Replacement is on the same level as IntelliShield?

CSI8

Cisco Security Remote Management Services
Summary

	VPN Management	Access Control Management	Intrusion Prevention
Technologies	Routers Layer 3 Switches VPN Concentrators Firewalls ISRs ASAs	Routers Layer 3 Switches Firewalls ISRs ASAs	IDS IPS Routers w/ IOS/IPS Routers w/ NM-CIPS IDSMs ASAs w/ SSM-AIP
Services	Fault Monitoring Performance Monitoring Tunnel Monitoring Incident Management Change Management Configuration Management	Fault Monitoring Performance Monitoring Incident Management Change Management Configuration Management Release Management Access Policy Reviews	Fault Monitoring Performance Monitoring Incident Management Security Incident Response Change Management Configuration Management Release Management Tuning
Metrics	Availability Response to Logical MACs Response to Incidents	Availability Response to Logical MACs Response to Incidents Audit Log and Policy Review	Availability Response to Logical MACs Response to Incidents Security Event Metrics

CSI8 What are MACs?

Cisco Systems, Inc.; 04.10.2007

Cisco Security Remote Management Services
Access Control Management

- Service Features
  - Incident Management
    - Fault Monitoring and management
    - Monitoring and management of security incidents through syslog
  - Change and Release Management
    - Access policy troubleshooting
  - Configuration Management
    - Regular configuration backups
    - Configuration review every 6 months

- Service Benefits
  - Coverage for the broad Cisco installed base in security
  - Maximizes the value of Cisco security devices by insuring that they are operational and processing events correctly
  - Saves time, money, and effort by helping customers scale their change processes

Cisco Security Remote Management Services
Intrusion Prevention

- Service Features
  - Incident Management
    - Fault Monitoring and management
      Monitoring and management
      of security incidents
      - Classification, investigation, isolation
      - Impact assessment, notification,
      - Recommendations
    - Automatic blocking, shunning,
      TCP reset
    - Manual shunning/update
      of access control
    - Manual port configuration
  - Change and Release Management
    - Deployment of signature packs
    - Lifecycle tuning of signature configuration
    - Managed access control response
      to detected threat

- Service Benefits
  - Coverage for the broad Cisco installed base in Security
  - Helps customers understand the scope and impact of security incidents
  - Provides customers with recommendations to assist in next-steps and preventing future incidents
  - Reduces the noise generated by IDS/IPS devices by tuning over a customer's lifecycle
  - Provides a real-time intelligent response to threats in the form of changes
  - Customers have access to security expertise from Cisco at a monthly fee, reacting to threatening incidents for them

Cisco Security Remote Management Services
Service Level Objectives

Key Performance Indicator (KPI)	KPI Details	Cisco Security Access Control Remote Management Service	Cisco Security Intrusion Prevention Remote Management Service	Cisco Security Virtual Private Network (VPN) Remote Management Service
MTTN	Notify Customer of Fault, Performance or Security Incidents within X minutes	15 min	15 min	15 min
MTTInv	Investigate Fault & Performance Incidents within X minutes	30 min	30 min	30 min
MTTBa	Begin Analysis of Security Incidents within X minutes	30 min	30 min	n/a
MTTCa	Complete Analysis and Provide Recommendations for Remediating Security Incidents within X minutes	75 min	75 min	n/a
MTTIso	Isolate Root Cause of Fault & Performance Incidents within X minutes	75 min	75 min	75 min
MTTR	Resolve Fault & Performance Incidents within X hours	P1: 4 hours P2: 24 hours P3: 72 hours	P1: 4 hours P2: 24 hours P3: 72 hours	P1: 4 hours P2: 24 hours P3: 72 hours

Details included in the Cisco Security Remote Management Services Description

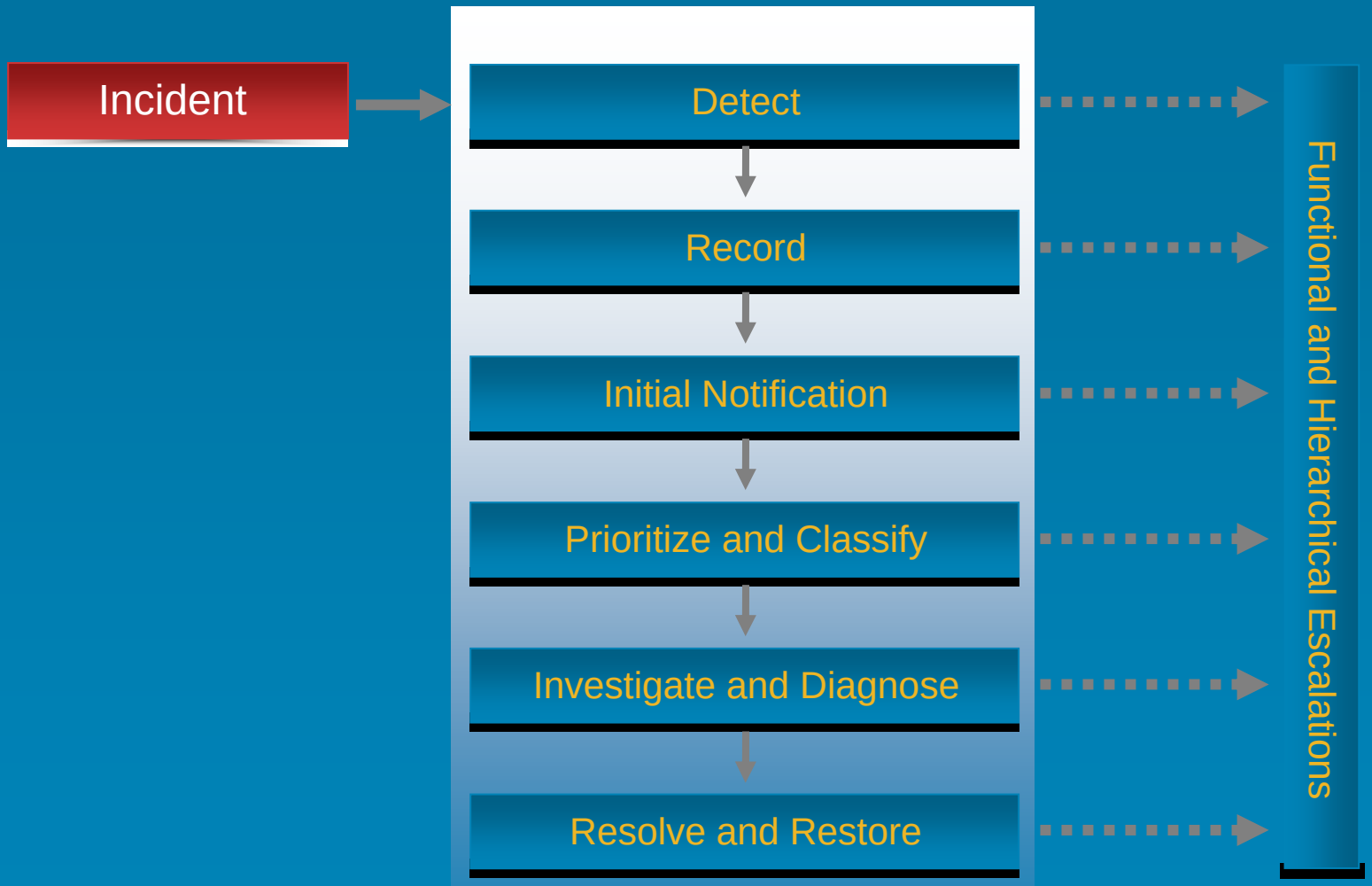
Agenda

- Enterprise Security Threats & Challenges
- Cisco Remote Management Services Overview
- Cisco Security Remote Management Services
- Operational Approach Based on ITIL Framework
- Cisco IPS Signature Management Service
- Conclusion – Why Cisco!

Operational Approach Based on ITIL Process
ITIL Foundation

Cisco

Operational Approach Based on ITIL Process
Incident Management

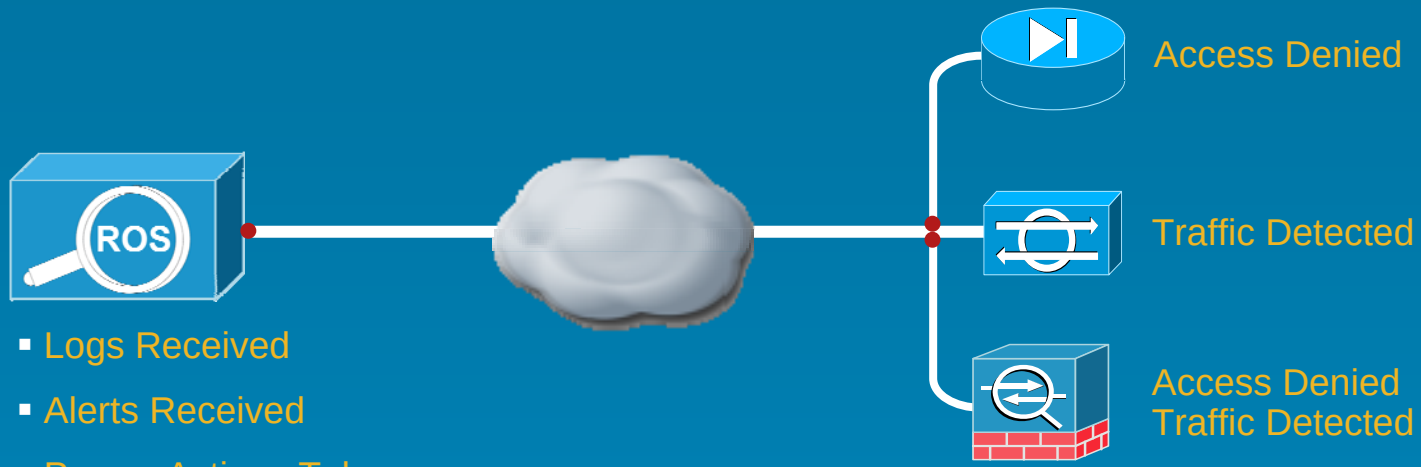


Operational Approach Based on ITIL Process
Incident Management - Monitoring

- Can Cisco reach the device?

Operational Approach Based on ITIL Process
Incident Management - Monitoring

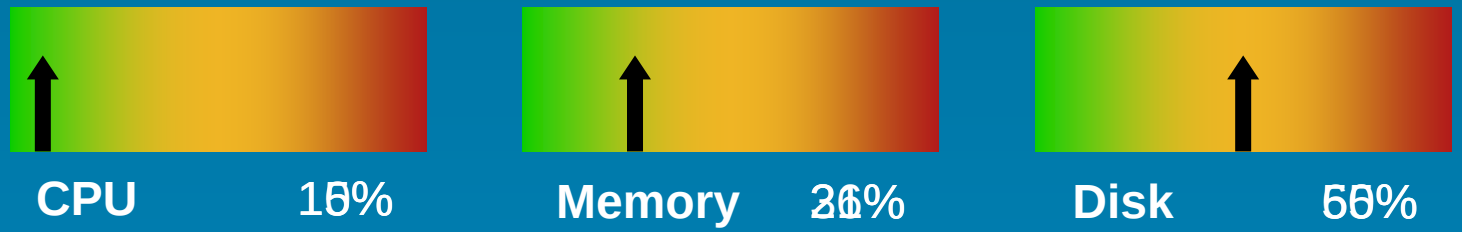
- Can Cisco reach the device?
- Is the device performing essential functions?



Incident Monitoring

Operational Approach Based on ITIL Process
Incident Management - Monitoring

- What is the performance and capacity of the device?



Performance Monitoring

Incident Monitoring

Operational Approach Based on ITIL Process
Incident Management - Monitoring

- Monitor for evidence of security issues, and declare Security Incidents?

Security Incident Monitoring

Performance Monitoring

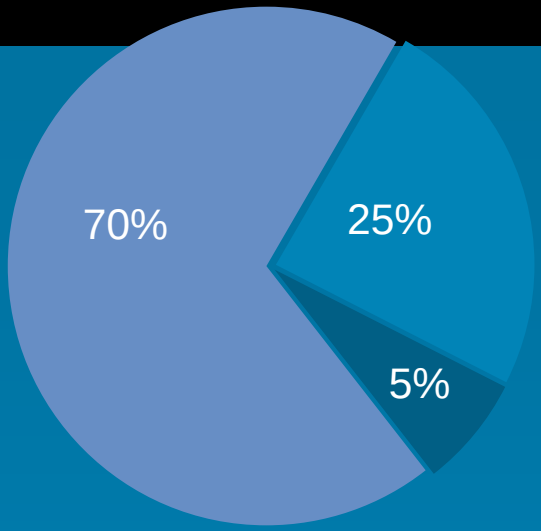
Fault Monitoring

Operational Approach Based on ITIL Process
Incident Management - Monitoring

1. Start ticket via proactive incident alarm (alarm comes after verification)
2. Verify alarm
3. Correlate with other alarms occurring at same time

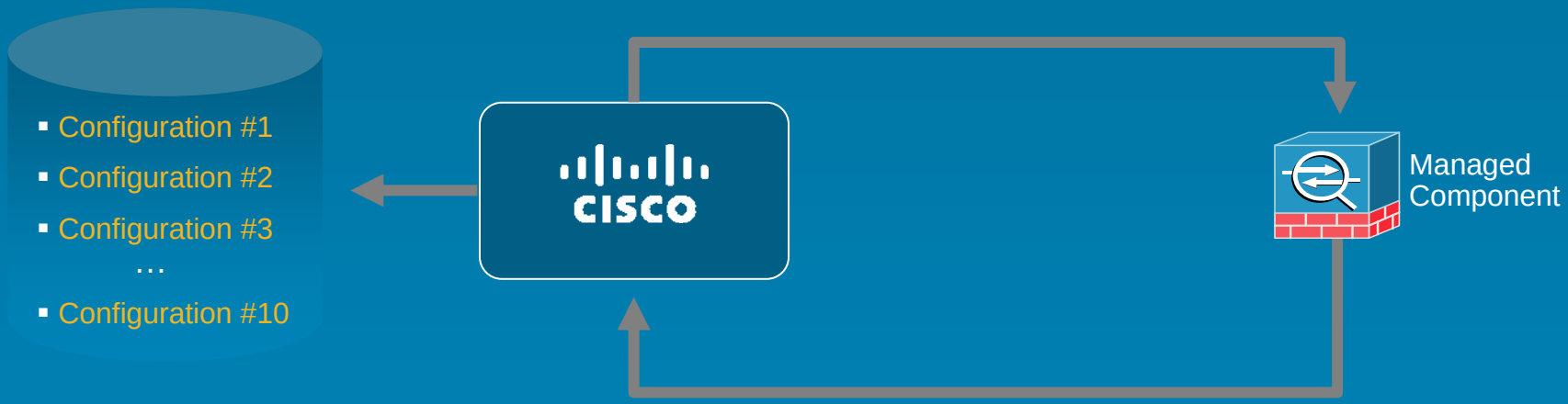
----- (Reactive Support Starts Here) -----

1. Generate ticket and notify customer
2. Ticket is picked up and analysis begins
3. Isolate and prioritize incident
4. Complete analysis or remediation (provide recommendation or perform resolution)

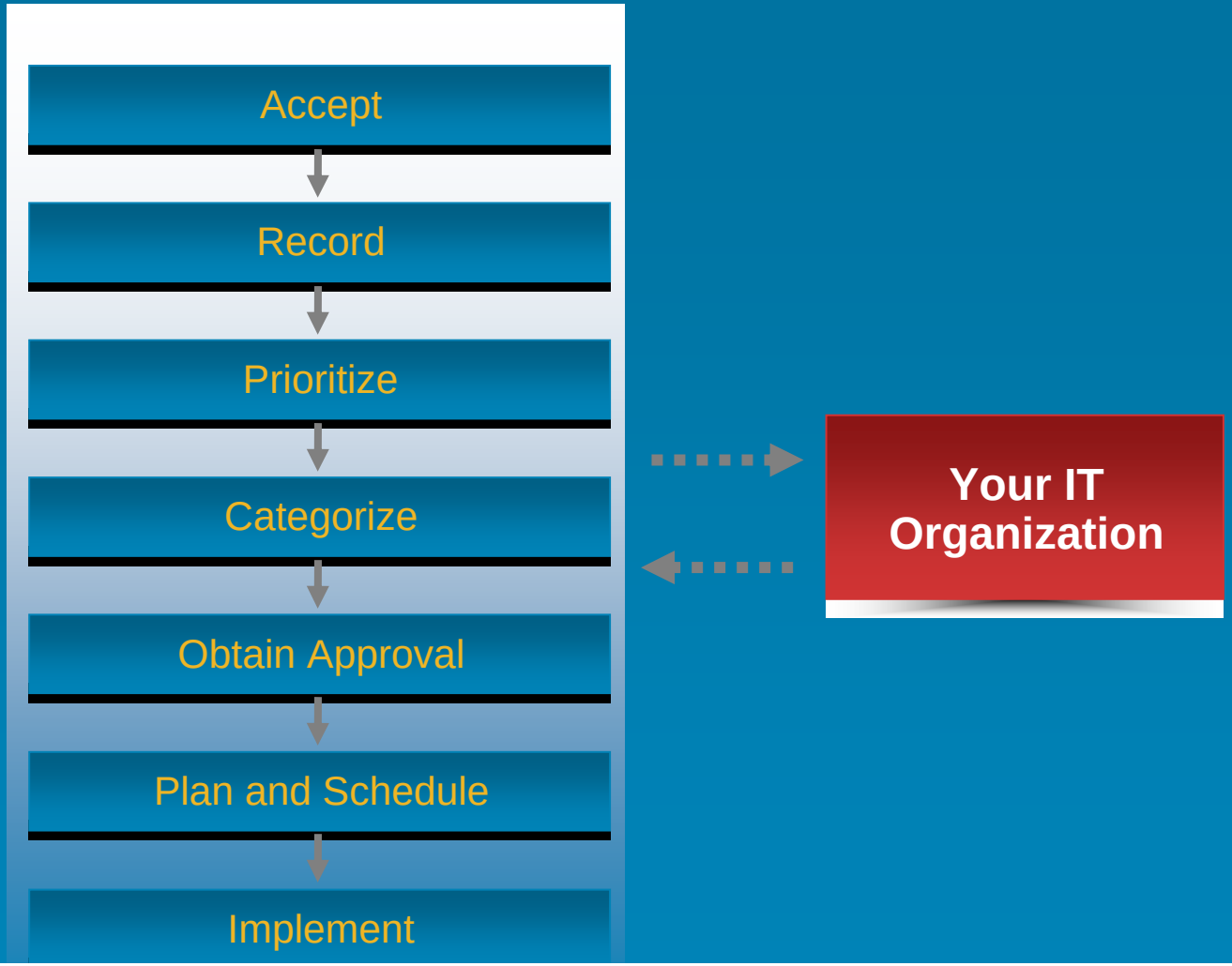


Operational Approach Based on ITIL Process
Configuration Management

Daily Backups of Device Configurations

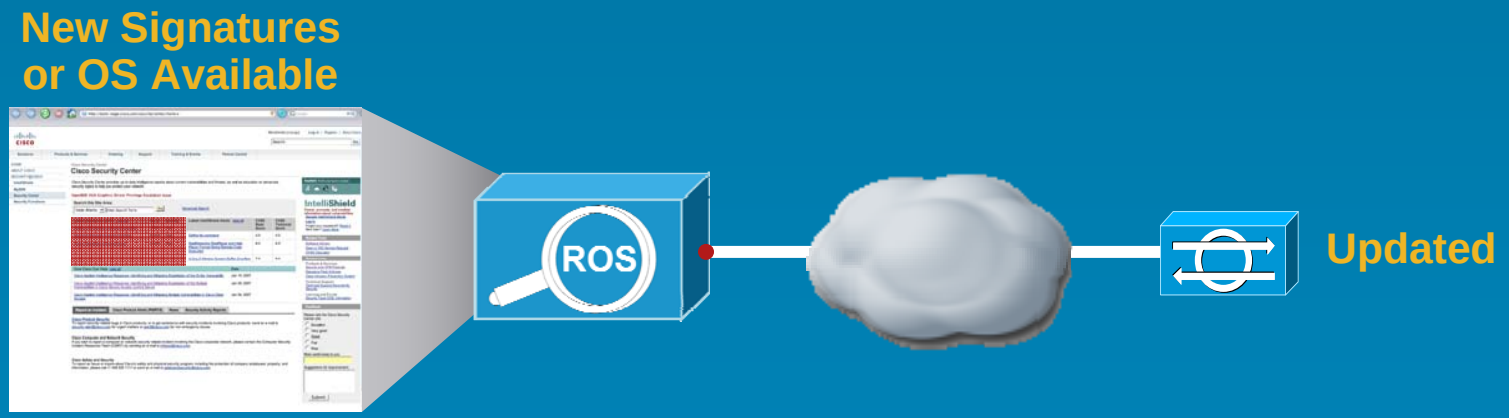


Operational Approach Based on ITIL Process
Change Management

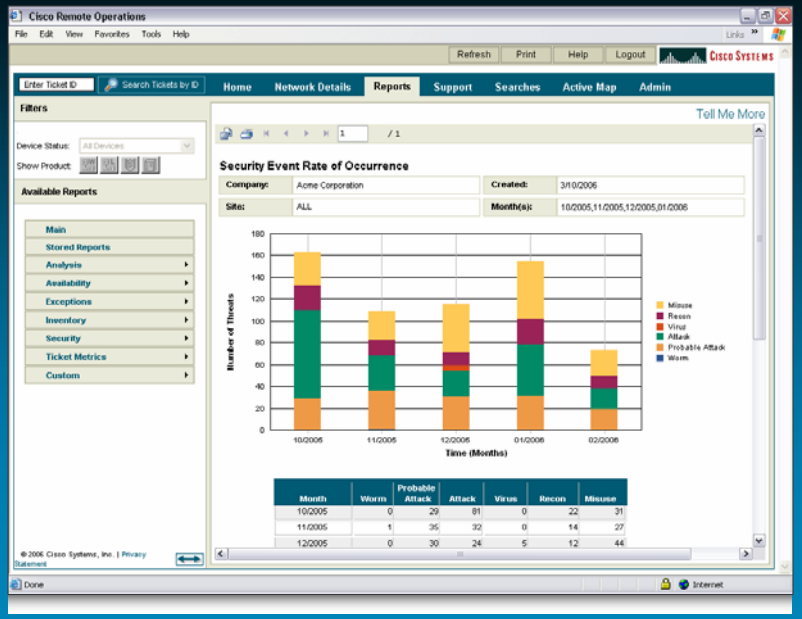


Operational Approach Based on ITIL Process
Release Management

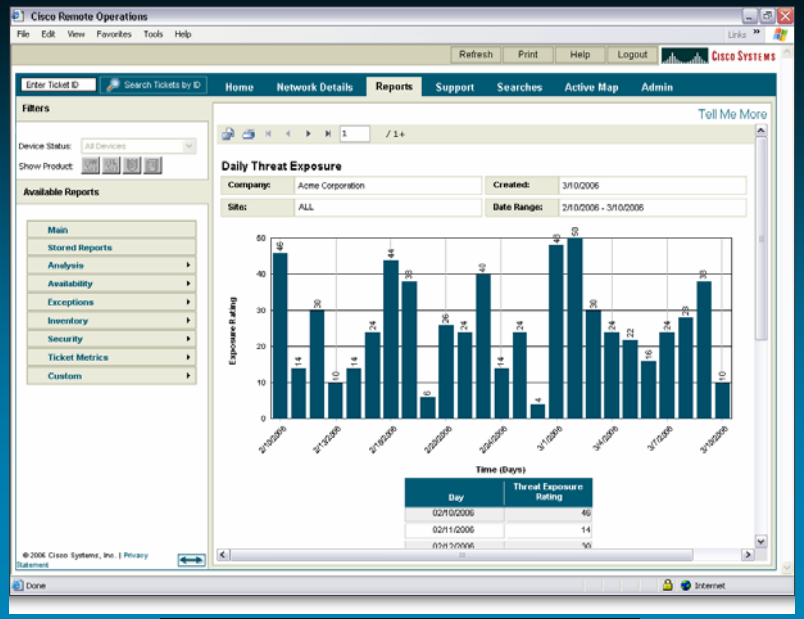
- Same day distribution of signature updates
- OS updates during next scheduled maintenance
- Ongoing tuning in response to events



Operational Approach Based on ITIL Process
Management Reporting

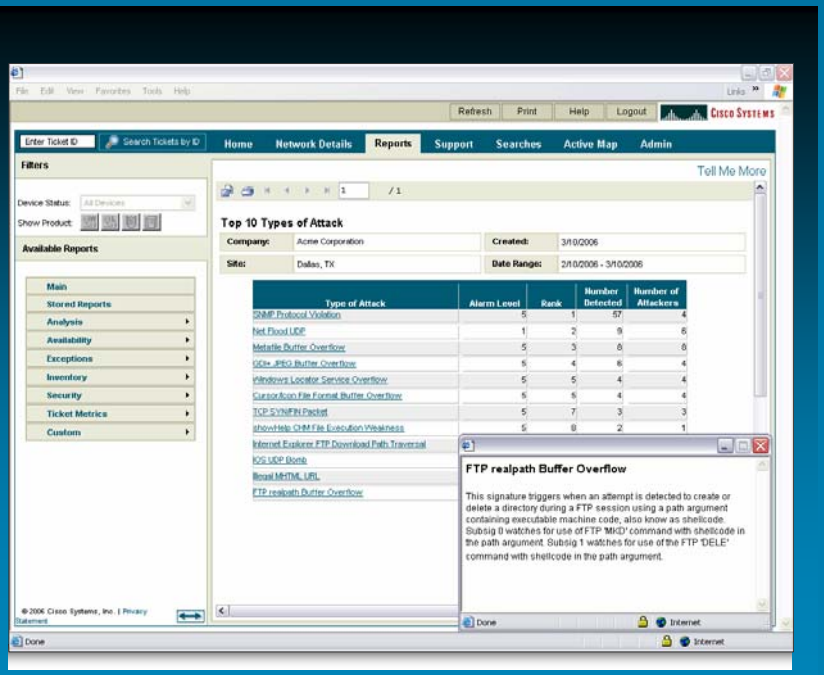


Rate of Occurrence

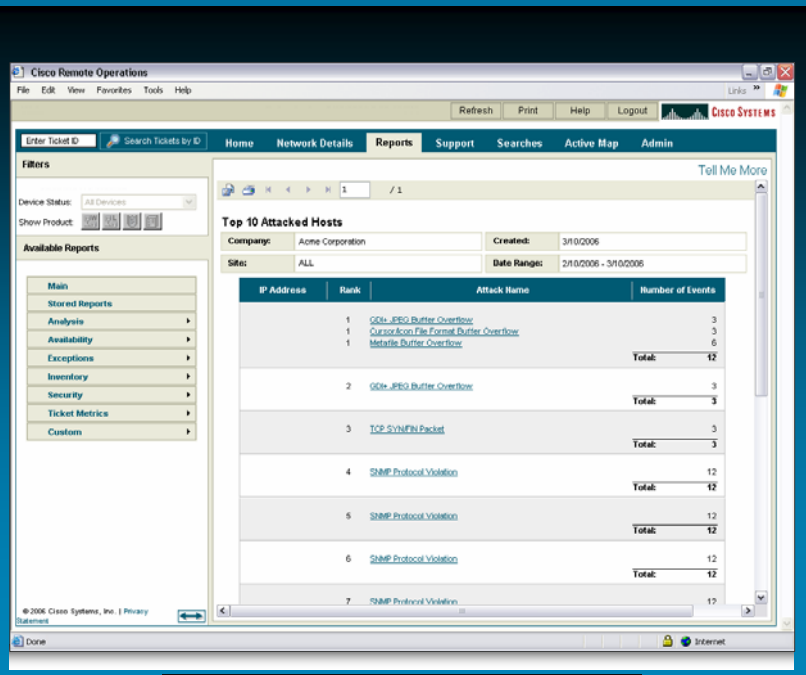


Threat Exposure

Operational Approach Based on ITIL Process
Management Reporting



Top 10 Types of Attack



Top 10 Sources/ Destinations

Agenda

- Enterprise Security Threats & Challenges
- Cisco Remote Management Services Overview
- Cisco Security Remote Management Services
- Operational Approach Based on ITIL Framework
- Cisco IPS Signature Management Service
- Conclusion – Why Cisco!

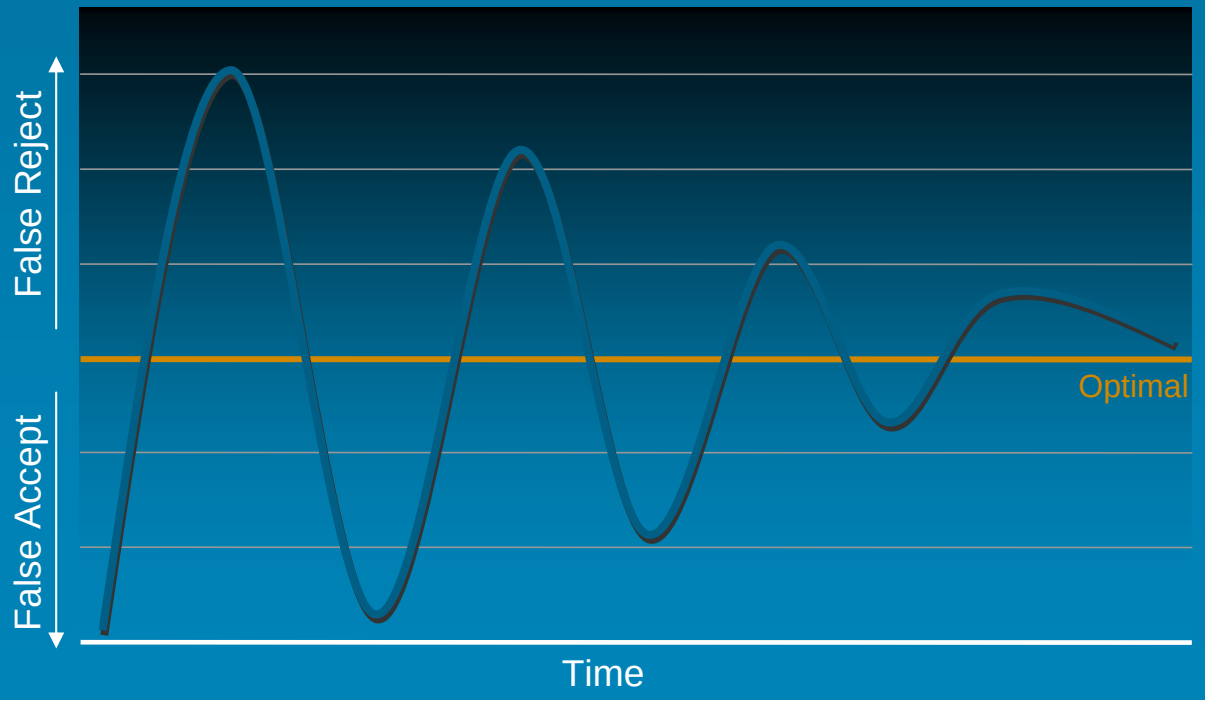
Cisco IPS Signature Management Service
Service Features Overview

- Automatic Distribution of New Signatures
  - New Cisco IPS signatures pushed to entitled* IPS devices with 24 hours of release
- Remote Signature Tuning
  - Review applicable alarm activity for evidence of benign triggers within 2 weeks following signature distribution
  - Implement filters for benign triggers to reduce benign alarms
- Notification Activities
  - Notify Customer via email within 4 hours of the completion of signature distribution & tuning activities

* Concurrent coverage by Cisco Services for IPS is required for successful push/distribution of signature updates to IPS solutions

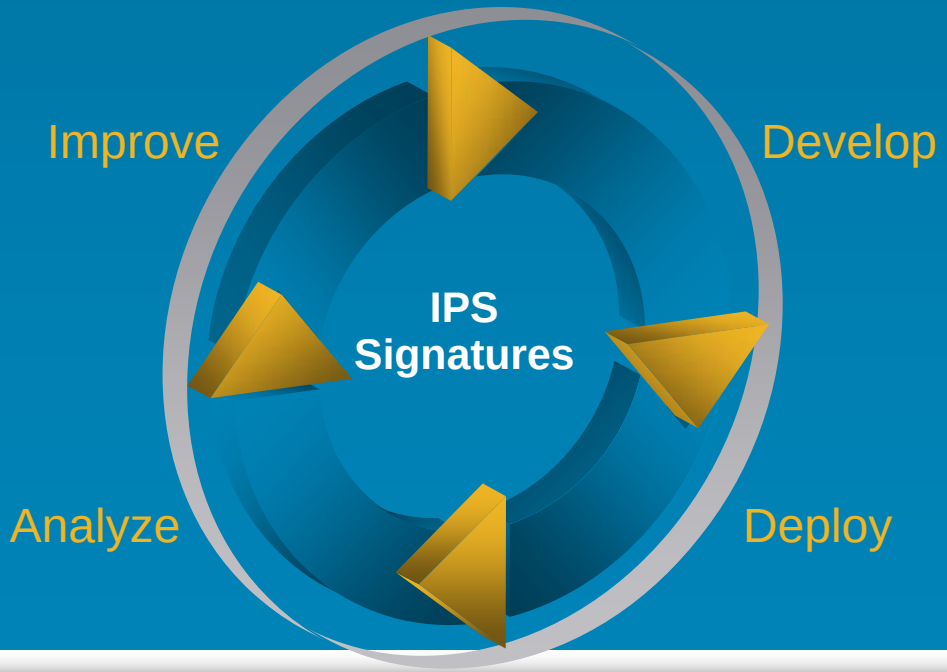
Cisco IPS Signature Management Service
Importance of Signature Tuning

- Analysis and careful tuning after every signature update results in more accurate event detection and effective protection
- What about new systems, new services, and evolving applications? Regular tuning helps intrusion prevention systems move at the speed of the business



Cisco IPS Signature Management Service
Importance of Expertise

- Intelligent analysis means tuning the right signatures the right way; maximizing visibility and minimizing operational complexity
- Knowing the global threat environment and your business environment enables analysts and technicians to keep improving signature tuning

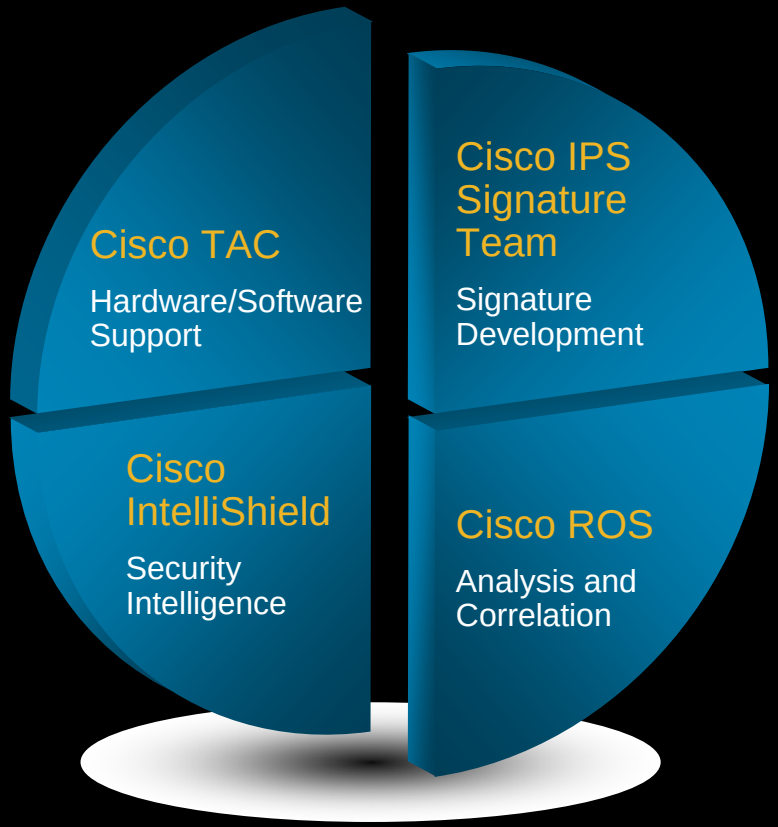


Agenda

- Enterprise Security Threats & Challenges
- Cisco Remote Management Services Overview
- Cisco Security Remote Management Services
- Operational Approach Based on ITIL Framework
- Cisco IPS Signature Management Service
- Conclusion – Why Cisco!

Conclusion – Why Cisco!
Security Expertise

- Cisco Security Remote Management Services and Cisco IPS Signature Management Service leverage four centers of security expertise



- Deep expertise in data networking, IP Communications and Security
- Integrated into security product plans
- Integrated within Lifecycle Services methodology—end-to-end services

CSI20 delete across TS

Cisco Systems, Inc.; 04.10.2007

Conclusion – Why Cisco!
Focus on Customer Satisfaction

- Standardized ITIL-based processes drive consistent customer experience
- Cisco Security Remote Management Services include Service Level Objectives (SLO)
- SLO goals published on the Cisco Remote Management Portal

"I'm very impressed with the level of ownership the entire technical team has taken with our account. Each experience that I have had, the technicians [were] very knowledgeable in their field. Everyone was dedicated to resolving the problem as if they were an employee."

-IT Manager, IT Services Company

CSI14 changes in green

Cisco Systems, Inc.; 04.10.2007