# SEC-2030

# Deploying IPS Solutions

Munawar Hossain

# Recuerde siempre:

- Apagar su teléfono móvil/pager, o usar el modo “silencioso”.

- Completar la evaluación de esta sesión y entregarla a los asistentes de sala.

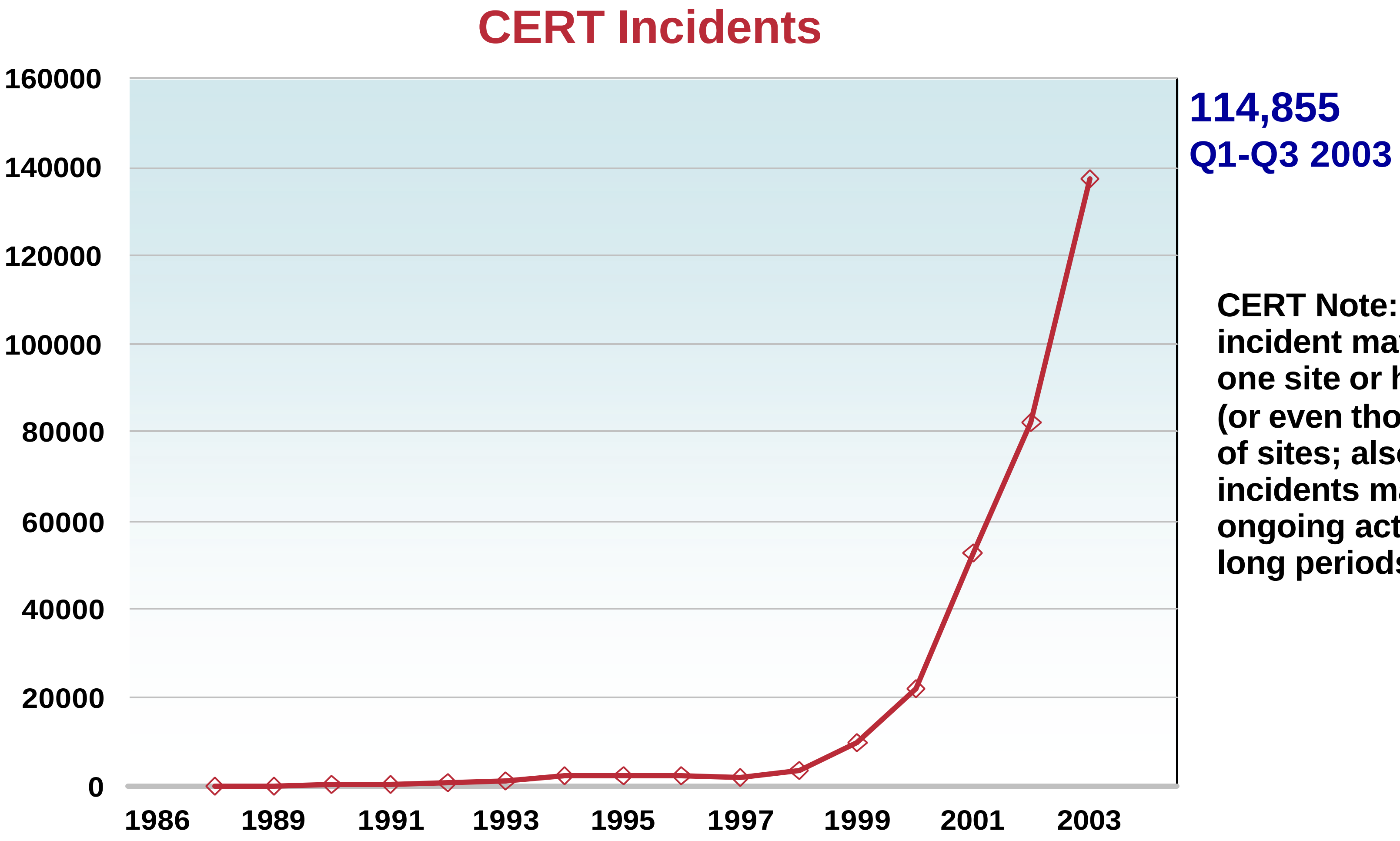
- Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.

- Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.

# Agenda

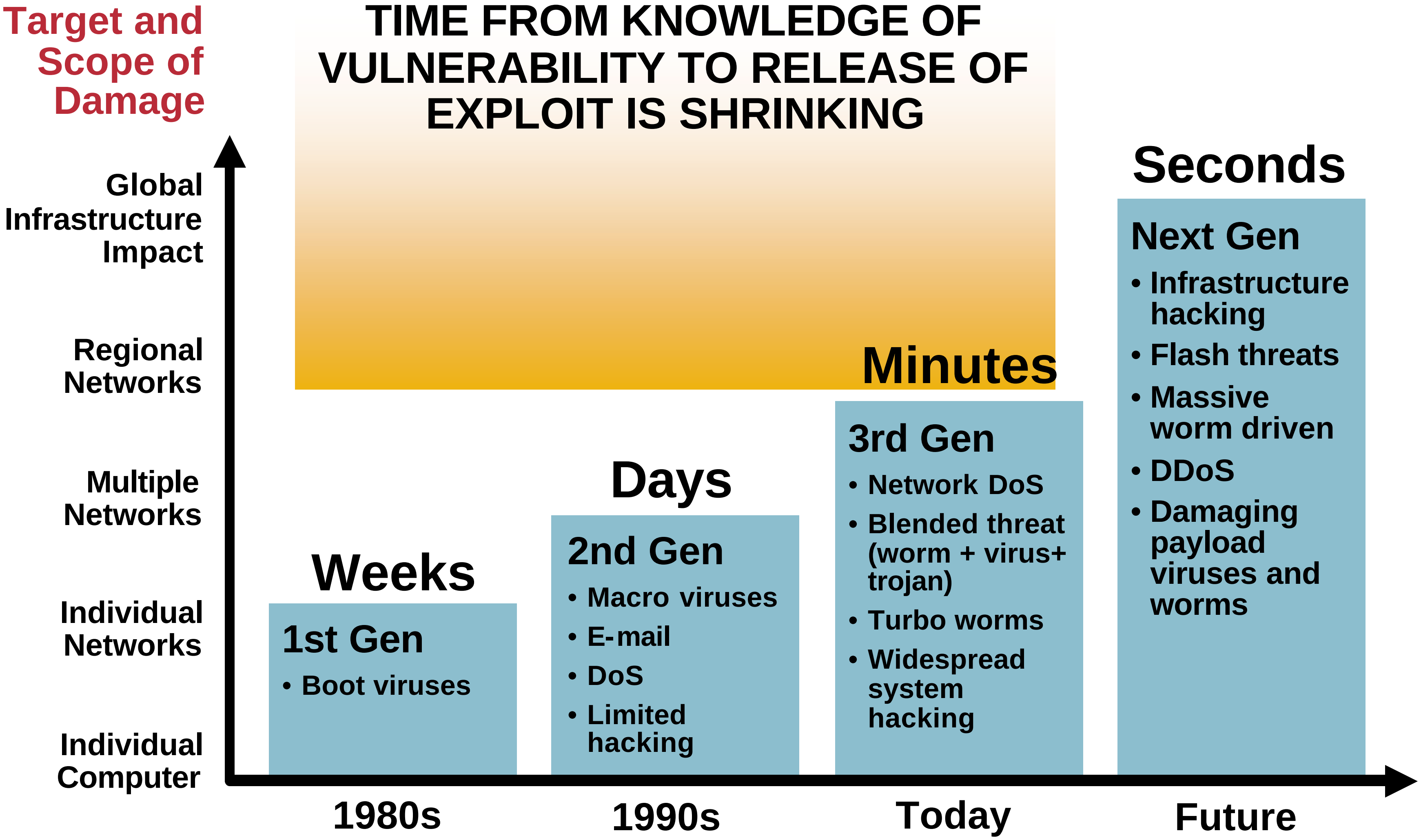
- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# Incidents on the Rise



CERT Note: An incident may involve one site or hundreds (or even thousands) of sites; also, some incidents may involve ongoing activity for long periods of time

# The Threats Have Evolved:
## Increasing Speed and Damage



Target and Scope of Damage

Global Infrastructure Impact

Regional Networks

Multiple Networks

Individual Networks

Individual Computer

TIME FROM KNOWLEDGE OF VULNERABILITY TO RELEASE OF EXPLOIT IS SHRINKING

Weeks

1st Gen

- Boot viruses

Days

2nd Gen

- Macro viruses
- E-mail
- DoS
- Limited hacking

Minutes

3rd Gen

- Network DoS
- Blended threat (worm + virus+ trojan)
- Turbo worms
- Widespread system hacking

Seconds

Next Gen

- Infrastructure hacking
- Flash threats
- Massive worm driven
- DDoS
- Damaging payload viruses and worms

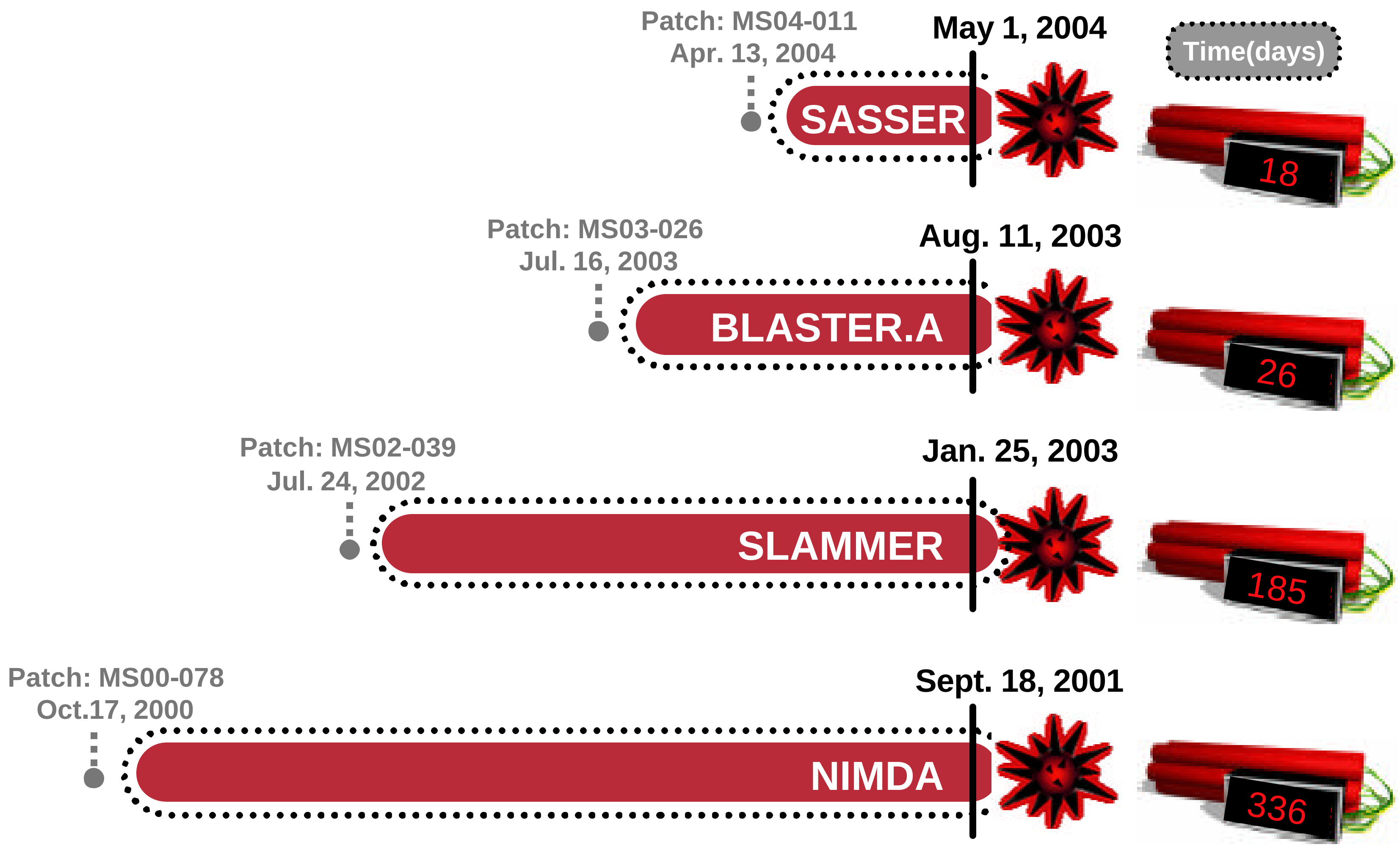
1980s

1990s

Today

Future

# Vanishing Patch to Outbreak Window



Time(days)

Patch: MS04-011
Apr. 13, 2004

May 1, 2004

SASSER

18

Patch: MS03-026
Jul. 16, 2003

Aug. 11, 2003

BLASTER.A

26

Patch: MS02-039
Jul. 24, 2002

Jan. 25, 2003

SLAMMER

185

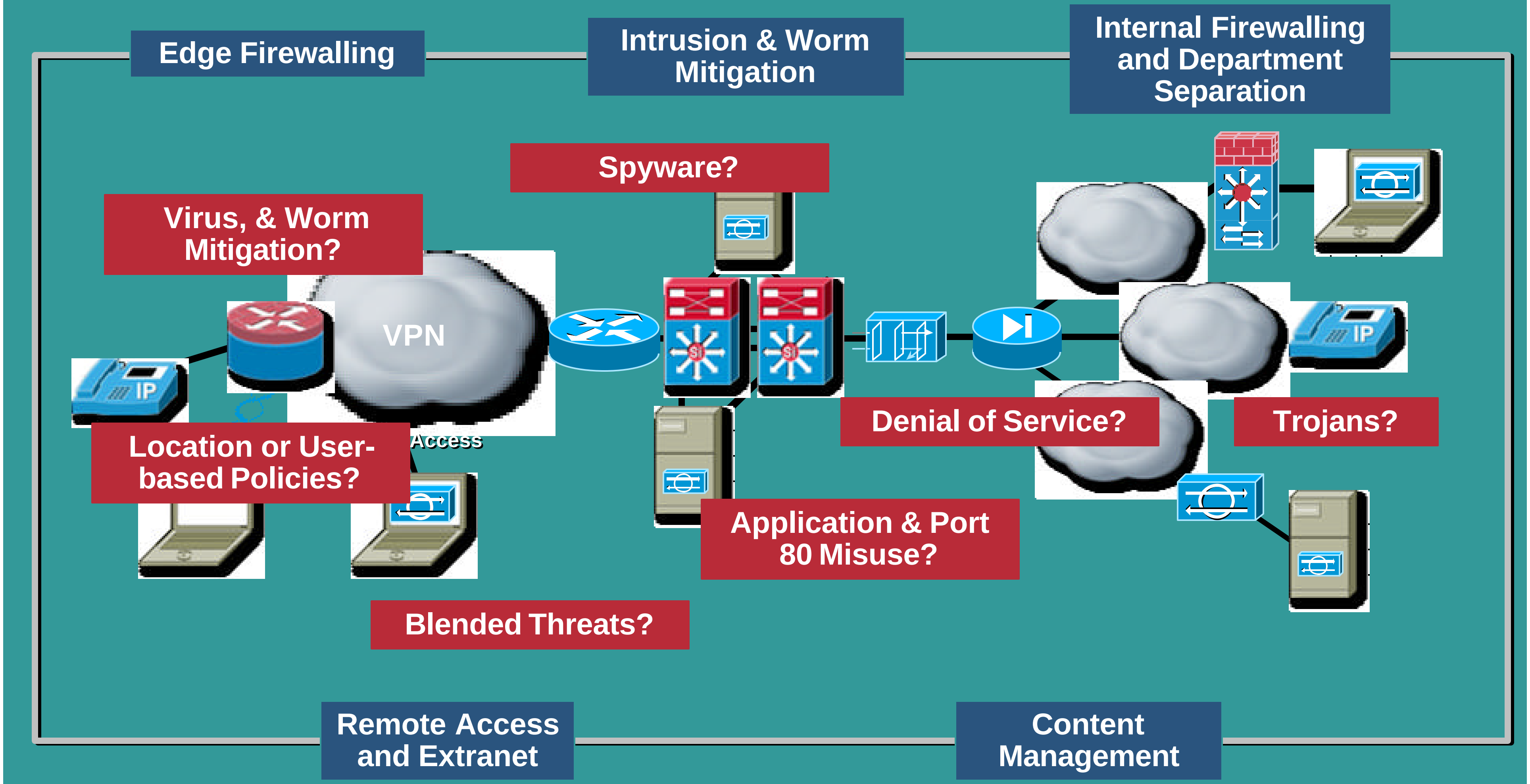
Patch: MS00-078
Oct.17, 2000

Sept. 18, 2001

NIMDA

336

# New Security Challenges


Edge Firewalling
Intrusion & Worm Mitigation
Internal Firewalling and Department Separation
Spyware?
Virus, & Worm Mitigation?
VPN
IP
Location or User-based Policies?
Access
Denial of Service?
Trojans?
IP
Application & Port 80 Misuse?
Blended Threats?
Remote Access and Extranet
Content Management

***Evolution of Threats***

# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# Introduction to IPS:
## *The Marketing of IDS/IPS*

- IDS Intrusion Detection System—Traditionally limited to promiscuous sensors that mirror the traffic to a monitoring port

- IPS Intrusion Prevention—The term most commonly applied to an inline IDS sensor that is in the data path and has the ability to drop offending traffic

- IDP Intrusion Detection and Prevention—Marketing term coined by a vendor for product differentiation

# IDS vs. IPS

## *Network-Based IDS—The Sensor*

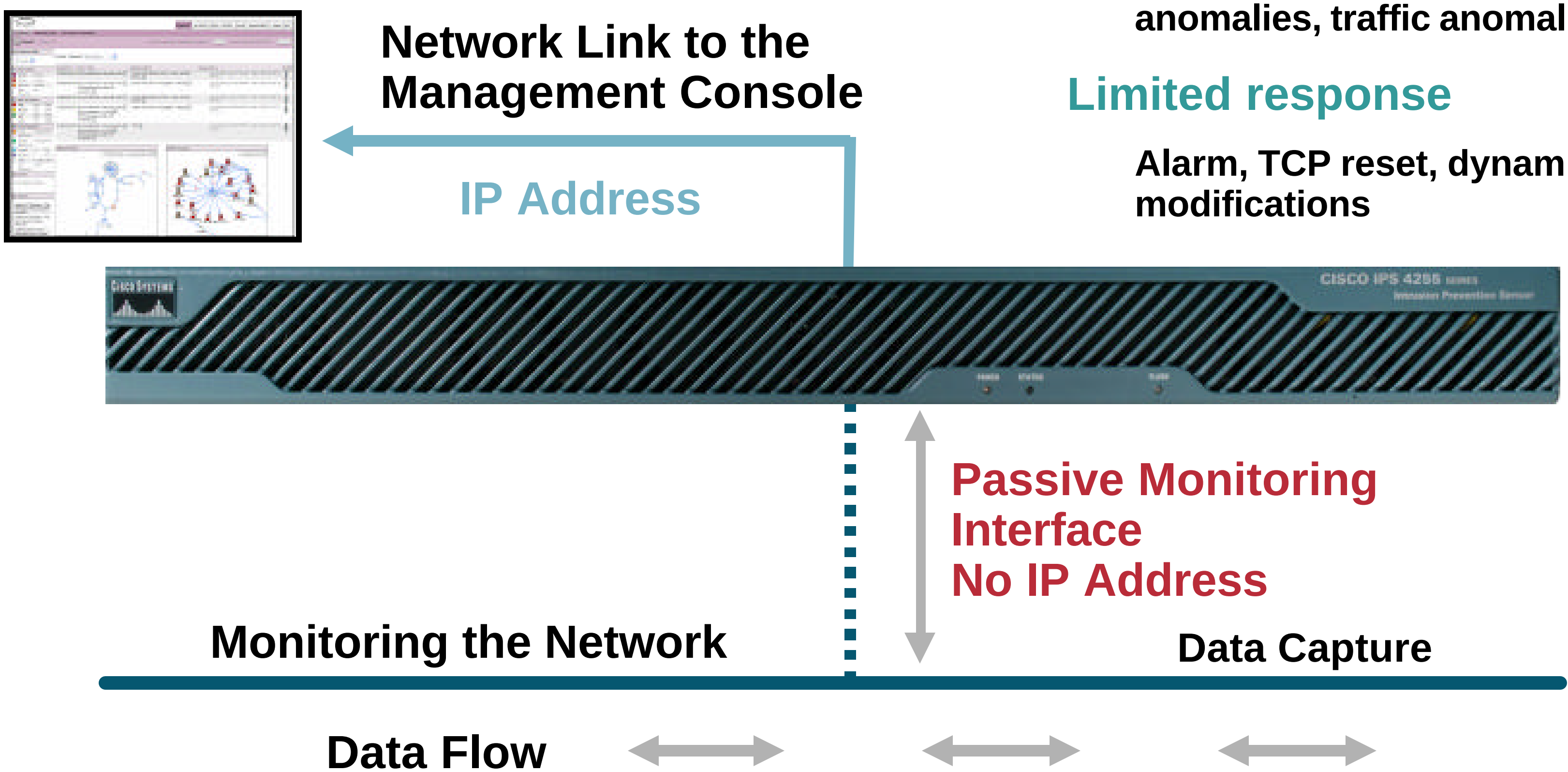
### Promiscuous mode

### Attack patterns

**Signatures, heuristics, protocol anomalies, traffic anomalies**

### Limited response

**Alarm, TCP reset, dynamic ACL modifications**



**Network Link to the Management Console**

IP Address

**Passive Monitoring Interface**
**No IP Address**

**Monitoring the Network**

**Data Capture**

**Data Flow**

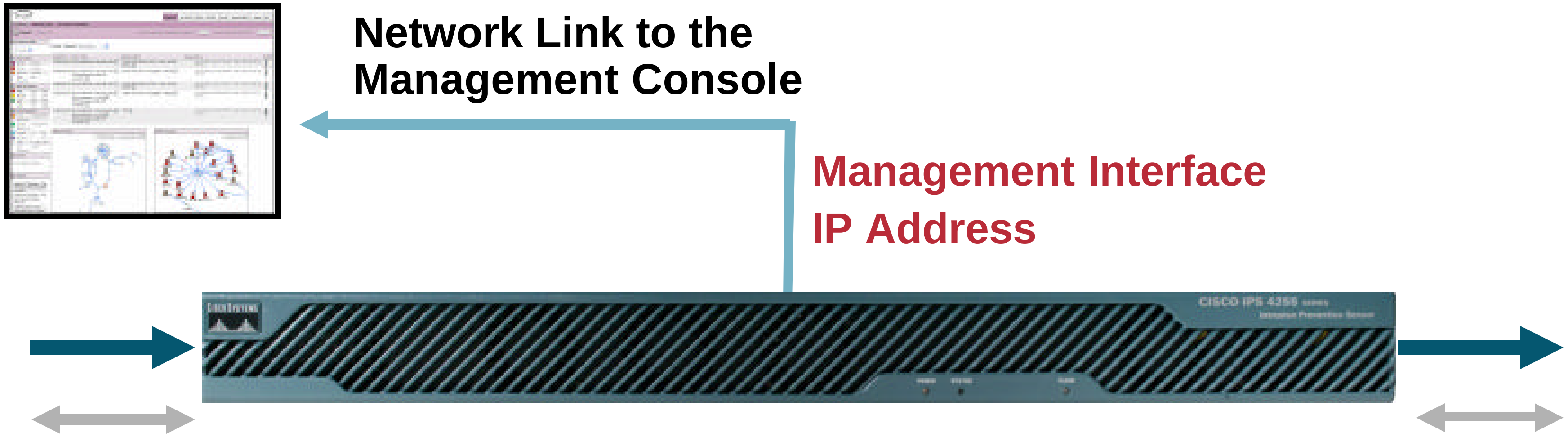
# IDS vs. IPS

## *Network-Based IPS—The Sensor*

Inline Monitoring (active)

Same detection/response as IDS

Added traffic filtering/drop action



Network Link to the Management Console

Management Interface
IP Address

Data Flow

Data Flow

TRANSPARENT MONITORING INTERFACES
NO IP ADDRESS

# IPS Terminology:
## *What is IPS?*

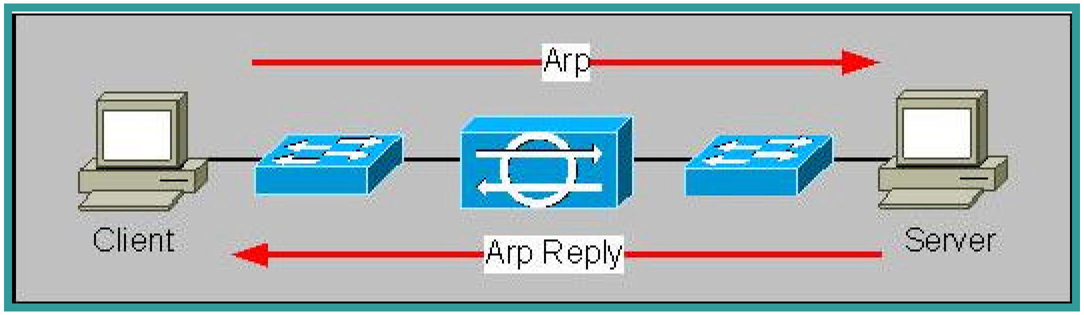
- IPS closely resembles a Layer 2 bridge or repeater

  "Identical to a wire" is the closest analogy

  Inline interfaces have no MAC or IP and cannot be detected directly

  Network IPS passes all packets without directly participating in any communications including spanning tree (but spanning tree packets are passed)

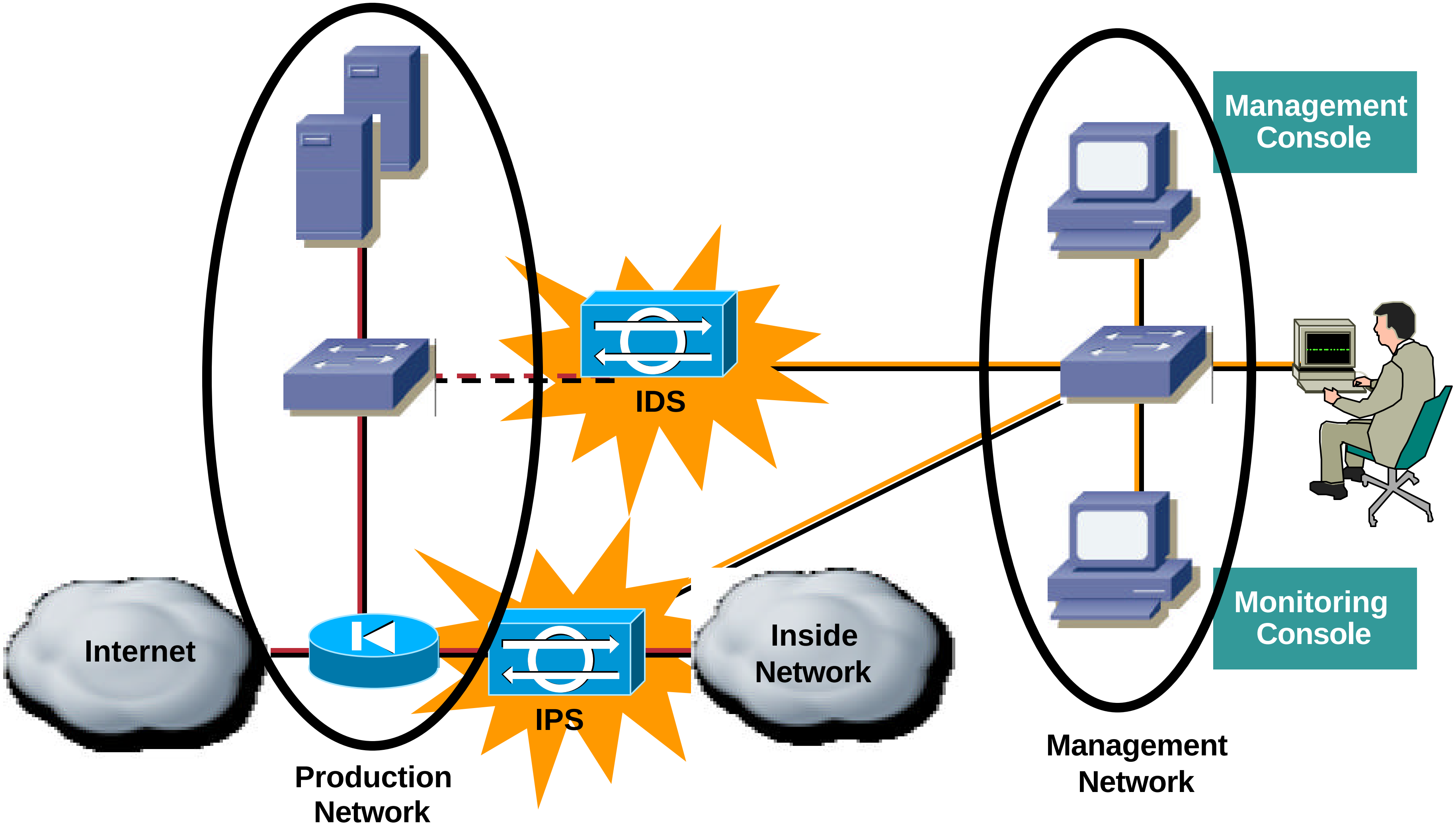
  Default Behavior is to pass all packets even if unknown, (ie IPX, Appletalk, etc) unless specifically denied by policy or detection



# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# IPS/IDS System Level Architecture



# IPS Components

- Network-Based Sensors

  Specialized software and/or hardware used to collect and analyze network traffic (either in IPS or IDS mode: inline or promiscuous)

  Appliances, modules, embedded in network infrastructure (either inline or promiscuous)

- Security Management and Monitoring

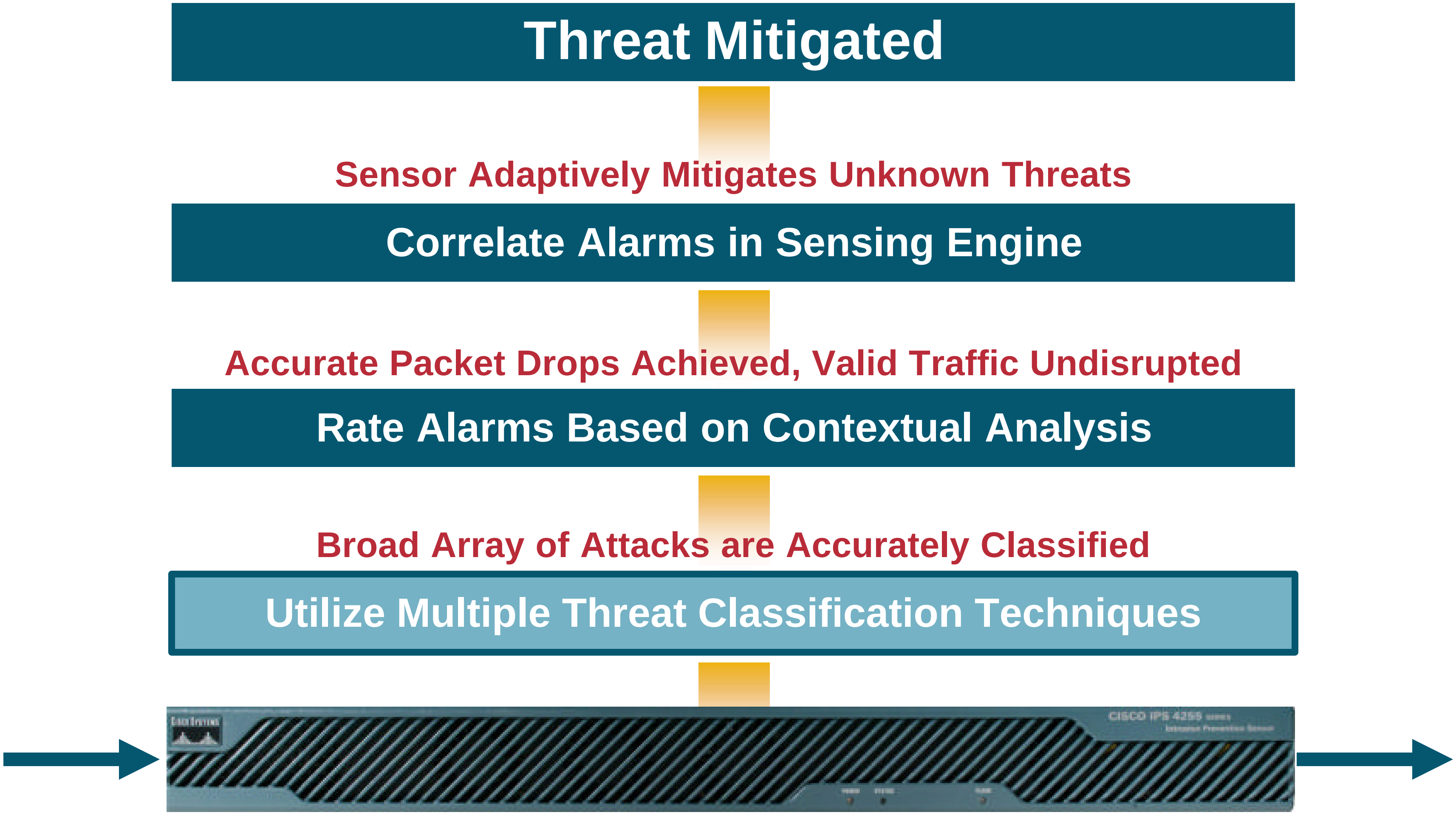
  Performs configuration and deployment services

  Performs alert collection, aggregation, and correlation

# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# Process for Accurate Threat Mitigation



Threat Mitigated

Sensor Adaptively Mitigates Unknown Threats

Correlate Alarms in Sensing Engine

Accurate Packet Drops Achieved, Valid Traffic Undisrupted

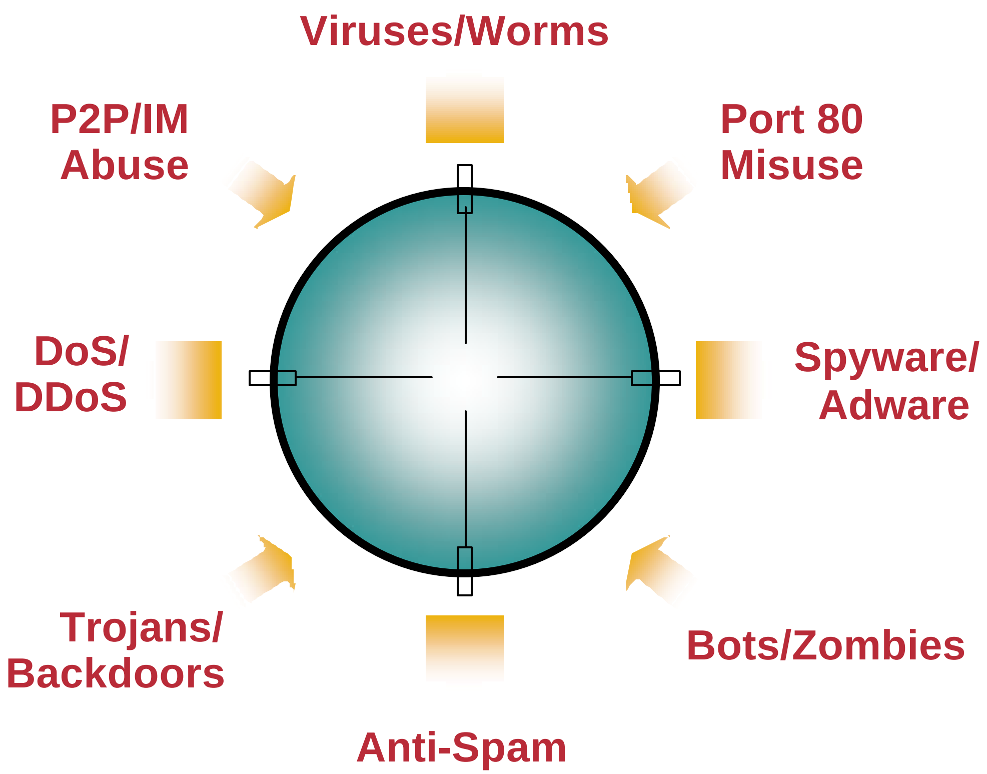
Rate Alarms Based on Contextual Analysis

Broad Array of Attacks are Accurately Classified

Utilize Multiple Threat Classification Techniques

# Accurate Threat Classification

## *Multi-Vector Attack Identification*



**Multiple techniques must be utilized to block broad classes of attacks**

**Vulnerability – encoding signatures to the underlying vulnerability for day-zero protection**

**Exploit-specific – protection from unknown threats and quickly mutating viruses**

**Policy – traffic filtering based on security policy**

**Anomaly – Traffic and protocol anomaly detection to complement signature based analysis**

**Heuristic – statistically based algorithms to rate limit alarms produced by sensing engine**

# Simple Pattern Matching

## *Multi-Vector Attack Identification*

- **Looking for a fixed sequence of bytes in a single packet. Can be associated with a specific service.**

**Example:**

**Fire alarm if packet is an IPv4 TCP packet destined for port 2222 and contains the string "foo" between starting point "x" to endpoint "y"**

**Conditions for signature to fire:**

**Version: IPv4** **Protocol: TCP** **Destination Port: 2222** **String: "xxxfooyyy"**

| Pros | Cons |
|---|---|
| Simple to create | False positives rates due to pattern not being unique |
| Highly Specific | Attack modification could lead to false negative |
| Reliable Alerts | Multiple signatures could be required for a single vulnerability |
| Applicable across protocols | Single packet inspection does not apply well to stream based traffic |

# Stateful Pattern Matching

## *Multi-Vector Attack Identification*

- **Matches are made in context within the state of the stream.**

**Conditions for signature to fire:**

**Version:** IPv4 **Protocol:** TCP **Destination Port:** 2222 **String:** “xxxfooyyy”

**1st packet sent in stream :**

**Version:** IPv4 **Protocol:** TCP **Destination Port:** 2222 **String:** “xxxfoyyy”

**2nd packet sent in stream:**

**Version:** IPv4 **Protocol:** TCP **Destination Port:** 2222 **String:** “xxxoyyy”

## Pros

Simple to formulate

Highly Specific, Reliable

Applicable across protocols

## Cons

False positives rates due to pattern not being unique

Attack modification could lead to false negative

Multiple signatures could be required for a single vulnerability

# Protocol Decode-Based Analysis

## *Multi-Vector Attack Identification*

- Decode protocols elements like the client or server in the conversation would do then look for RFC violations.

Example Attack:
Protocol: "BGS"
Attack Name: "ABC"
Description of Attack:
Requires "foo" to be passed in "BGS Type" field

Scenario 1:
Protocol: "BGS"
Options: "fooh, mooh"
Type: "abc…..xyz"
Header: "NORMAL"

False positive

Scenario 2:
Protocol: "BGS"
Options: "mooh"
Type: "fx00ox00ox00"
Header: "NULL"

False negative

### Pros

Minimize occurrence of false positive for well defined protocols

Broader method that allow catching variations

### Cons

May lead to high false positive if RFC is ambiguous

Longer and more complex development time to develop protocol parser

# Heuristic-Based Analysis

## *Multi-Vector Attack Identification*

- **Based on algorithmic logic such as  statistical evaluations of the type of traffic being presented.**

| Packets from IP ”A” to IP “B” | Count | Threshold | Is Count > Threshold? | Observation: Unique Ports |
|---|---|---|---|---|
| TCP Port 1 | 1 | 3 | No | 1 |
| TCP Port 80 | 2 | 3 | No | 1, 80 |
| TCP Port 80 | 2 | 3 | No | 1, 80 |
| TCP Port 2 | 3 | 3 | No | 1, 2, 80 |
| TCP Port 3 | 4 | 3 | Yes | 1, 2, 3, 80 |

**Pros**

**Some types of suspicious/malicious activity cannot be detected through any other means.**

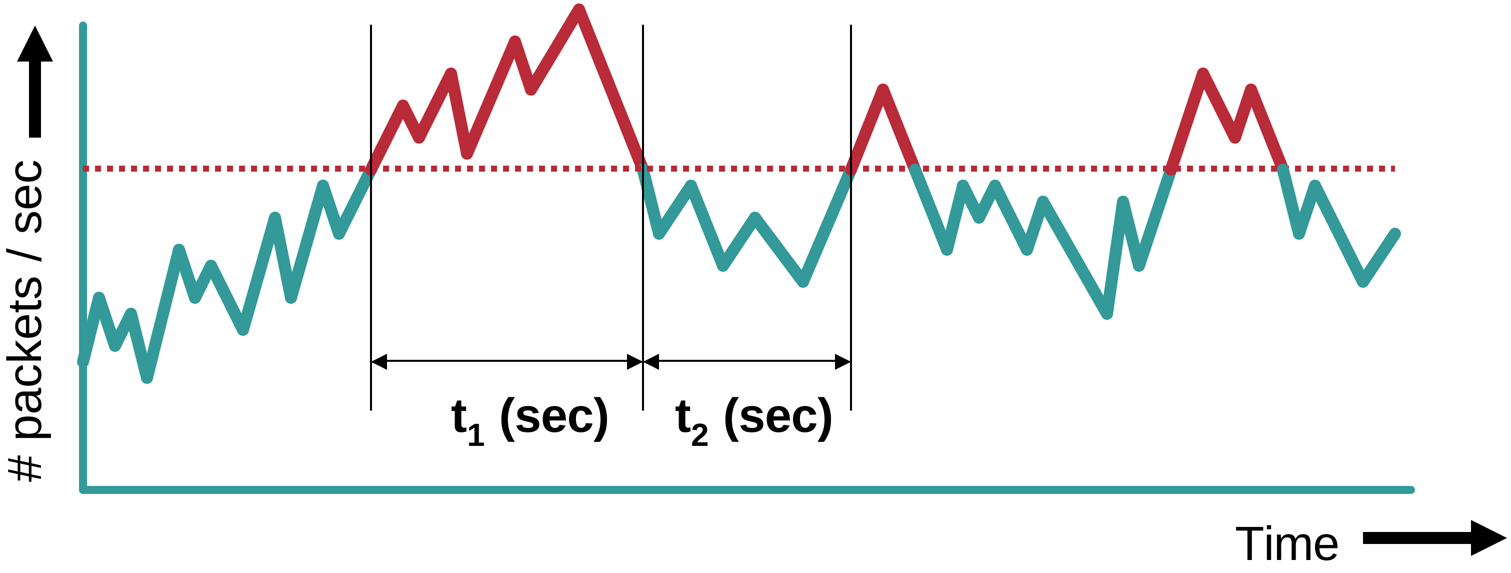
**Cons**

**Algorithms may require tuning or modification in order to better conform to network traffic and limit false positives.**

# Anomaly-Based Analysis

## *Multi-Vector Attack Identification*

- Look for traffic that deviates from what is seen “normally.”



### Pros

Can detect unknown attack if implemented properly

Low overhead - no new signature to develop and install

### Cons

No intrusion granularity (no pattern unknown attacks)

Highly dependant on what has been learned as normal

# Additional Threat Classification Goals

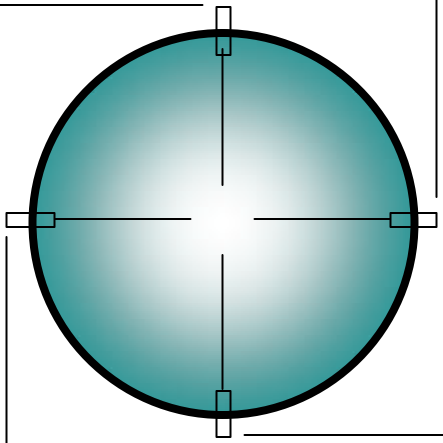
## *Anti-X and Application Abuse Vectors*

### Spyware/Adware

- Controls the transmission of confidential data
- Polices the network traffic to filter out spyware communications

### Voice Over IP (VoIP)

- Ensures protocol compliance for call setup
- Protects voice gateways from attacks
- Prevents excess memory allocation of URL overflows



### Application Abuse

- Provides deep inspection for web protection and control of “port 80 misuse”
- Controls usage of IM, P2P, methods/commands, MIME types

### Network Virus

- Leverages Trend Micro partnership to integrate late-breaking malware
- Improves virus coverage and response time

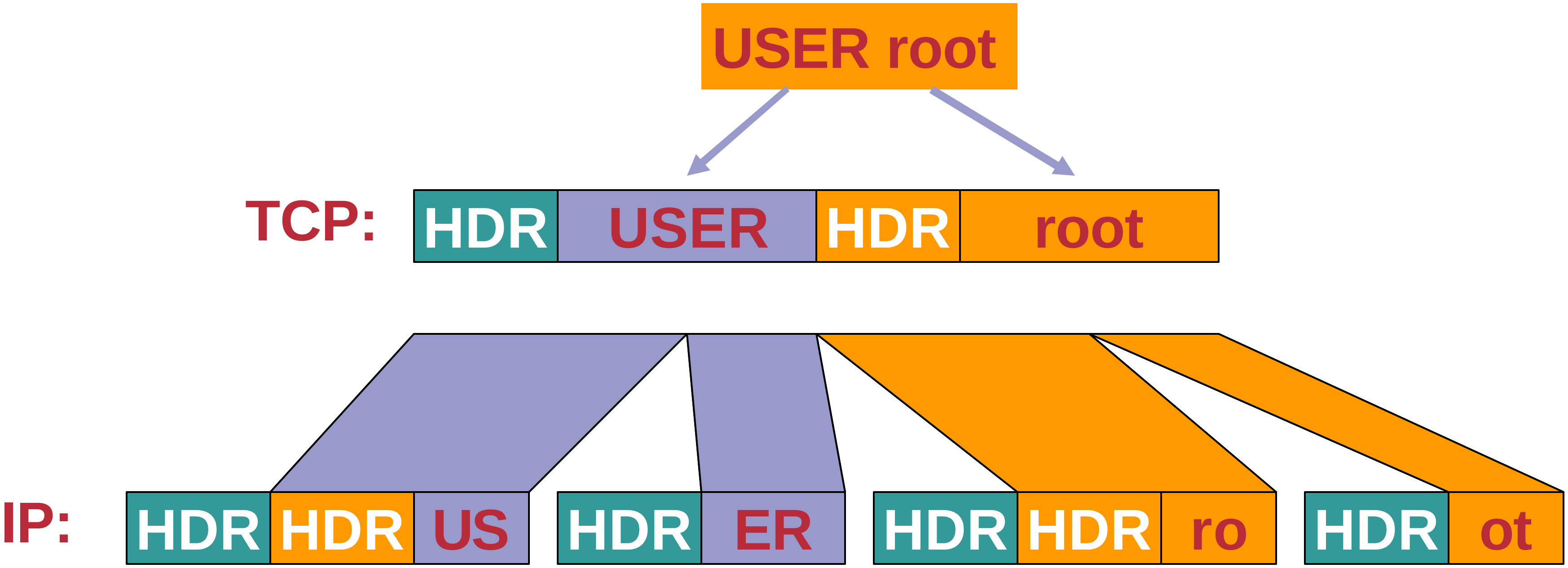
# IPS Anti-Evasion Features

## *IPS Evasion Techniques*

- Fragmentation Reassembly
- TCP Stream Reassembly
- De-obfuscation
- TTL - based evasion techniques

# Reconstructing Flows
## *IPS Evasion Techniques*

- Fragmentation may be naturally occurring or performed intentionally to evade IPS
- Fragmentation Reassembly must be applied to mitigate this evasion technique



# Deobfuscation

## *IPS Evasion Techniques*

- Tools such as Whisker may be used to encode Unicode characters that result in numerous possible transformations that attempt to evade IPS

**Example:**

**Attacker's cgi script to exploit a vulnerability is named "attack.cgi"**

**Attacker obfuscates attack.cgi:**

**Result: %3A%4E%4Eack.cgi**

**%3A represents "A" ; %4E represents "T"**

**IPS de- obfuscates :**

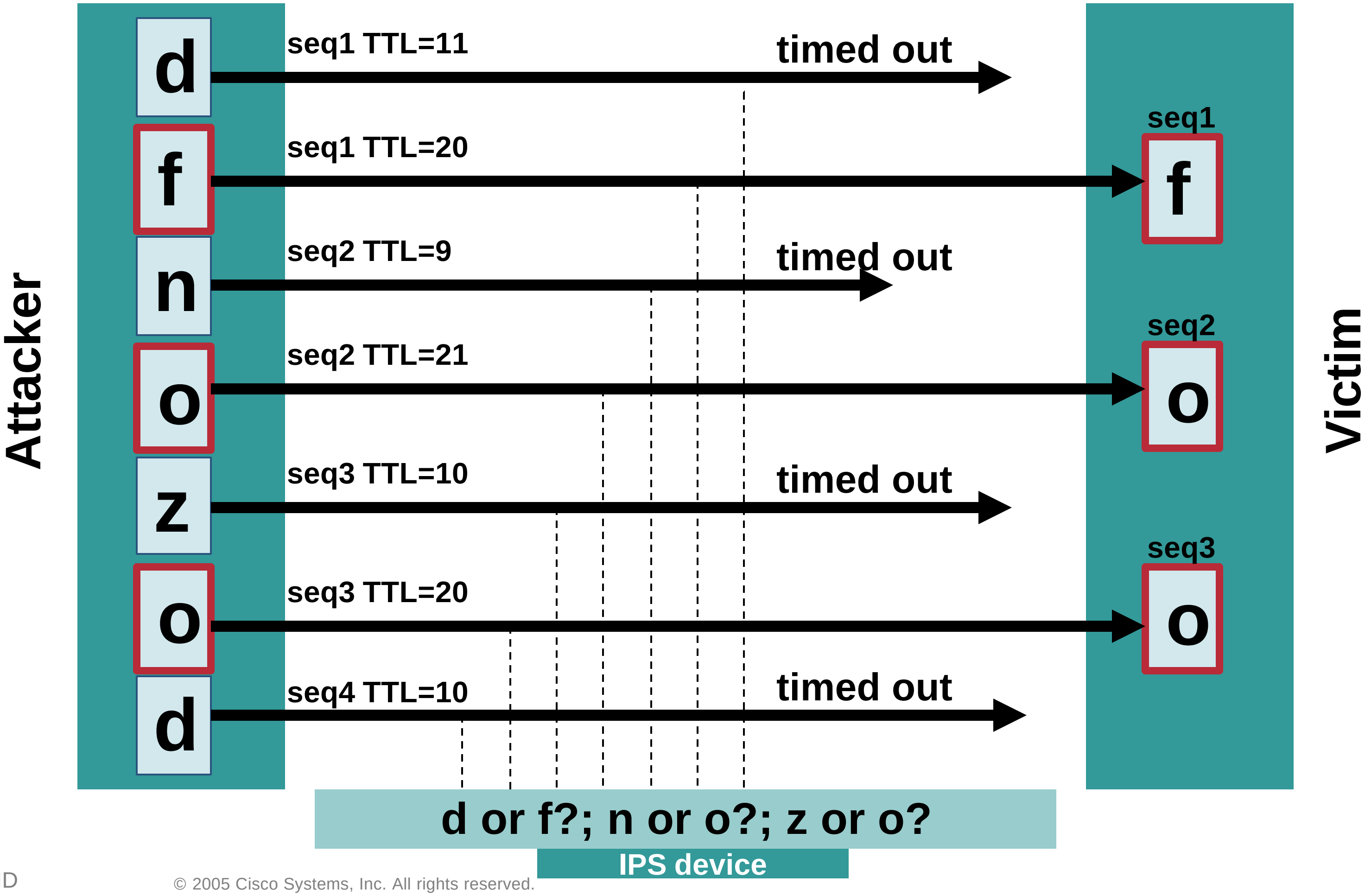
**Result: attack.cgi**

**Simple Pattern Match can now be performed**

# TTL Manipulation

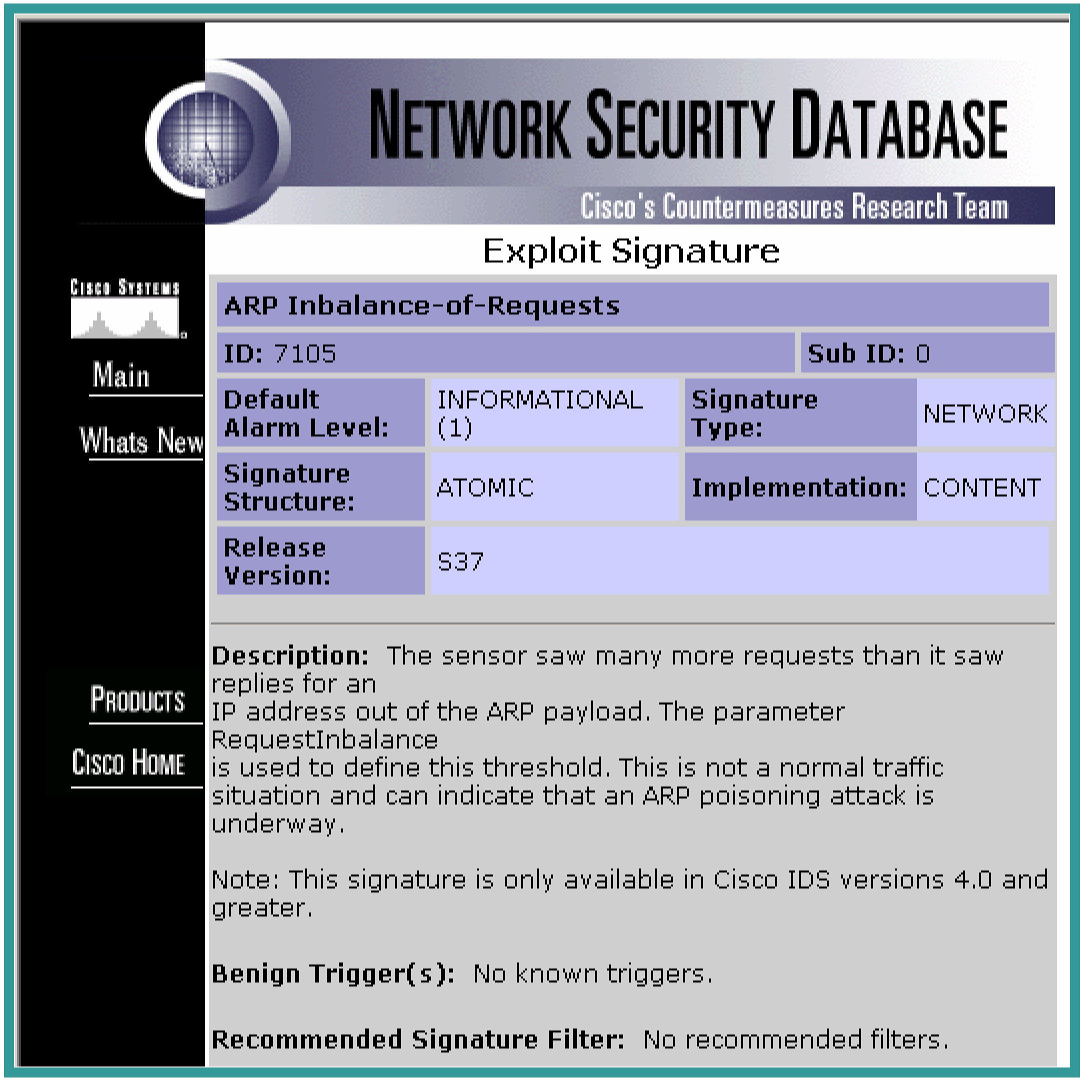
## *IPS Evasion Techniques*

- **Attackers can adjust TTL values on packets to purposely confuse IPS devices**



# Alarm Guidance: NSDB

- **Most products have an alarm database that provides guidance on alarms**
- **Web or text-based DBs can allow addition of custom information or directions for operations staff**


Network Security Database
Cisco's Countermeasures Research Team
Cisco Systems
Main
Whats New
Products
Cisco Home

Exploit Signature

| | | | |
|---|---|---|---|
| **ARP Inbalance-of-Requests** | | | |
| **ID:** 7105 | | **Sub ID:** 0 | |
| **Default Alarm Level:** | INFORMATIONAL (1) | **Signature Type:** | NETWORK |
| **Signature Structure:** | ATOMIC | **Implementation:** | CONTENT |
| **Release Version:** | S37 | | |

**Description:** The sensor saw many more requests than it saw replies for an IP address out of the ARP payload. The parameter RequestInbalance is used to define this threshold. This is not a normal traffic situation and can indicate that an ARP poisoning attack is underway.

Note: This signature is only available in Cisco IDS versions 4.0 and greater.

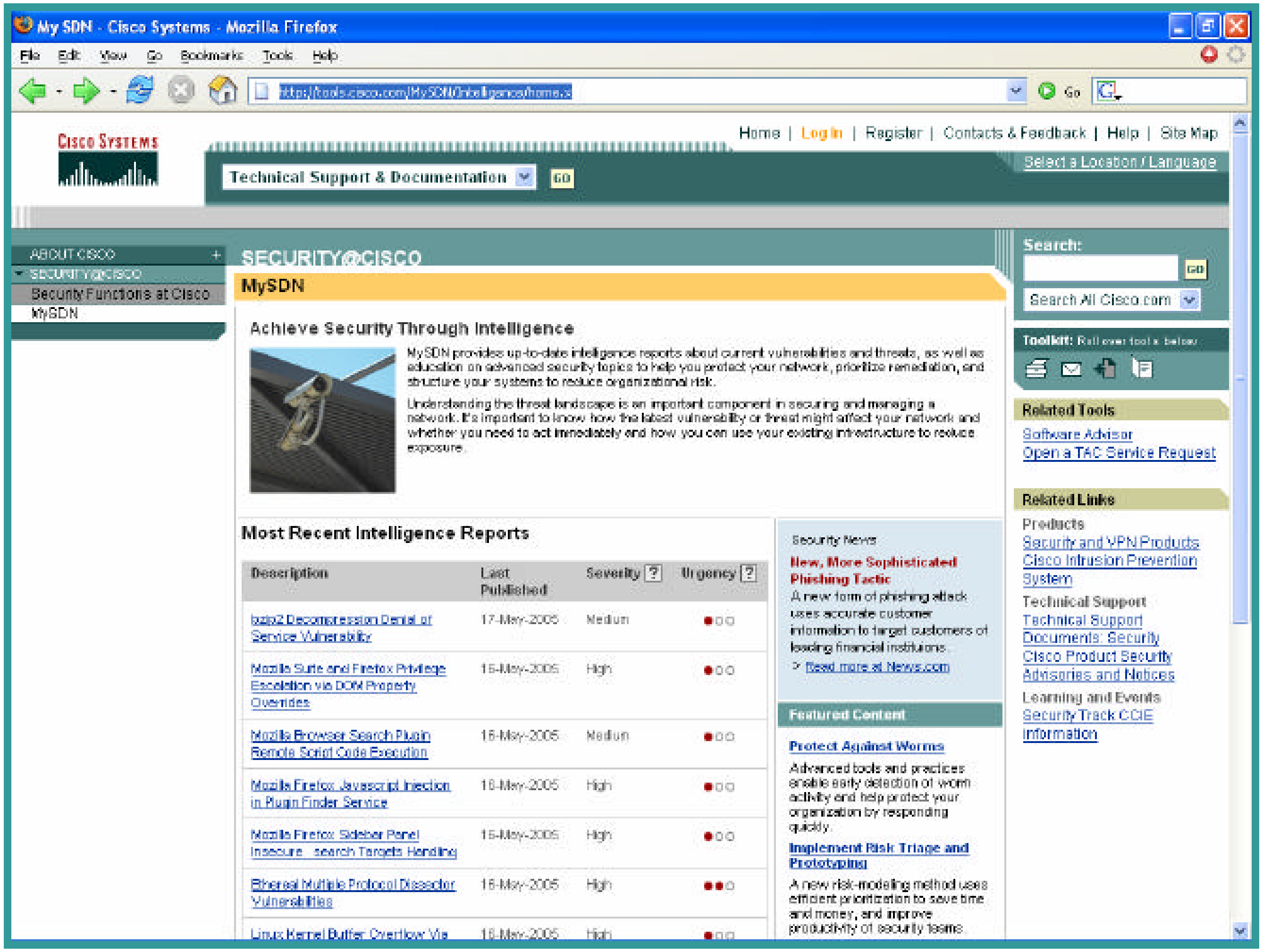
**Benign Trigger(s):** No known triggers.

**Recommended Signature Filter:** No recommended filters.

# Signature Updates

- Much like anti-virus, network IPS's must be kept up to date
- Process must be developed to rapidly update new signatures as released
- Cisco has developed a new partnership with Trend Micro to provide enhanced virus and worm coverage as part of the normal IPS signature updates
- Signature releases can be updated using automated, secure mechanisms

# MySDN: Cisco’s Security Portal


My SDN - Cisco Systems - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://tools.cisco.com/MySDN/Intelligence/home.x
Go
Cisco Systems
Home | Log In | Register | Contacts & Feedback | Help | Site Map
Technical Support & Documentation
GO
Select a Location / Language
ABOUT CISCO +
SECURITY@CISCO
Security Functions at Cisco
MySDN
SECURITY@CISCO
Search:
GO
Search All Cisco.com
Toolkit: Roll over tools below

MySDN

Achieve Security Through Intelligence

MySDN provides up-to-date intelligence reports about current vulnerabilities and threats, as well as education on advanced security topics to help you protect your network, prioritize remediation, and structure your systems to reduce organizational risk.

Understanding the threat landscape is an important component in securing and managing a network. It's important to know how the latest vulnerability or threat might affect your network and whether you need to act immediately and how you can use your existing infrastructure to reduce exposure.

Most Recent Intelligence Reports

| Description | Last Published | Severity ? | Urgency ? |
|---|---|---|---|
| bzip2 Decompression Denial of Service Vulnerability | 17-May-2005 | Medium | ●○○ |
| Mozilla Suite and Firefox Privilege Escalation via DOM Property Overrides | 16-May-2005 | High | ●○○ |
| Mozilla Browser Search Plugin Remote Script Code Execution | 16-May-2005 | Medium | ●○○ |
| Mozilla Firefox Javascript Injection in Plugin Finder Service | 16-May-2005 | High | ●○○ |
| Mozilla Firefox Sidebar Panel Insecure _search Targets Handling | 16-May-2005 | High | ●○○ |
| Ethereal Multiple Protocol Dissector Vulnerabilities | 16-May-2005 | High | ●●○ |
| Linux Kernel Buffer Overflow Via | 16-May-2005 | High | ●○○ |

Security News

**New, More Sophisticated Phishing Tactic**

A new form of phishing attack uses accurate customer information to target customers of leading financial institutions.

> Read more at News.com

Featured Content

**Protect Against Worms**

Advanced tools and practices enable early detection of worm activity and help protect your organization by responding quickly.

**Implement Risk Triage and Prototyping**

A new risk-modeling method uses efficient prioritization to save time and money, and improve productivity of security teams.

Related Tools

Software Advisor
Open a TAC Service Request

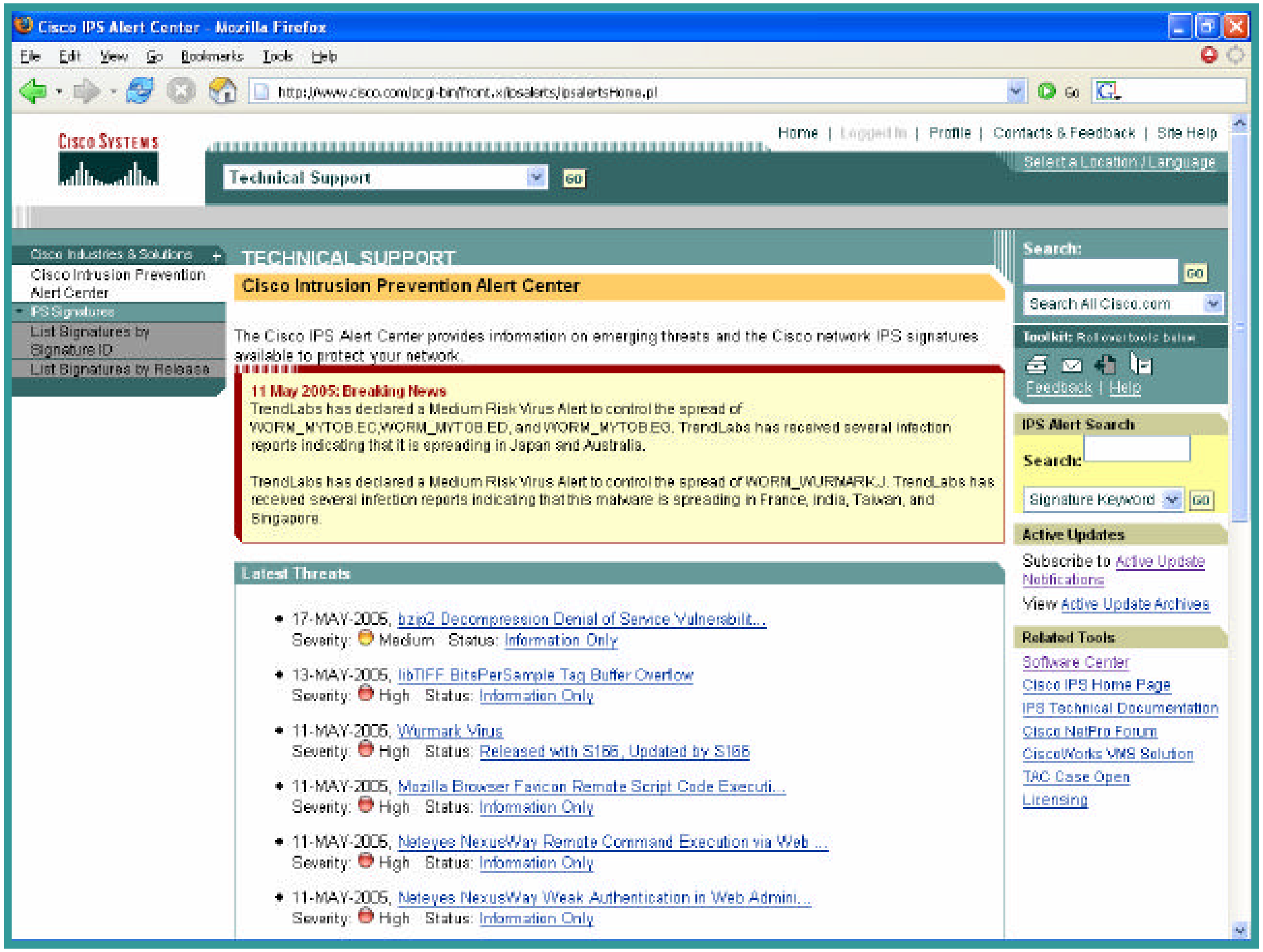
Related Links

Products
Security and VPN Products
Cisco Intrusion Prevention System

Technical Support
Technical Support
Documents: Security
Cisco Product Security
Advisories and Notices

Learning and Events
Security Track CCIE
Information

# IPS Alert Center for all things IPS related


Cisco IPS Alert Center - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.cisco.com/pcgi-bin/front.x/ipsalerts/ipsalertsHome.pl
Go
Cisco Systems
Home | Logged In | Profile | Contacts & Feedback | Site Help
Select a Location / Language
Technical Support
GO
Cisco Industries & Solutions +
Cisco Intrusion Prevention Alert Center
IPS Signatures
List Signatures by Signature ID
List Signatures by Release
Search:
GO
Search All Cisco.com
Toolkit: Roll over tools below
Feedback | Help
IPS Alert Search
Search:
Signature Keyword
GO
Active Updates
Subscribe to Active Update Notifications
View Active Update Archives
Related Tools
Software Center
Cisco IPS Home Page
IPS Technical Documentation
Cisco NetPro Forum
CiscoWorks VMS Solution
TAC Case Open
Licensing

TECHNICAL SUPPORT

**Cisco Intrusion Prevention Alert Center**

The Cisco IPS Alert Center provides information on emerging threats and the Cisco network IPS signatures available to protect your network.

**11 May 2005: Breaking News**
TrendLabs has declared a Medium Risk Virus Alert to control the spread of WORM_MYTOB.EC,WORM_MYTOB.ED, and WORM_MYTOB.EG. TrendLabs has received several infection reports indicating that it is spreading in Japan and Australia.

TrendLabs has declared a Medium Risk Virus Alert to control the spread of WORM_WURMARK.J. TrendLabs has received several infection reports indicating that this malware is spreading in France, India, Taiwan, and Singapore.

**Latest Threats**

- 17-MAY-2005, bzip2 Decompression Denial of Service Vulnerabilit...
  Severity: ● Medium Status: Information Only
- 13-MAY-2005, libTIFF BitsPerSample Tag Buffer Overflow
  Severity: ● High Status: Information Only
- 11-MAY-2005, Wurmark Virus
  Severity: ● High Status: Released with S166, Updated by S166
- 11-MAY-2005, Mozilla Browser Favicon Remote Script Code Executi...
  Severity: ● High Status: Information Only
- 11-MAY-2005, Neteyes NexusWay Remote Command Execution via Web ...
  Severity: ● High Status: Information Only
- 11-MAY-2005, Neteyes NexusWay Weak Authentication in Web Admini...
  Severity: ● High Status: Information Only

# www.cisco/com/go/ipsalerts

# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# IPS Terminology:
# *False Positives Defined*

- **False Positive is the term most likely used to indicate an event that was incorrectly reported; It is typically mistakenly applied to a broad group of possible results**

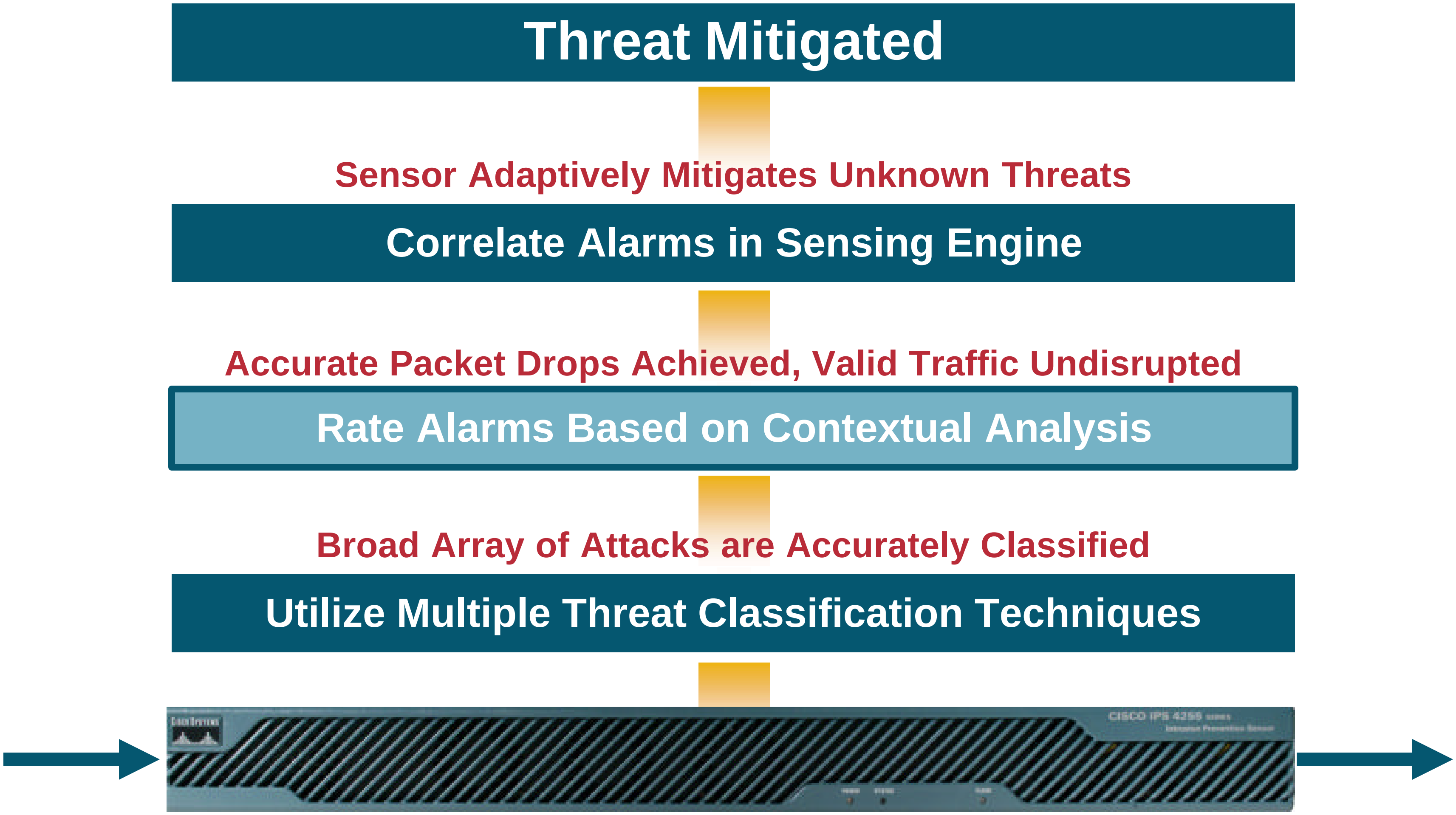
  **False Positive: A correctly named false positive is one where the IPS has triggered an alert based on a flawed algorithm or an analysis error; normally a fairly rare event**

  **Benign Trigger: The case where a sensor has correctly interpreted network as an attack, but the intentions behind the traffic were not malicious; potentially common**

  **False Alarms (or Noise): The case where a sensor has correctly detected than an event has occurred but the event is non-threatening or not applicable to the site being monitored or was not successful; very likely labeled as a False Positive, very common**

- **False Negatives is the term used to describe when an IPS misses a real attack or event**

# Process for Accurate Threat Mitigation



Threat Mitigated

Sensor Adaptively Mitigates Unknown Threats

Correlate Alarms in Sensing Engine

Accurate Packet Drops Achieved, Valid Traffic Undisrupted

Rate Alarms Based on Contextual Analysis

Broad Array of Attacks are Accurately Classified

Utilize Multiple Threat Classification Techniques

# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

**EVENT SEVERITY** — How urgent is the threat?

+

**SIGNATURE FIDELITY** — How prone to false positive?

+

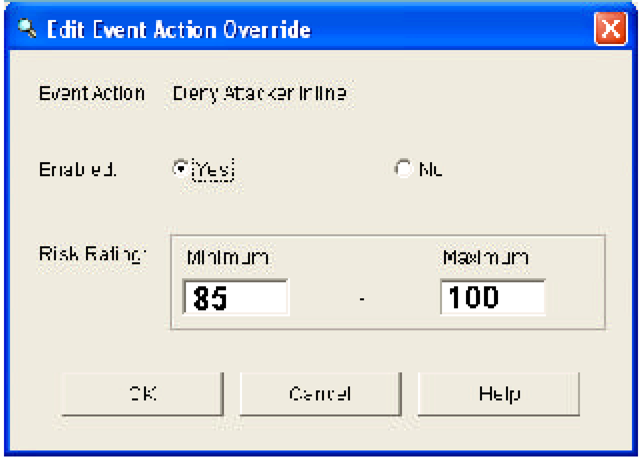
**ATTACK RELEVANCY** — Is attack relevant to host being attacked?

+

**ASSET VALUE OF TARGET** — How critical is this destination host?

**RISK RATING** — Drives Mitigation Policy →

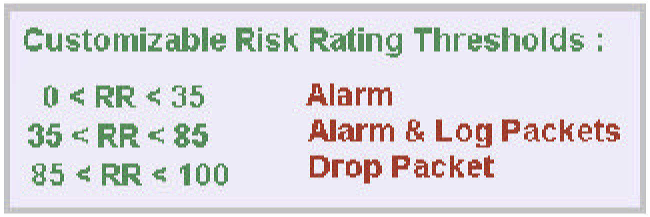
**Decision Support Balances Attack Urgency with Business Risk**


Edit Event Action Override

Event Action: Deny Attacker Inline

Enabled: ● Yes ○ No

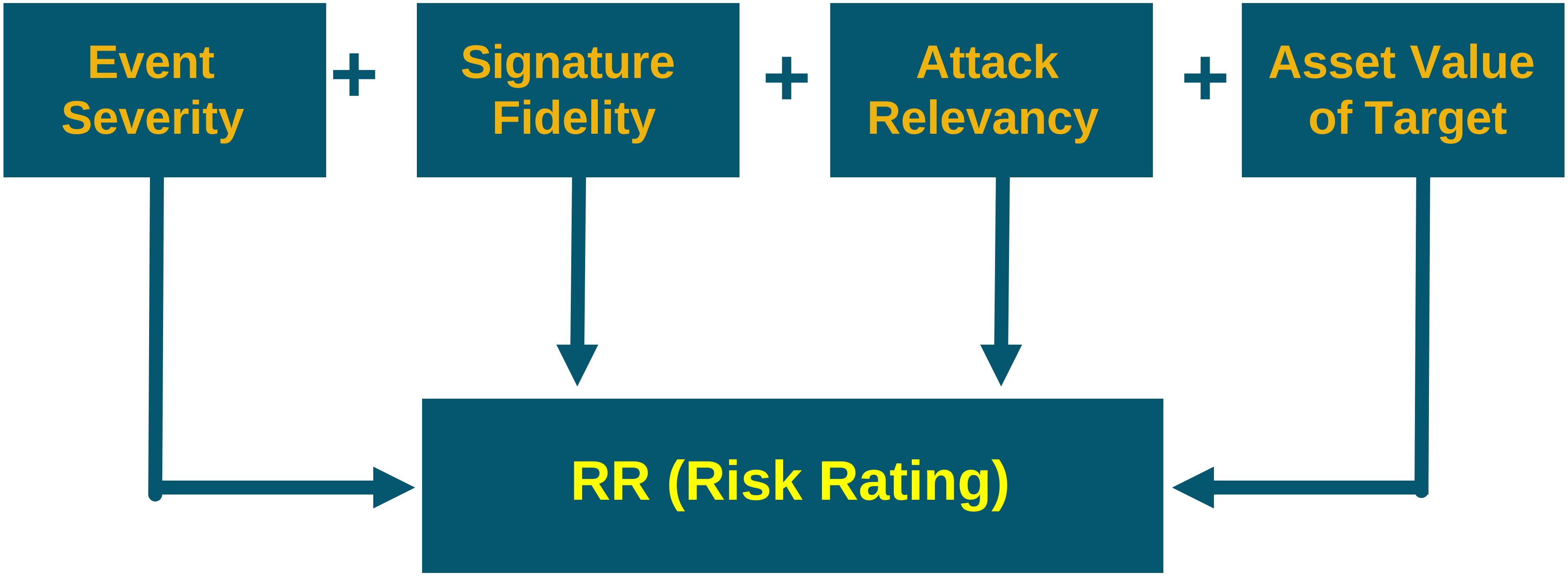
Risk Rating: Minimum 85 - Maximum 100


Customizable Risk Rating Thresholds :

| | |
|---|---|
| 0 < RR < 35 | Alarm |
| 35 < RR < 85 | Alarm & Log Packets |
| 85 < RR < 100 | Drop Packet |

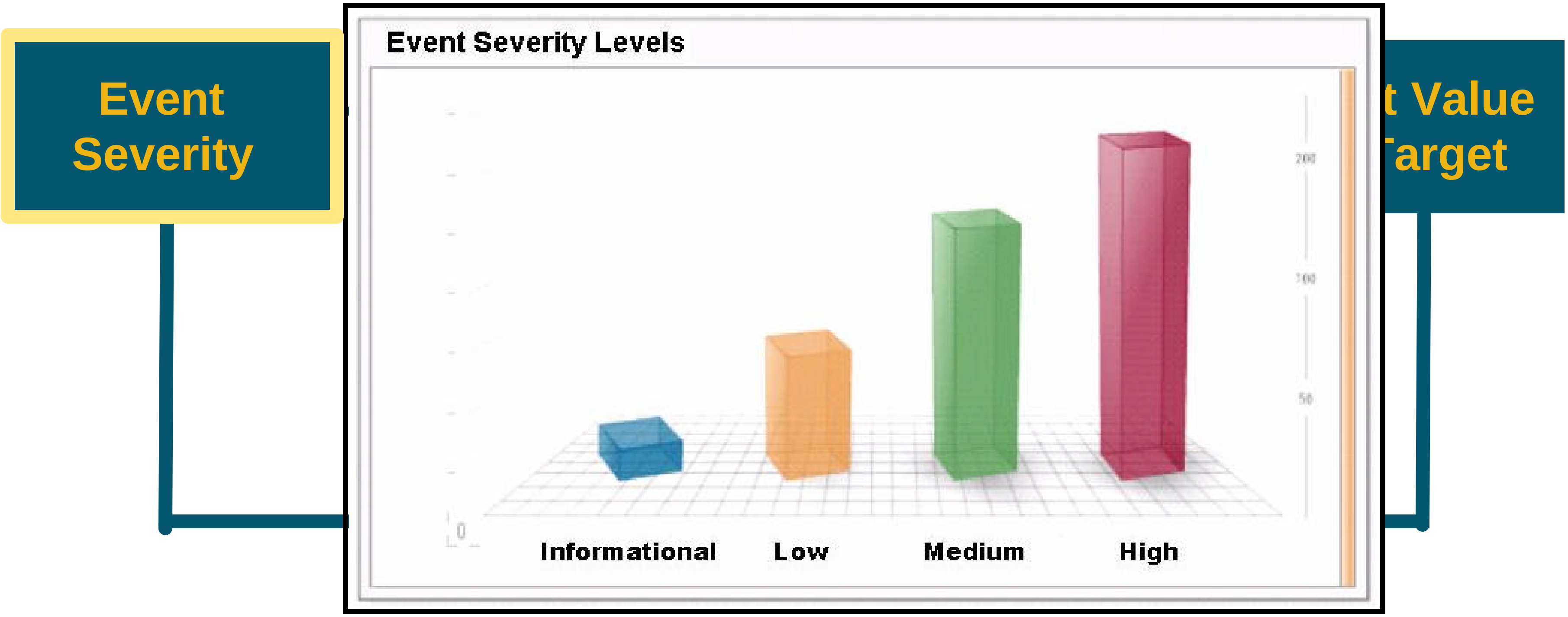
# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

**Rating the Risk Allows Users to Confidently Eliminate Malicious Packets Without Dropping Valid Traffic**



# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

### Alert Severity Defined for the Signature

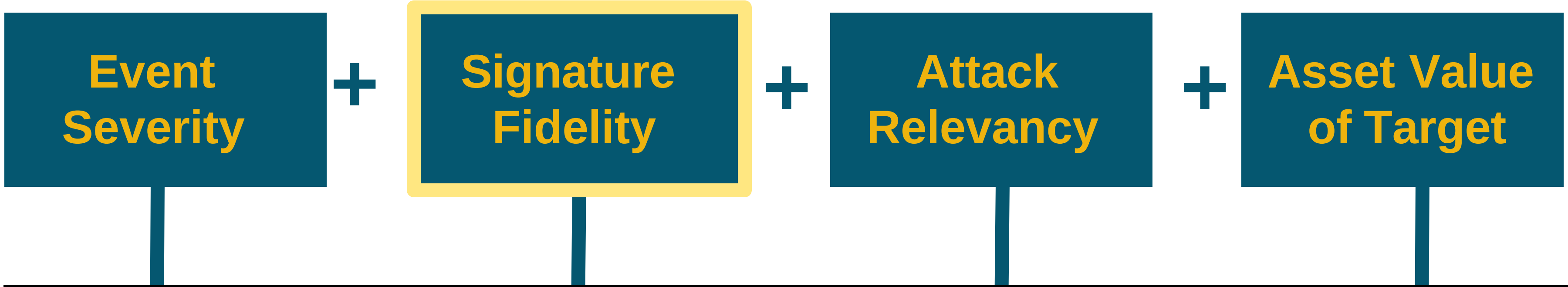


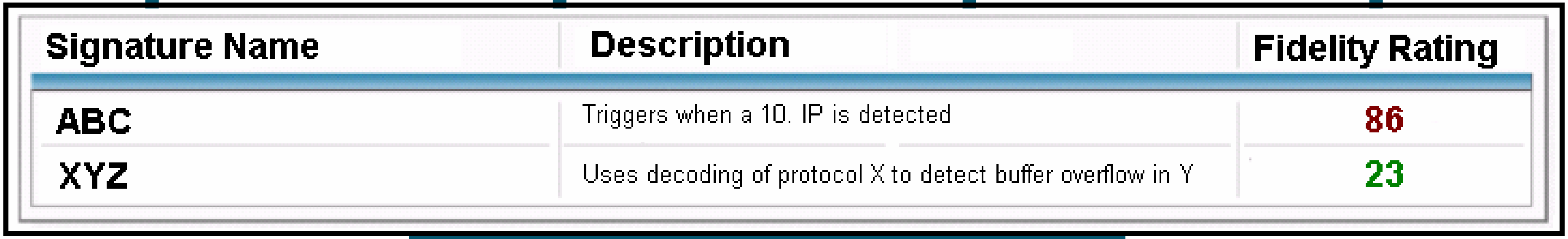
Event Severity

t Value
Target

# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

**Signature Fidelity Rating Delivers a Confidence Rating of the Signature’s Accuracy**



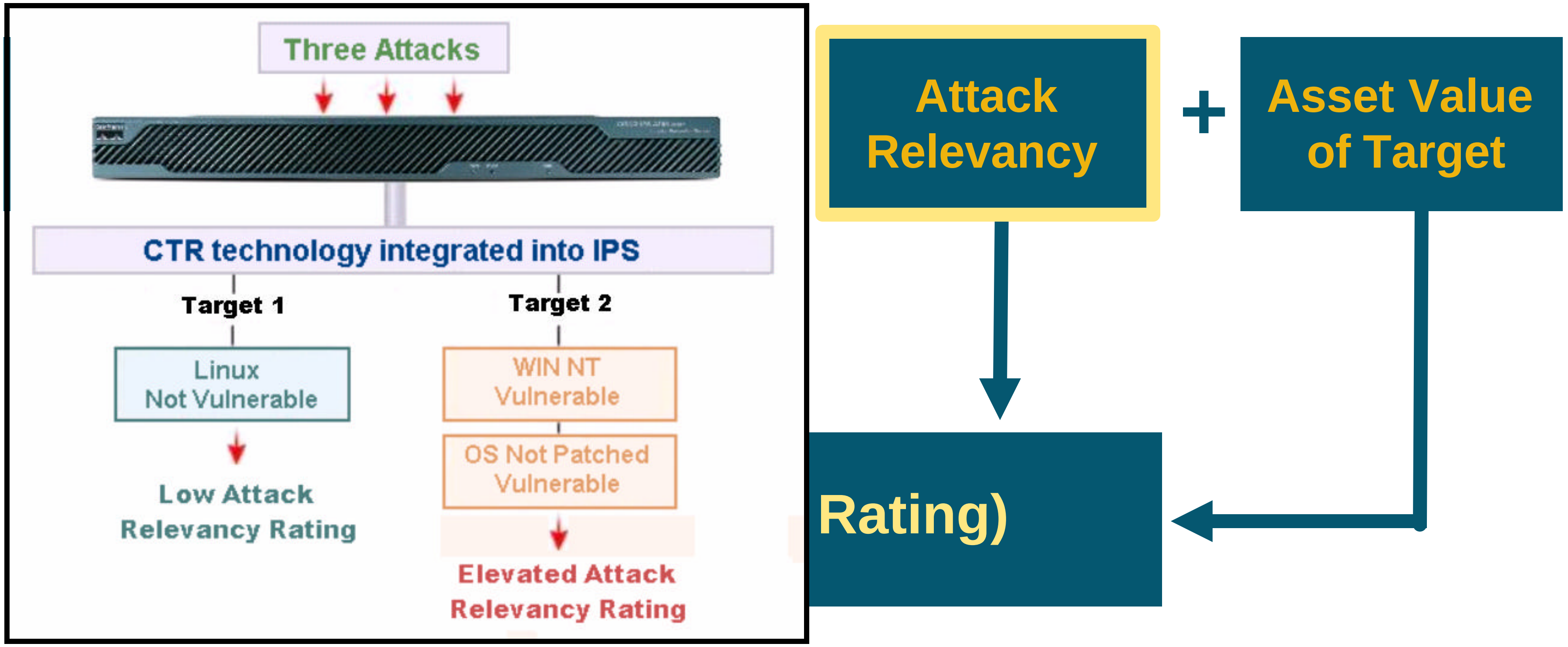


| Signature Name | Description | Fidelity Rating |
|---|---|---|
| ABC | Triggers when a 10. IP is detected | 86 |
| XYZ | Uses decoding of protocol X to detect buffer overflow in Y | 23 |

# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

Cisco.com

### False Alarm Reduction Through Active Target Analysis



Attack Relevancy

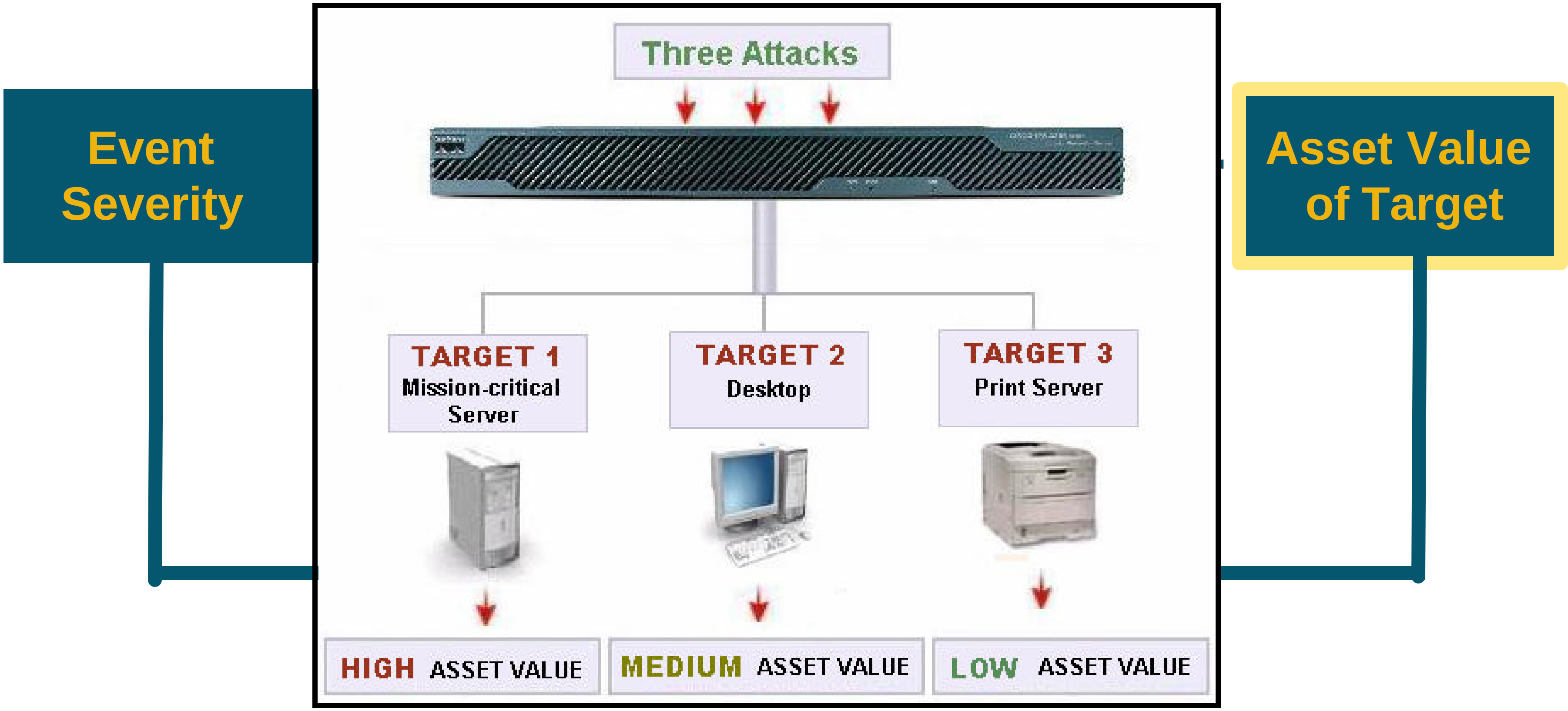
+

Asset Value of Target

Rating)

# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

## Delivering Greater Insight into Relative Criticality of Target Systems through Asset Value Designation

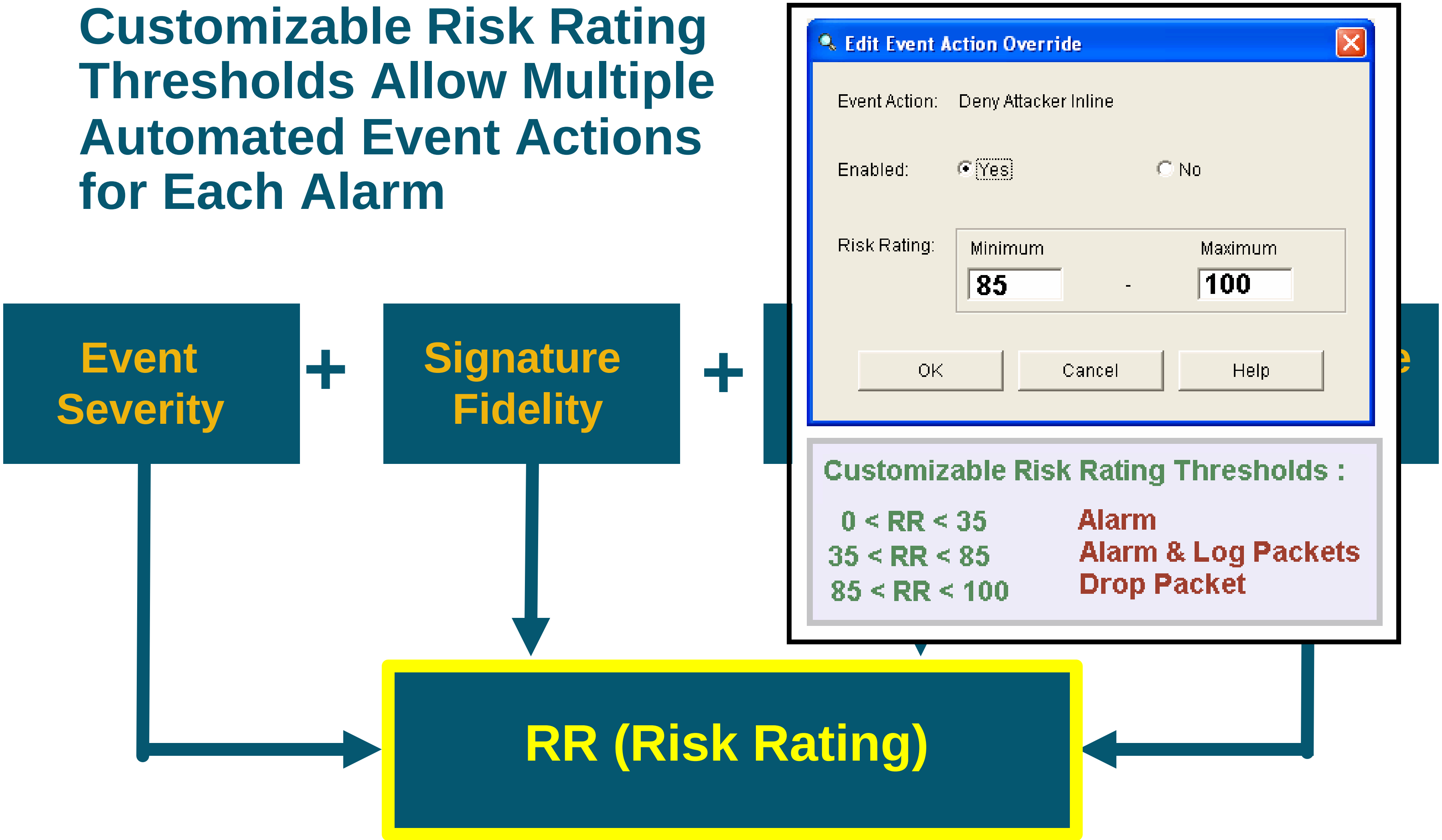


Event Severity

Asset Value of Target

# Process for Accurate Threat Mitigation:
## *Rating Alarms for Threat Context*

## Customizable Risk Rating Thresholds Allow Multiple Automated Event Actions for Each Alarm



**Edit Event Action Override**

Event Action: Deny Attacker Inline

Enabled: ● Yes ○ No

Risk Rating: Minimum 85 - Maximum 100

**Customizable Risk Rating Thresholds :**

| | |
|---|---|
| 0 < RR < 35 | Alarm |
| 35 < RR < 85 | Alarm & Log Packets |
| 85 < RR < 100 | Drop Packet |

# Process for Accurate Threat Mitigation

Threat Mitigated

Sensor Adaptively Mitigates Unknown Threats

Correlate Alarms in Sensing Engine

Accurate Packet Drops Achieved, Valid Traffic Undisrupted

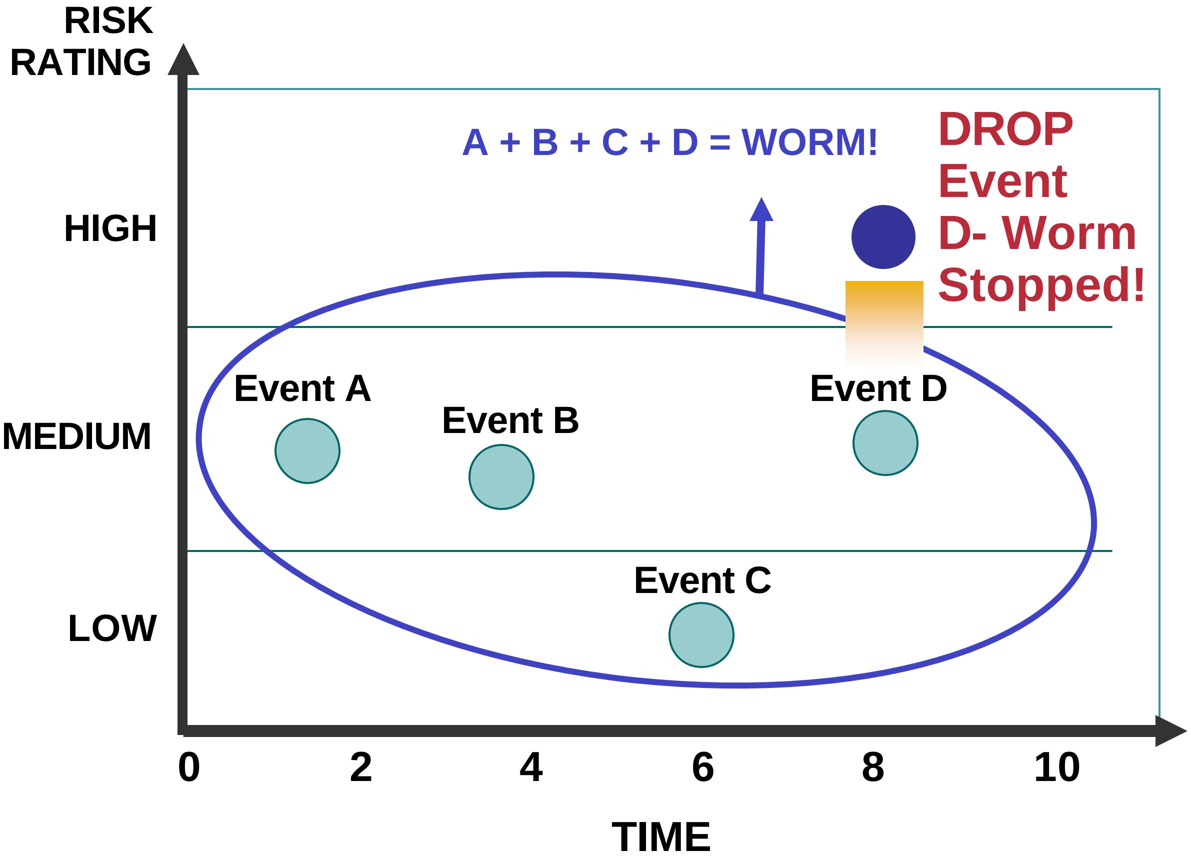
Rate Alarms Based on Contextual Analysis

Broad Array of Attacks are Accurately Classified

Utilize Multiple Threat Classification Techniques

# Process for Accurate Threat Mitigation:
## *Integrated Event Correlation*

On-Box Correlation Allows Adaptation to New Threats in Real-Time without User Intervention



- **Links lower risk events into a high risk meta-event, triggering prevention actions**
- **Models attack behavior by correlating:**

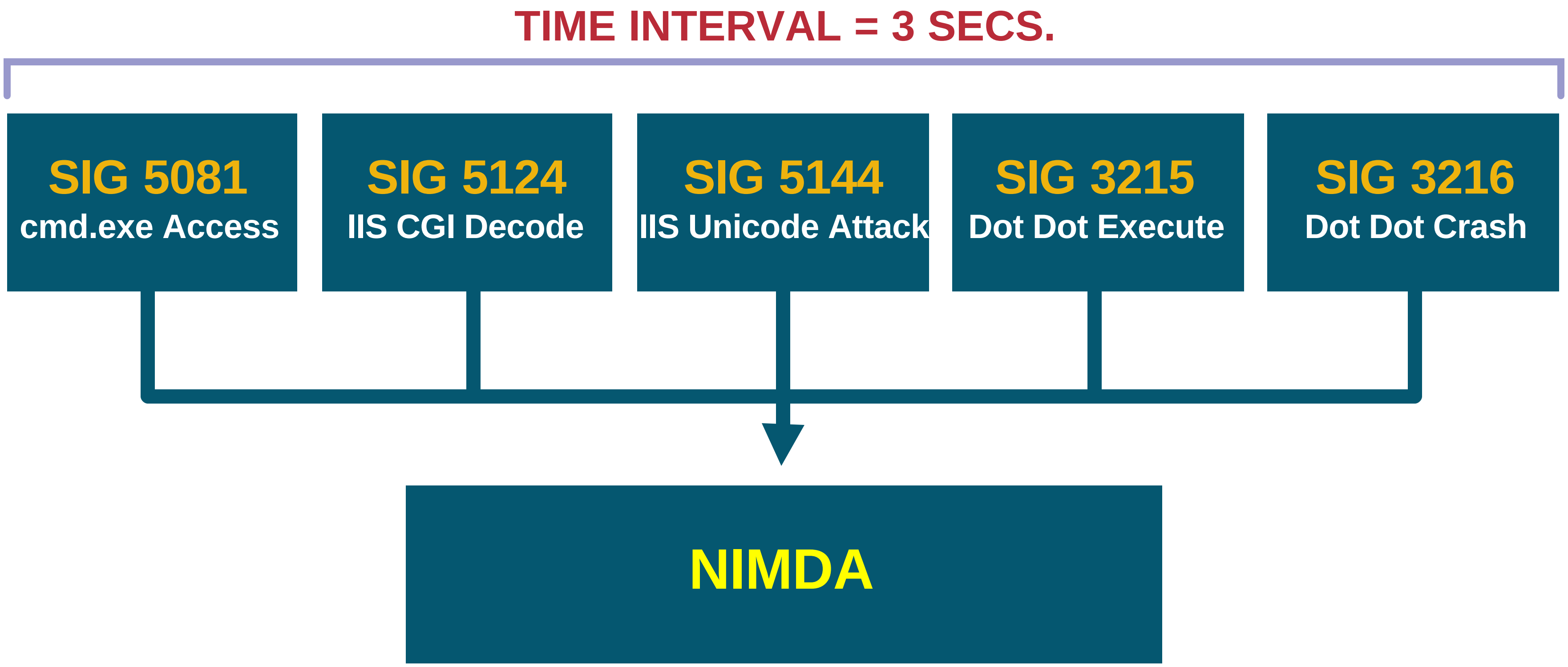
  Event type

  Time span

# Process for Accurate Threat Mitigation:

## *Integrated Event Correlation*

**If SIG IDs 5081, 5124, 5114, 3215 & 3216 Fire within a 3 Sec. Interval, then Trigger the Meta Event, “Nimda”**



TIME INTERVAL = 3 SECS.

SIG 5081
cmd.exe Access

SIG 5124
IIS CGI Decode

SIG 5144
IIS Unicode Attack

SIG 3215
Dot Dot Execute

SIG 3216
Dot Dot Crash

NIMDA

# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# Network IPS Sensor Packet Analysis:
## *A Day in the Life of a Packet*

**Threat Mitigated**

Sensor Adaptively Mitigates Unknown Threats

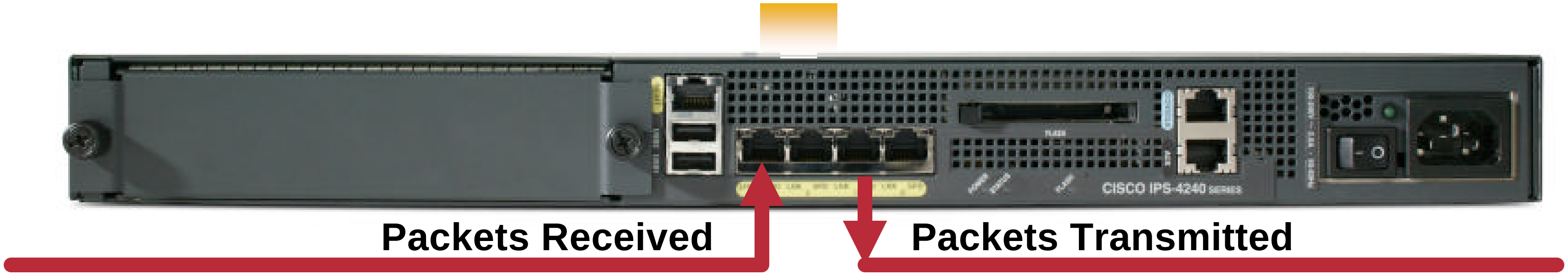
**Rate Alarms Based on Contextual Analysis**

Accurate Packet Drops Achieved, Valid Traffic Undisrupted

**Rate Alarms Based on Contextual Analysis**

Broad Array of Attacks are Accurately Classified

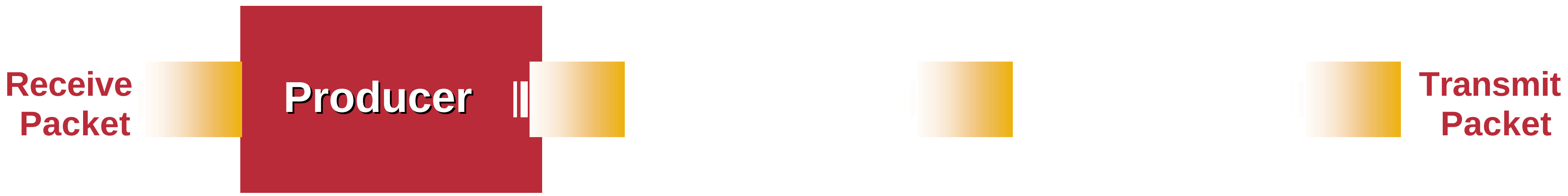
**Utilize Multiple Threat Classification Techniques**

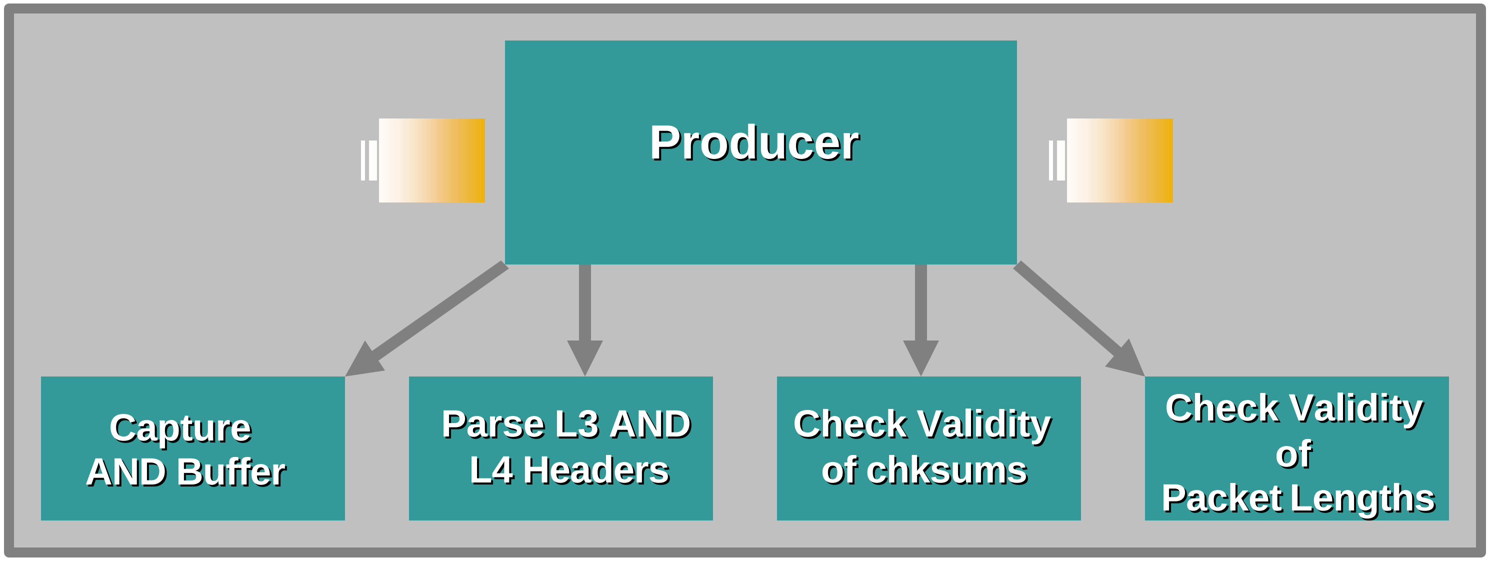


**Packets Received**

**Packets Transmitted**

# Network Sensor Packet Analysis: *The Producer*

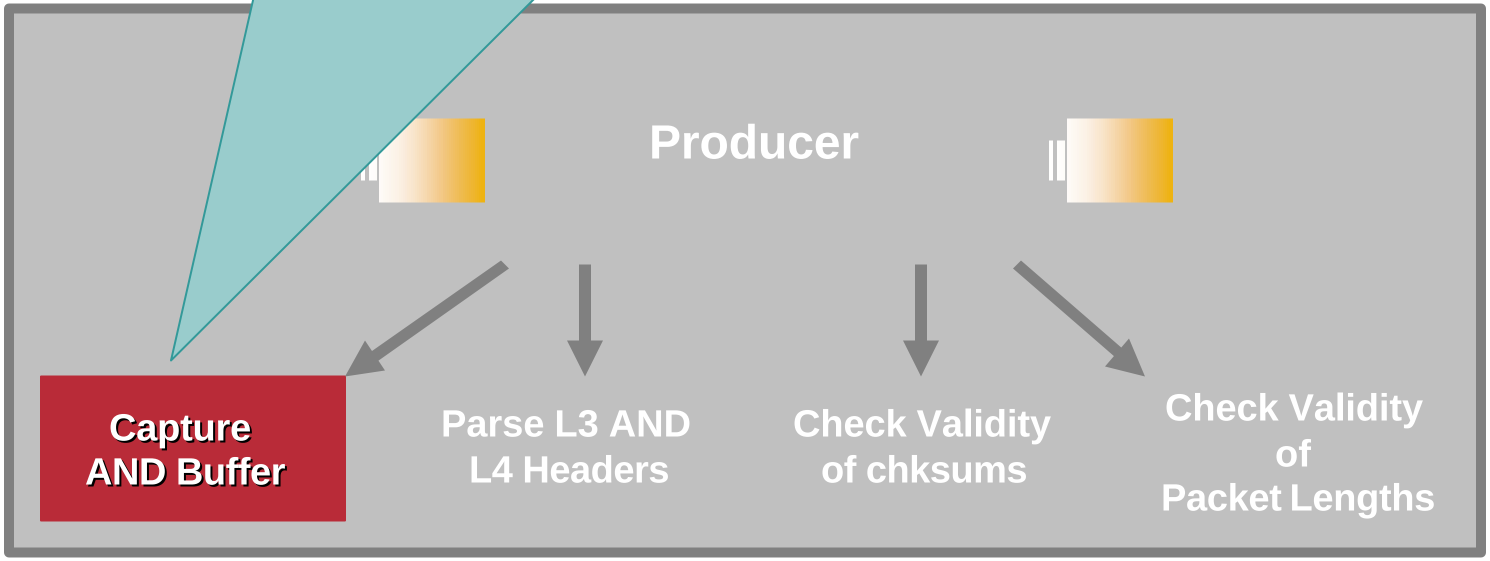




**Based on IPS 5.x Sensor Code**

# Network Sensor Packet Analysis:
## *The Producer*

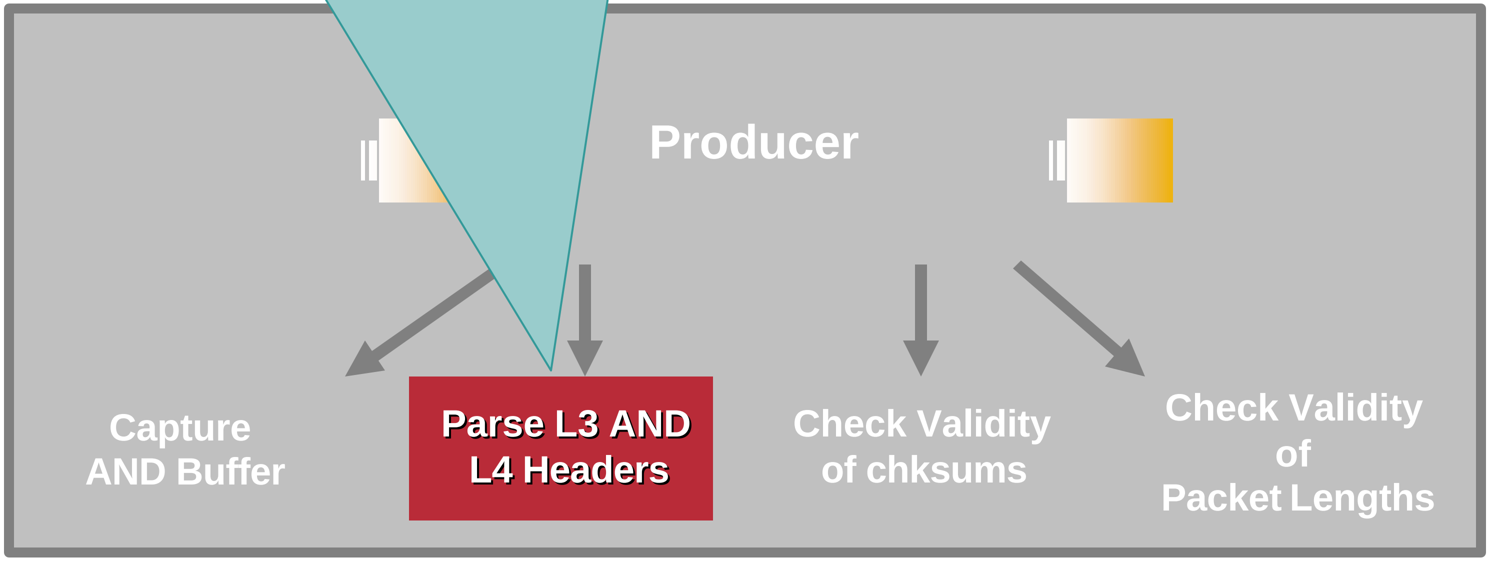
- Packet enter Producer from the NIC of the sensing
- Packets are Captured and Buffered.



**Based on IPS 5.x Sensor Code**

# Network Sensor Packet Analysis: *The Producer*

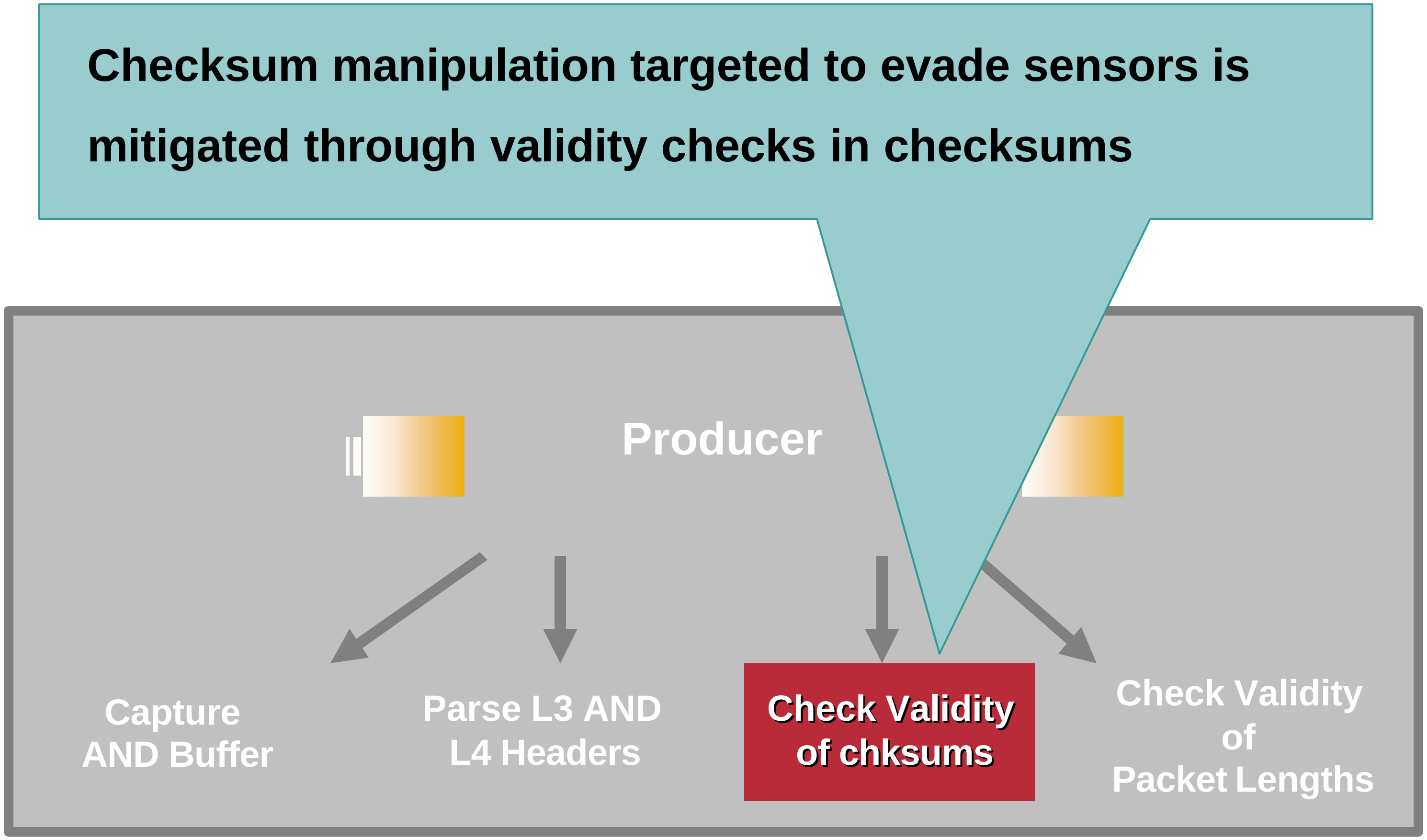
L3 / L4 header information on the packets are parsed and IP / port level information is determined for subsequent processes within the sensor



**Based on IPS 5.x Sensor Code**

# Network Sensor Packet Analysis:
## *The Producer*

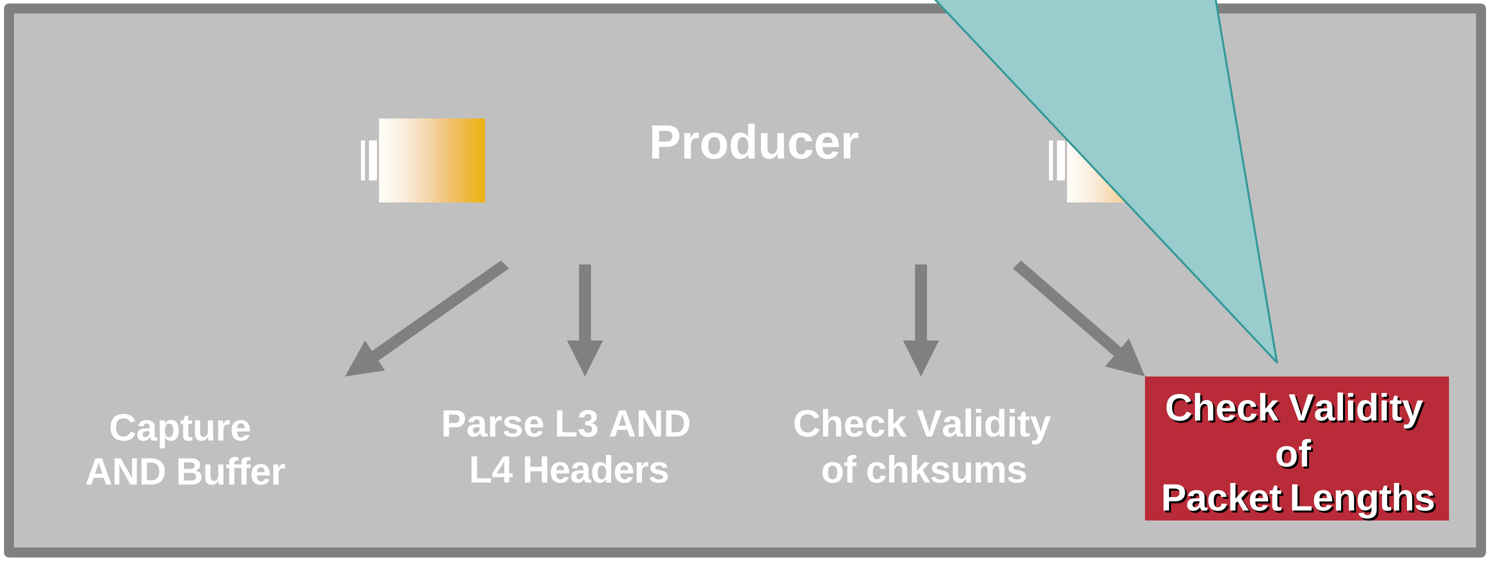
Checksum manipulation targeted to evade sensors is mitigated through validity checks in checksums



**Based on IPS 5.x Sensor Code**

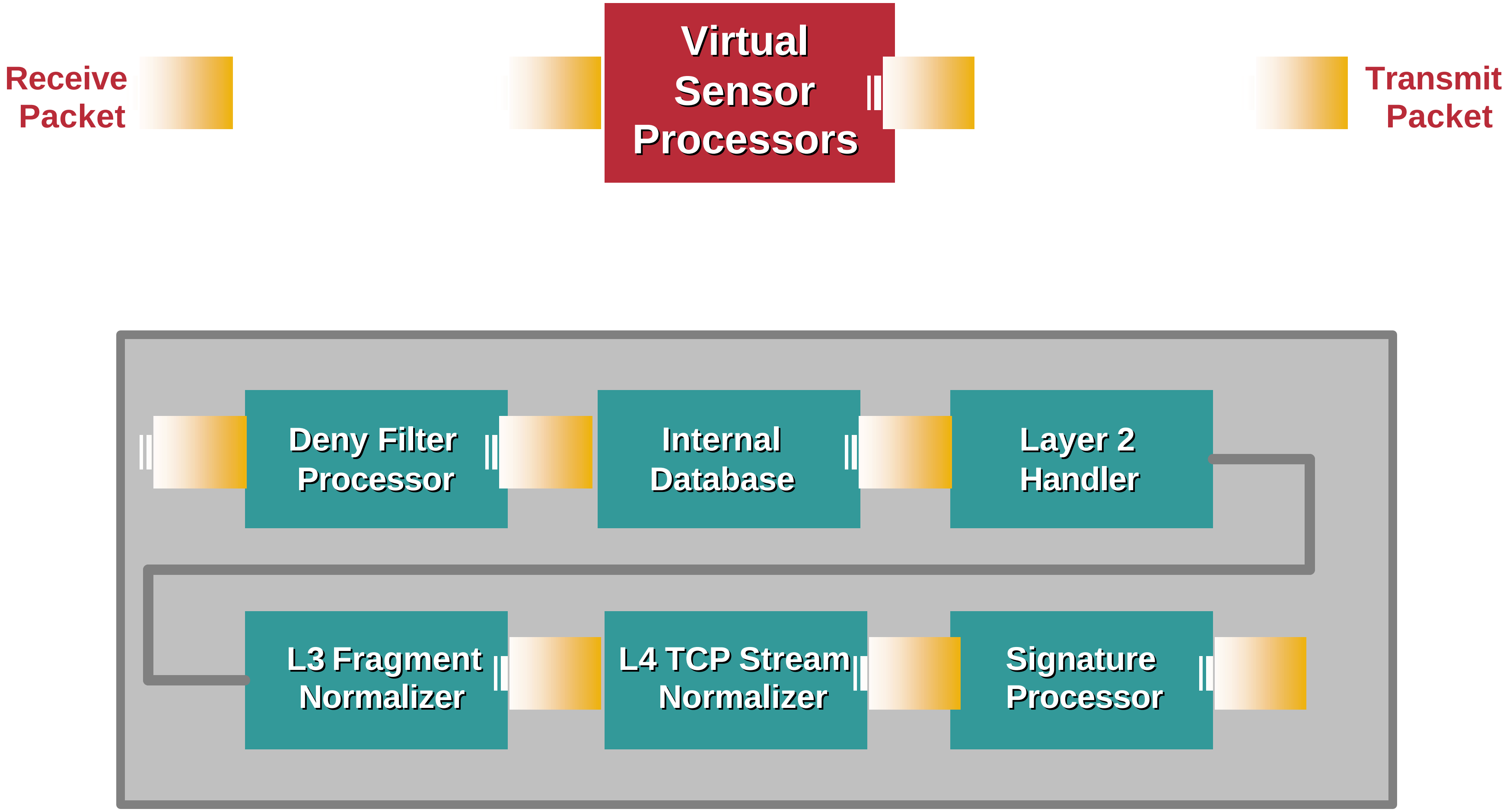
# Network Sensor Packet Analysis: *The Producer*

Validity checks on packet lengths prevent the attacker from evading an IPS by crafting packets to contain packet length specifications that are different from the actual packet length.



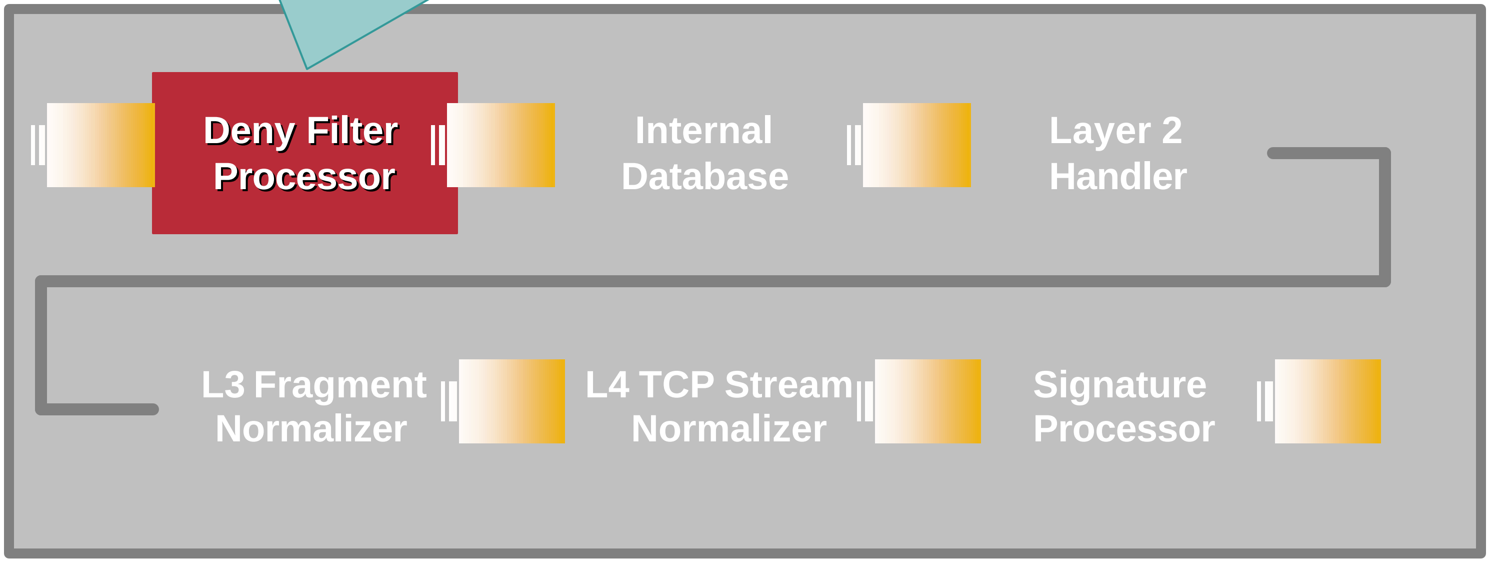
Based on IPS 5.x Sensor Code

# Network Sensor Packet Analysis: *Virtual Sensor Processors*



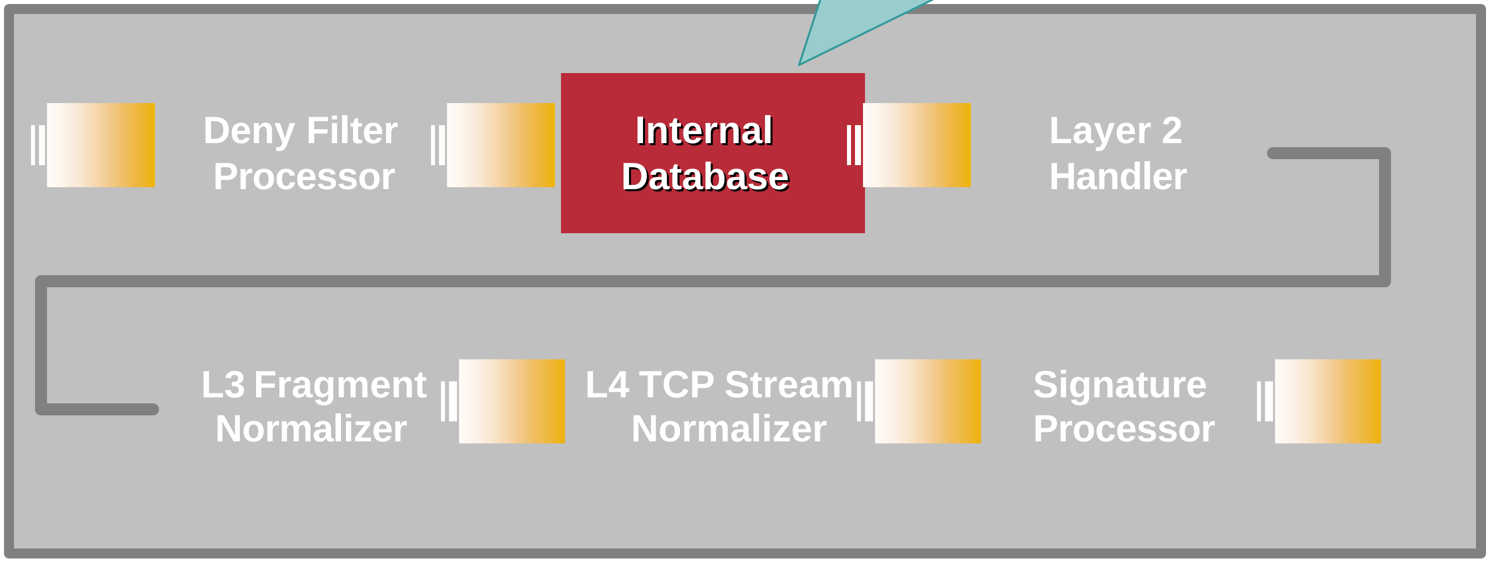
# Network Sensor Packet Analysis:
## *Virtual Sensor Processors*

**The Deny Filter Processor contains the list of IP addresses on which the “deny attacker inline” response action has been applied. The sensor discontinues subsequent processing on packets that originate from IP addresses on this list.**



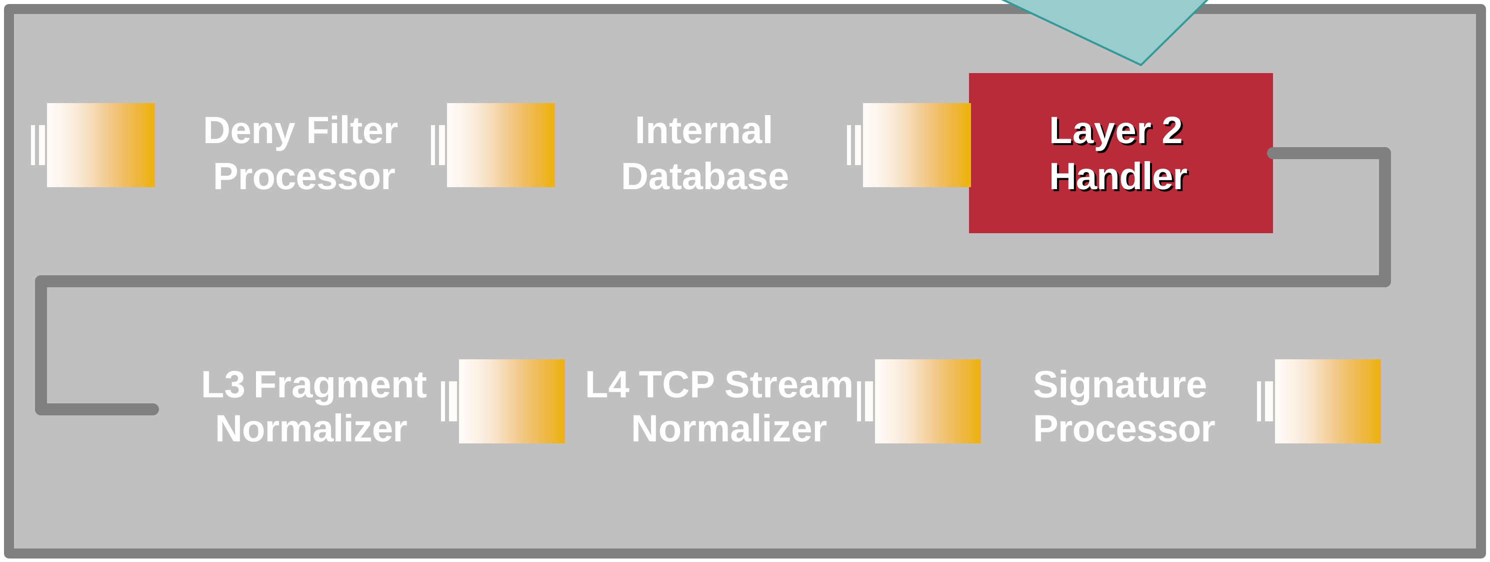
# Network Sensor Packet Analysis:
## *Virtual Sensor Processors*

The Internal Database Processor inspects the 4 tuple (i.e. AaBb where Aa is Source address/port and Bb is Destination address/port).



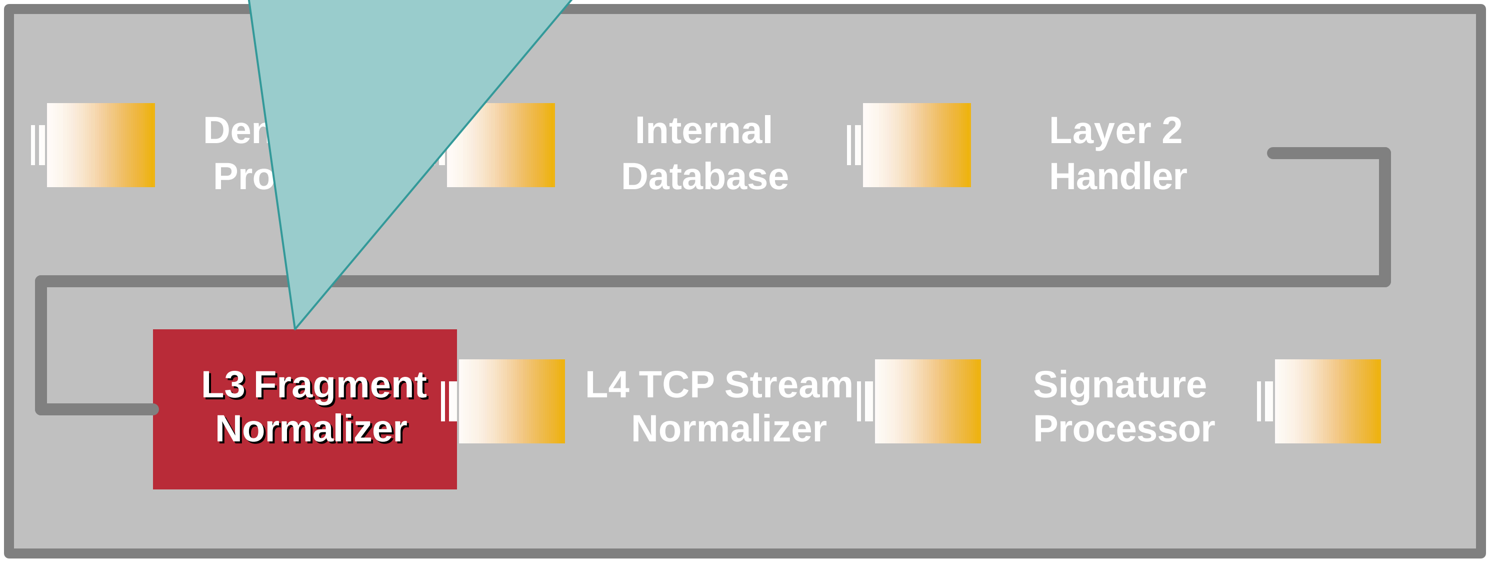
# Network Sensor Packet Analysis: *Virtual Sensor Processors*

The Layer 2 handler was designed to inspect packets for threats that are common in Layer 2 switched environments. The Layer 2 engine mitigates threats posed by Dsniff, for example ARP spoofing, MAC flooding among other attacks.



# Network Sensor Packet Analysis: *Virtual Sensor Processors*

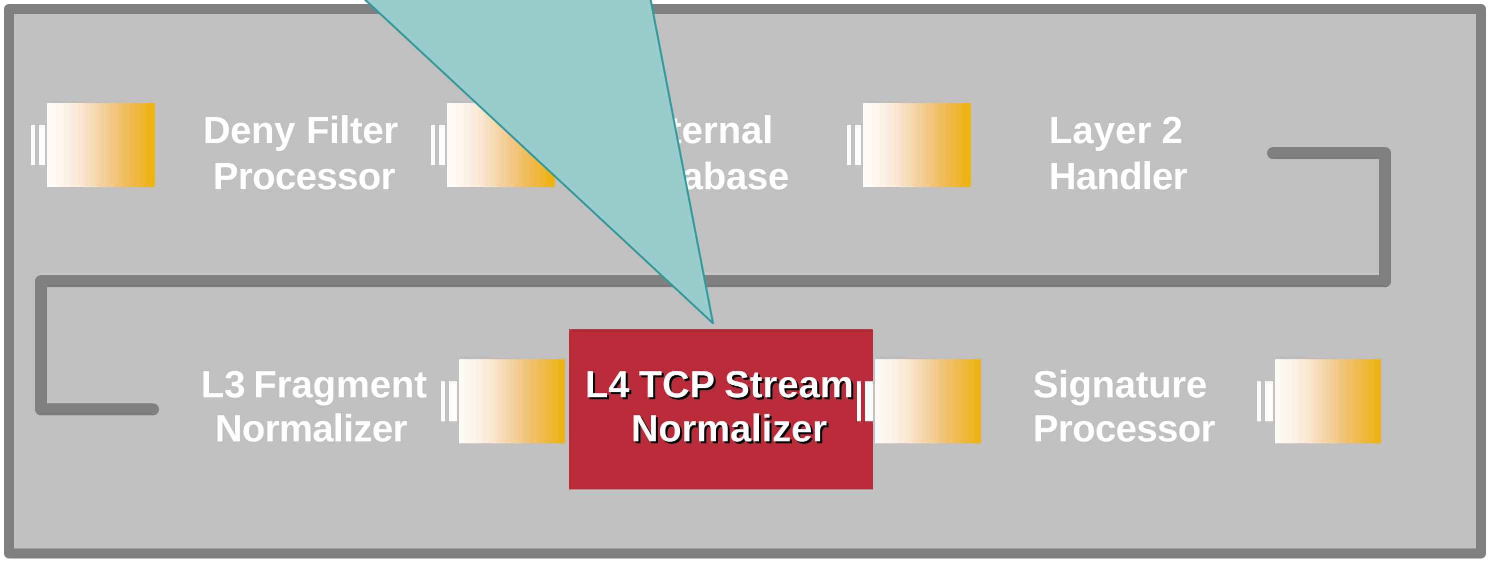
**In the L3 Fragmentation Normalizer, a datagram table is maintained that stores fragments of packets until all fragments within the stream have been collected, after which these fragments are reassembled and sent on for further signature processing.**



# Network Sensor Packet Analysis:
## *Virtual Sensor Processors*

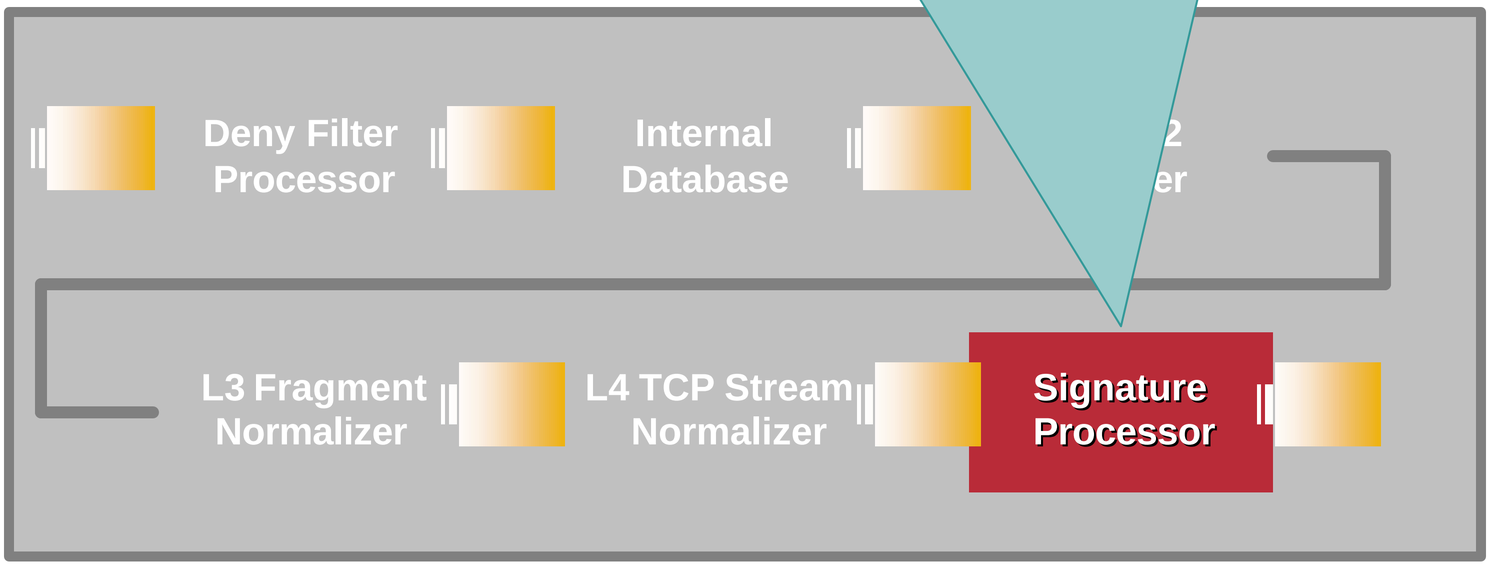
Cisco.com

The L4 TCP Stream Normalizer establishes whether or not the packets being detected are part of a valid stream to prevent the intentional injection of crafted packets that do not exhibit the TCP 3-way handshake

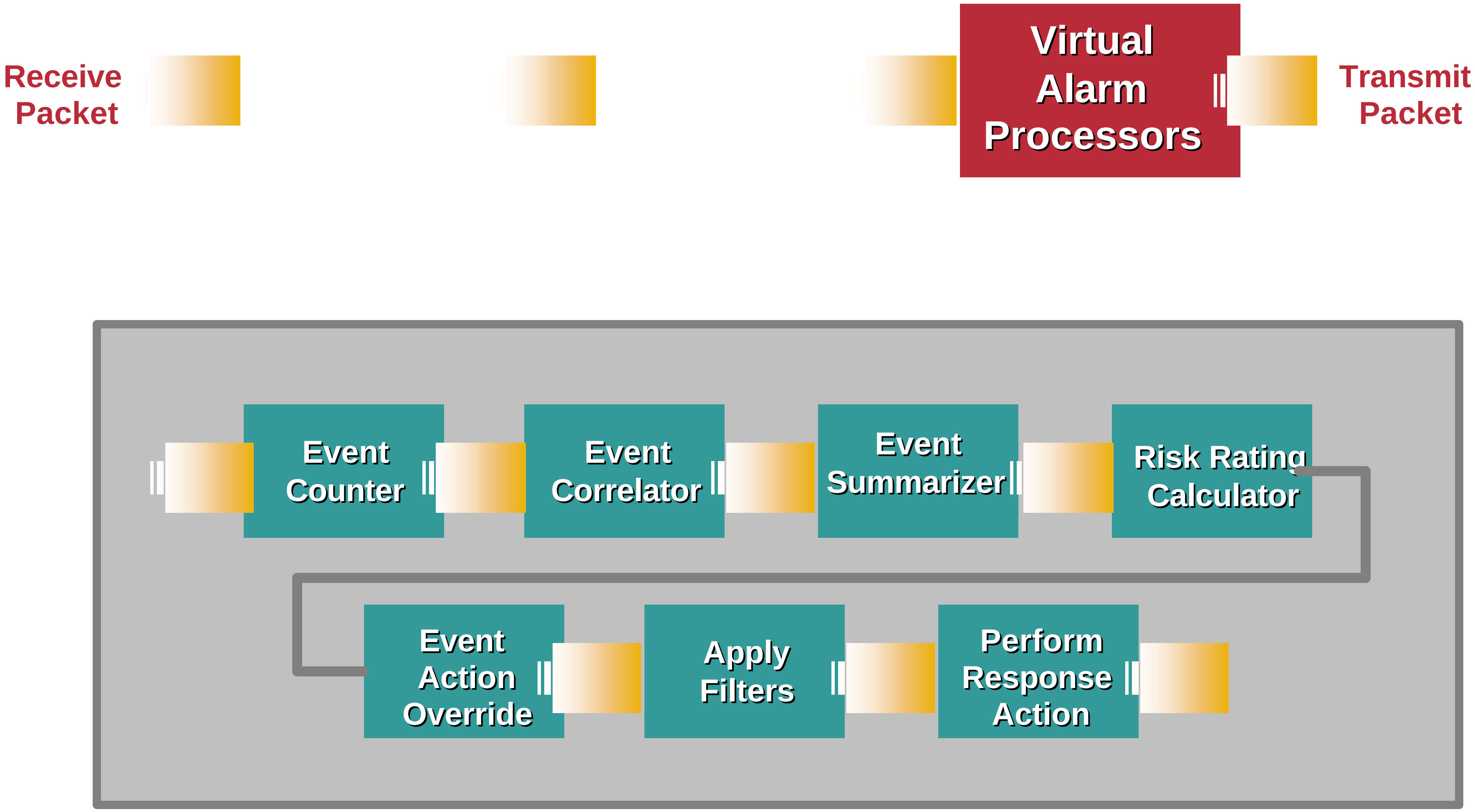


# Network Sensor Packet Analysis: *Virtual Sensor Processors*

**The Signature Processor performs signature matching analysis on all the packets. The Signature Processor utilizes hybrid detection capabilities to classify a broad array of threats.**

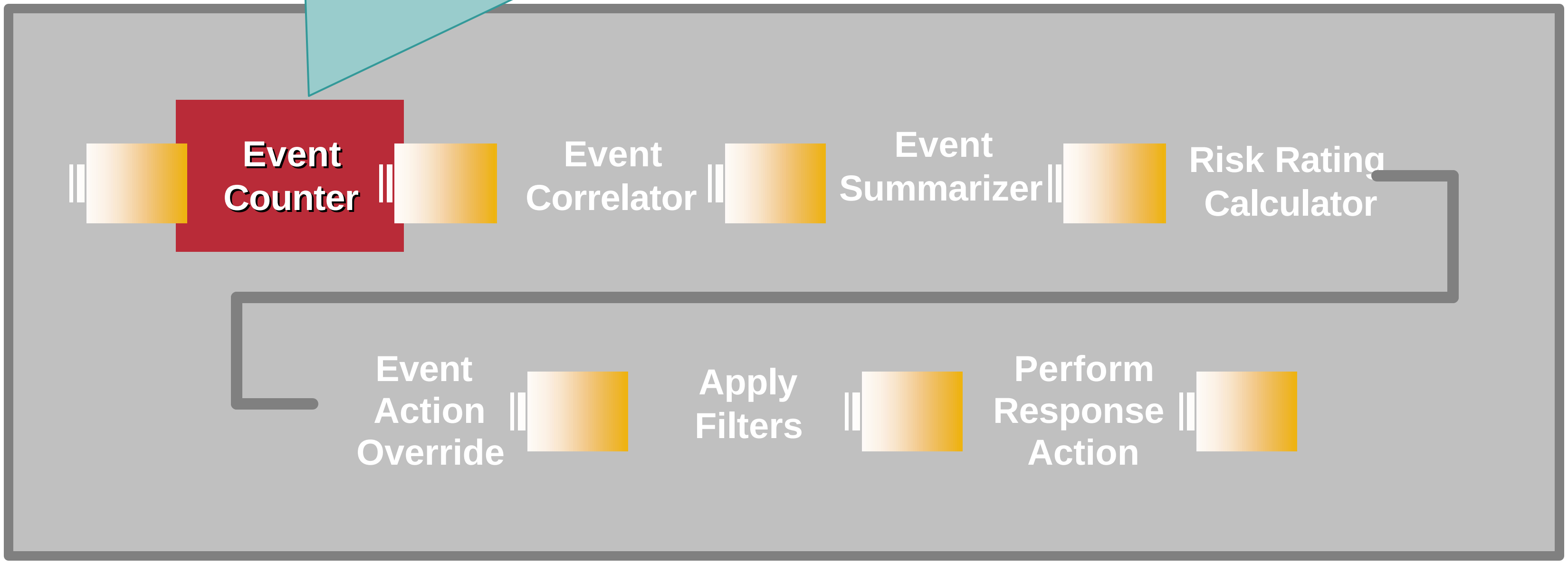


# Network Sensor Packet Analysis: *Virtual Alarm Processors*



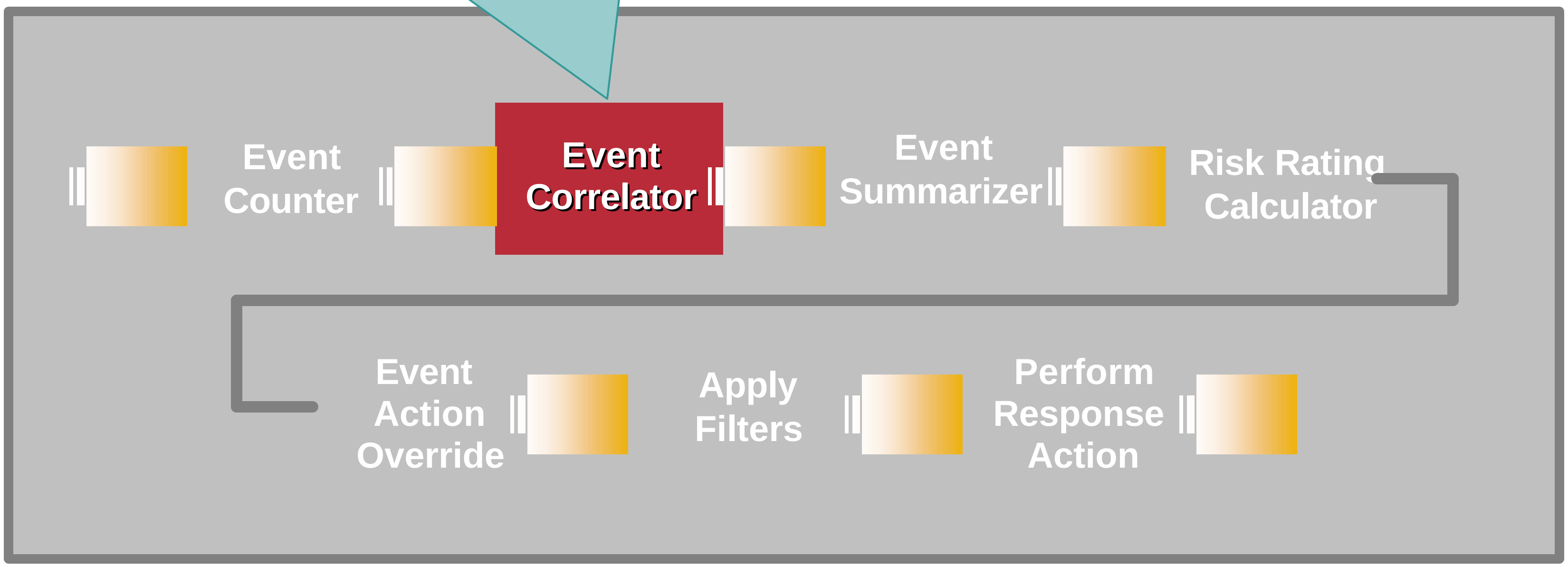
# Network Sensor Packet Analysis: *Virtual Alarm Processors*

The Event Counter performs tasks relating to the behavior of alarm triggers. An example of such a variable is “MinHits”, that specifies a minimum number of signature fires before the alarm is sent.



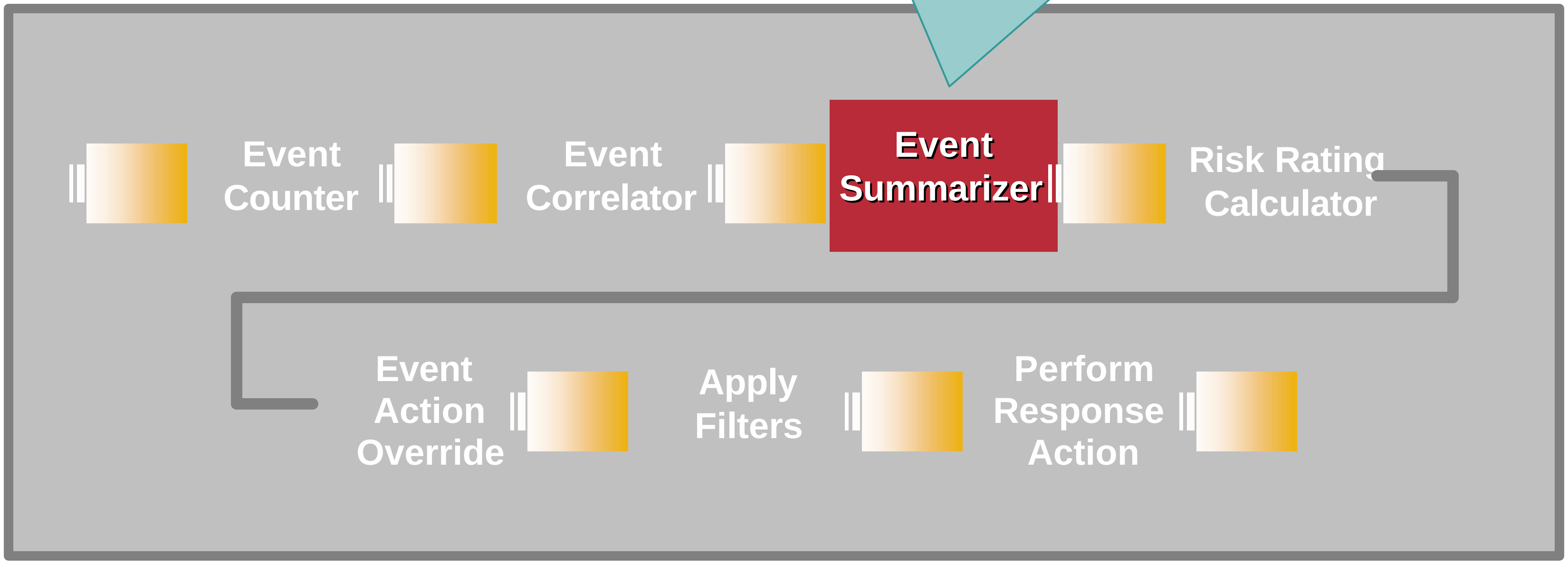
# Network Sensor Packet Analysis: *Virtual Alarm Processors*

**The Event Correlator contains MEG (Meta Event Generator) that delivers an extensible architecture to provides sensor-level event correlation and corroboration.**



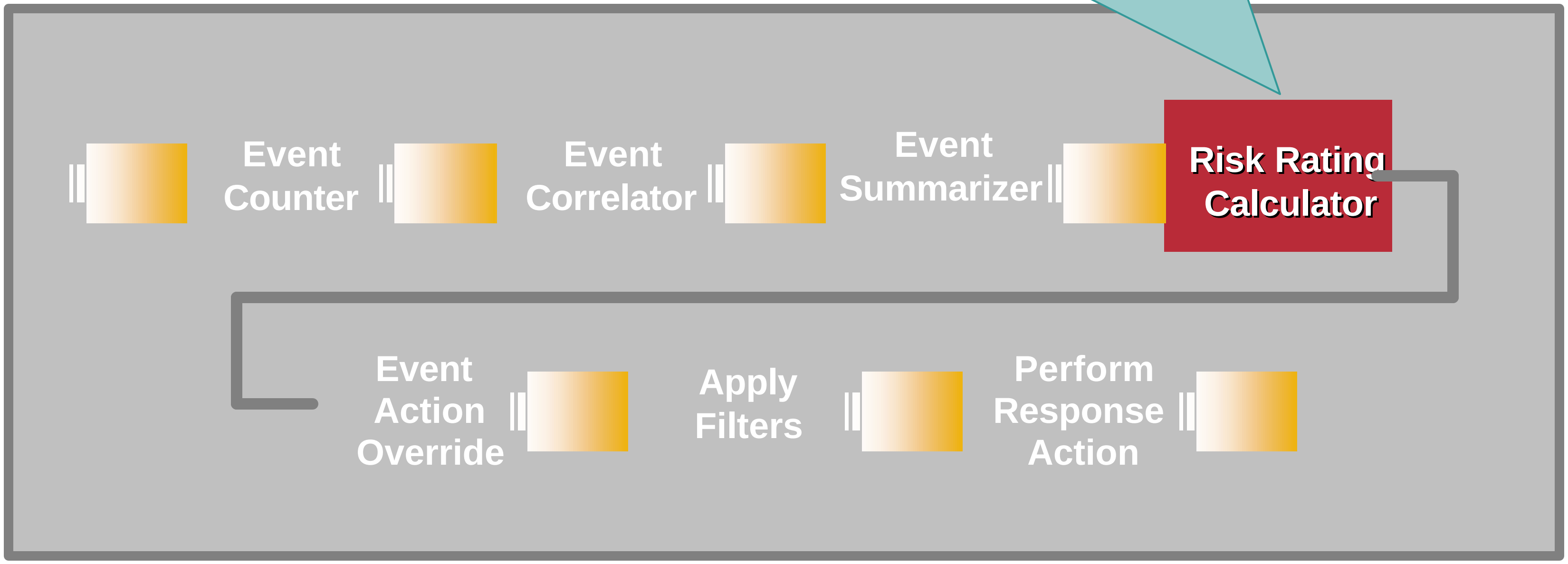
# Network Sensor Packet Analysis: *Virtual Alarm Processors*

**The Event Summarizer executes alarm throttling commands configured by the user. The end result is the ability for the user to minimize the alarm bandwidth of flood attacks.**



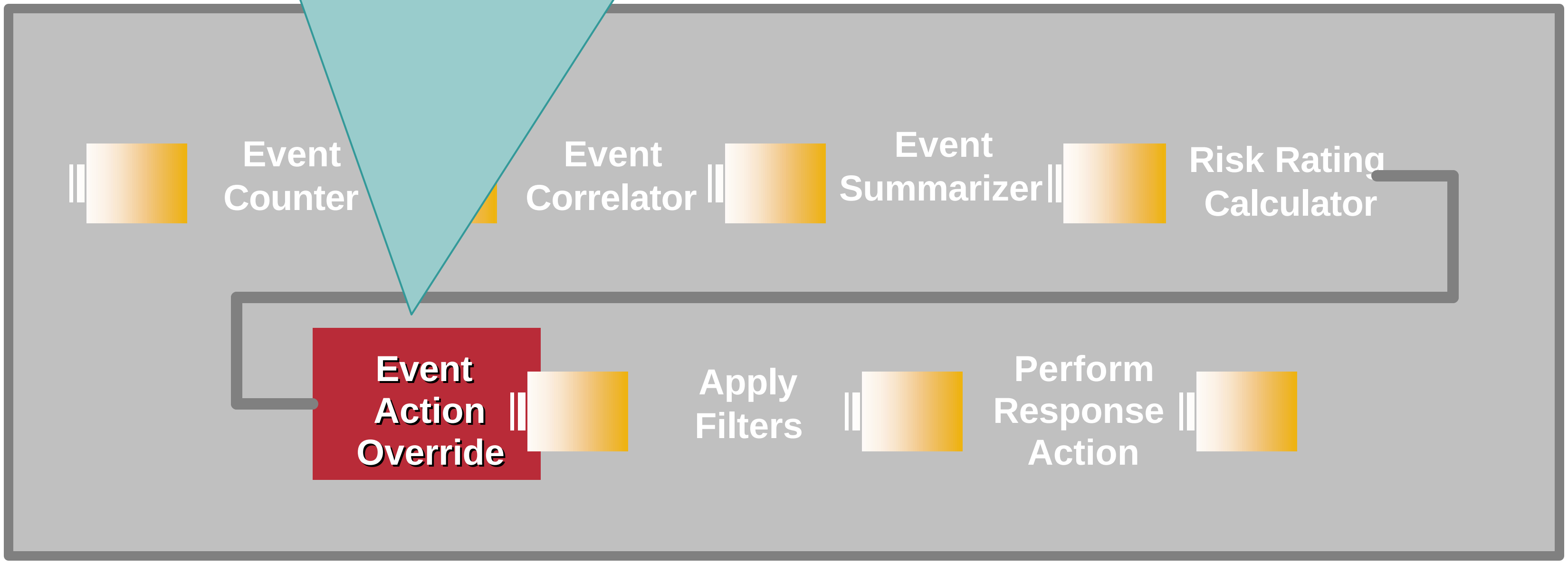
# Network Sensor Packet Analysis:
## *Virtual Alarm Processors*

This rating can be used to illuminate the events to provide a means for developing risk-oriented event action policies when the sensor is deployed in the IPS mode



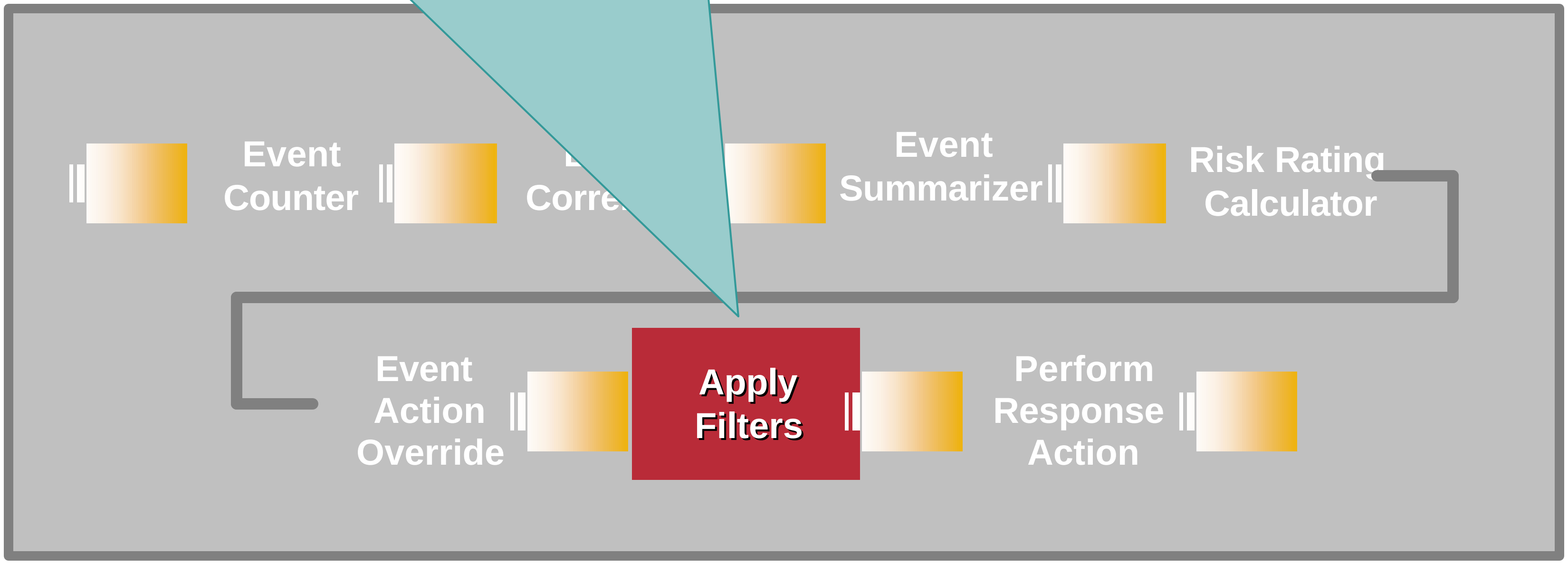
# Network Sensor Packet Analysis: *Virtual Alarm Processors*

The user may apply Risk Rating thresholds that can be globally applied across all alarms that are triggered by the sensor. The sensor can be dynamically made to override existing response actions with inline drop actions, when the thresholds are exceeded



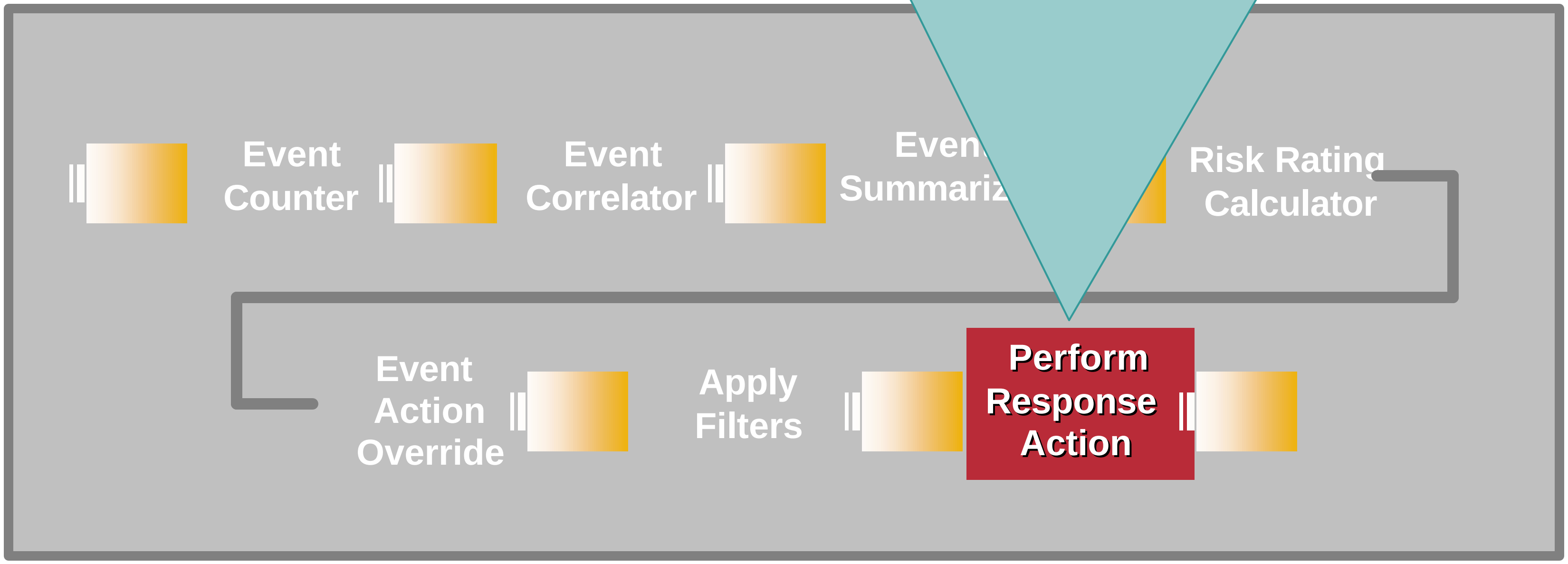
# Network Sensor Packet Analysis:
## *Virtual Alarm Processors*

**The last stage of the VAP, prior to the execution of response actions, is to apply user defined Filters that specify IP address sets on which response actions must not be applied.**



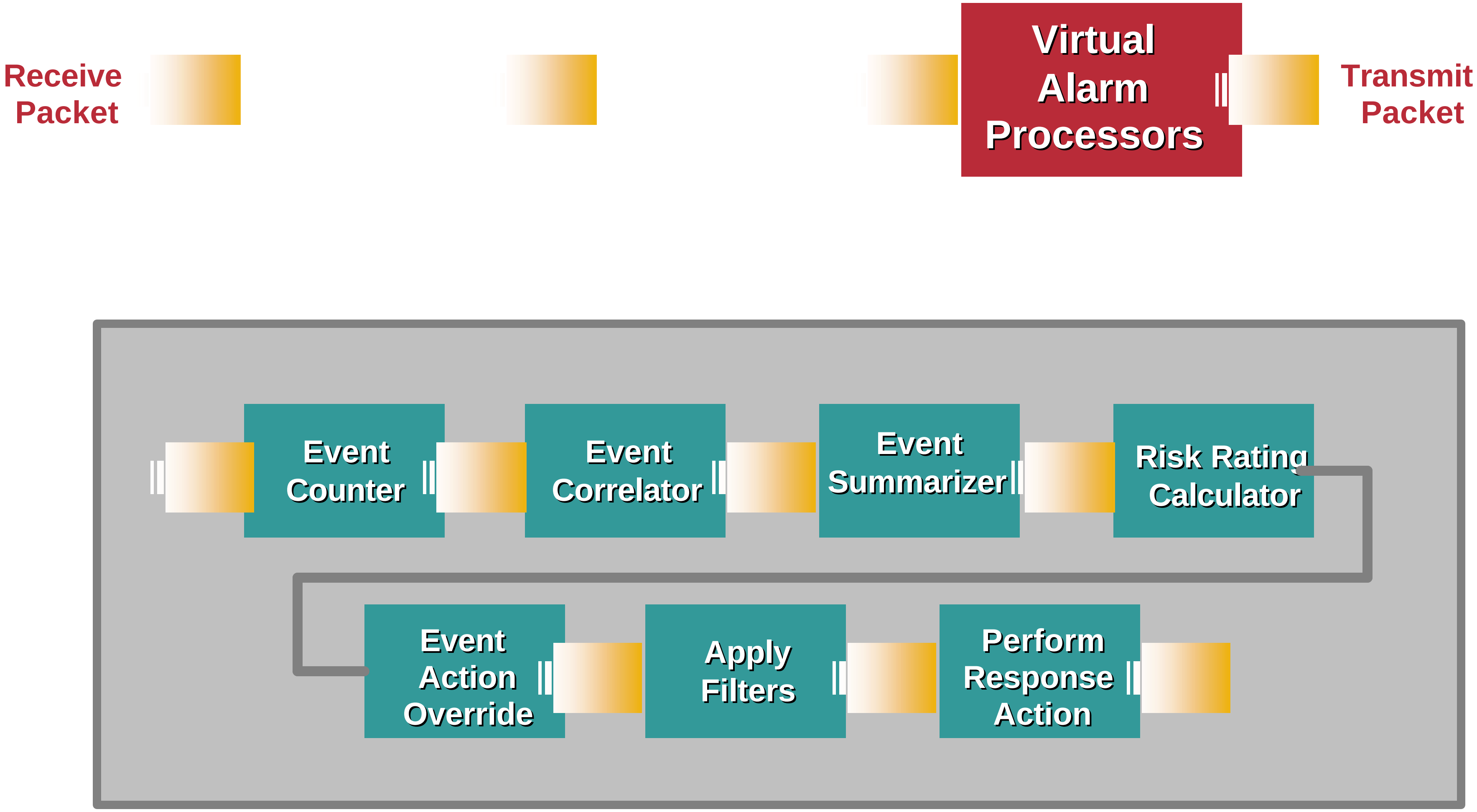
# Network Sensor Packet Analysis: *Virtual Alarm Processors*

The following response actions can be configured on a per signature basis: Produce Alert ; Produce Verbose Alert; Request SNMP Trap; Log Pair Packets; Log Victim Packets; Log Attacker Packets; Reset TCP Connection; Request Block Connection; Request Block Host; Deny Attacker Inline; Deny Connection Inline; Deny Packet Inline



# Network Sensor Packet Analysis:
## *Virtual Alarm Processors*

Cisco.com



# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# High Level Deployment Considerations

## Planning Points for IPS

- General Location Decisions

  Purpose of deployment

  Response actions used

- Specific Location Decisions

  Platform choice: Integrated or stand-alone

  Re-cabling and other physical requirements

  Inline Performance Requirements

  Control and Responsibility Issues for an inline device

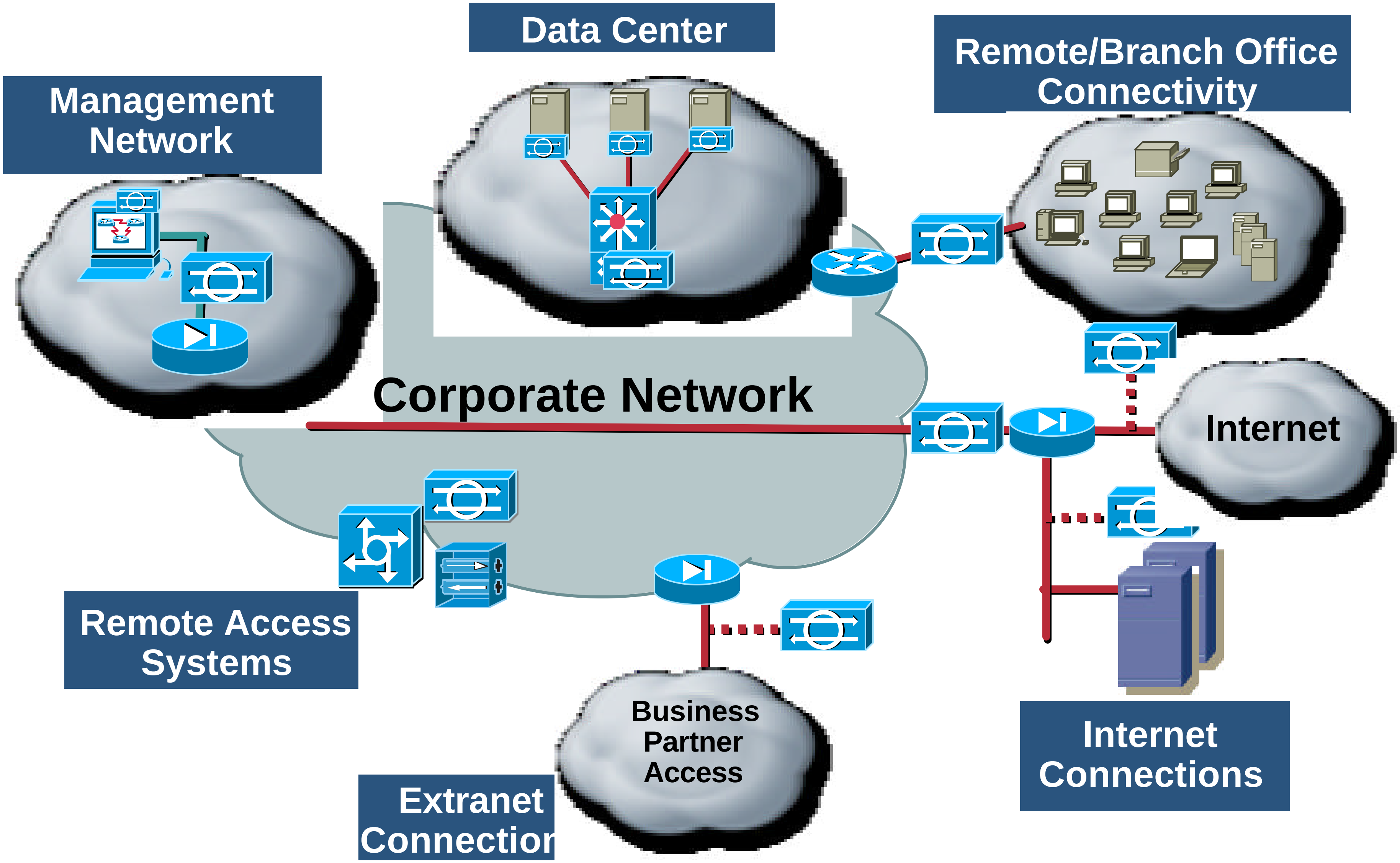
# IPS Traffic Considerations

An IPS sensor deployed into the traffic stream will have an effect on traffic flow.

- Packet effects: Latency should generally be under a millisecond; packet drops will impact traffic streams
- Network effects: Bandwidth restriction i.e. Do not try and push 500 mbps through a device rated for 200 mbps
- Exceeding the performance of a sensor will result in dropped packets and a general degradation of network performance. TCP resiliency (retransmits, changing window sizes, etc) will have an effect on the amount of degradation.

# IPS / IDS Deployment

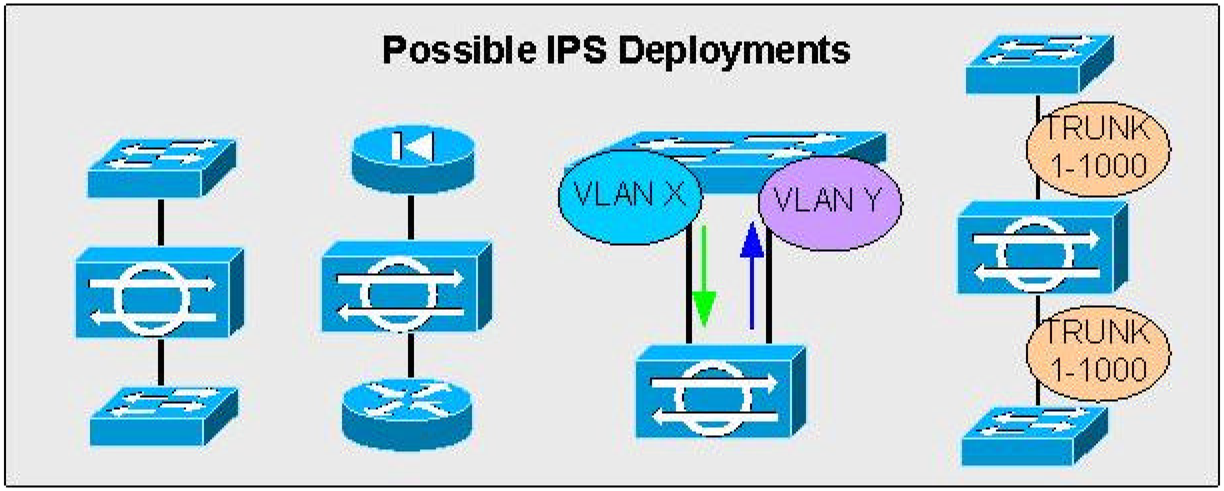
## *What Areas of the Network Are Candidates?*



# IPS Appliance Deployment Examples

**IPS Appliance Sensor deployment examples:**

- **Two L2 Devices (non trunk)**
- **Two L3 Devices**
- **Bridging 2 VLANs on same Switch**
- **Two L2 Devices (trunked; 802.1q)**
- **Hybrid IDS / IPS mode**



# Deployment Challenges

- **Asymmetric traffic – Due to the fact that IPS sensors need to see both sides of a conversation to be able to build the correct state, asymmetric traffic patterns pose challenges**

  **Solutions**

  **•Either the sensors need to share 'state' information between them; Exceptionally difficult with more than 2 sensors and typically requires that the total bandwidth be less than or equal to the capacity of a single sensor**

  **•An alternative is to use the network to pass the correct traffic to a single sensor until or unless that sensor fails, at which time all the traffic then gets redirected to the backup sensor;  Introduces a high degree of network complexity and requires that the total bandwidth be less than or equal to the capacity of a single sensor**

# Tuning IPS Sensors

- Tuning is the most important part of intrusion detection and prevention deployments

  The data reduction that results from proper tuning is essential for a fully functional system

- Not every sensor needs to alert on every event

  Implementing environment specific configurations increases scalability of the entire system

# Tuning: Where to Start

- **Most sensors ship with a default signature configuration**

  **This is a good starting point for an initial deployment in most cases**

- **Start by monitoring the default configuration**

  **Prioritize the tuning of the high priority alarms, and then move on to the mediums**

# How to Tune a Sensor: Techniques

- Understand the environment and traffic patterns
- List out potential false positives

    Analyze each alert and classify stimulus and response

- Define policy, and policy exceptions

    i.e. Ping sweeps generate alarms, except when coming from the management network

- Turn down severity of signatures not applicable to that environment
- Iterative process: as traffic patterns change, sensors can require re-tuning
- Use on-box correlation techniques

# Active Response Actions

**Inline Drop Actions** for comprehensive worm mitigation

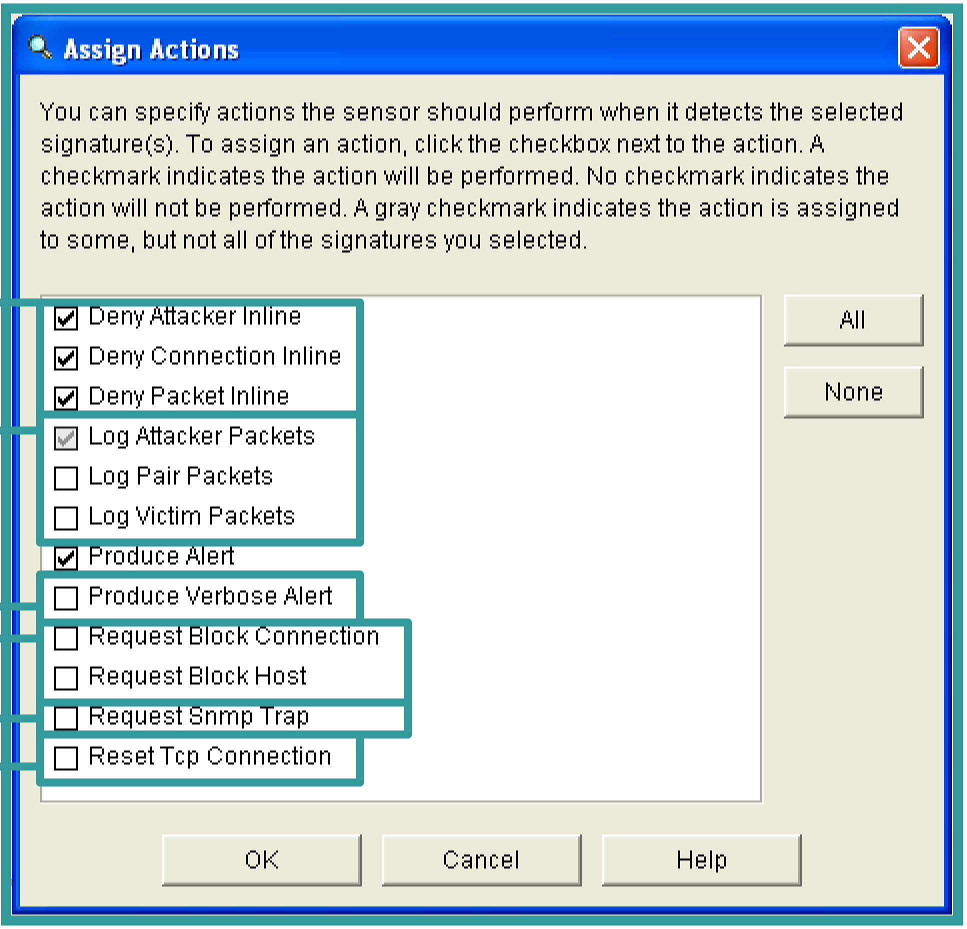
**Packet Logging** for advanced forensics analysis

Inclusion of **Trigger Packet** in alarm for greater visibility into attack

**Blocking** hosts at strategic network ingress points

**SNMP Trap** generation with alarm details and sensor diagnostics

**Connection resets** to mitigate TCP based attacks



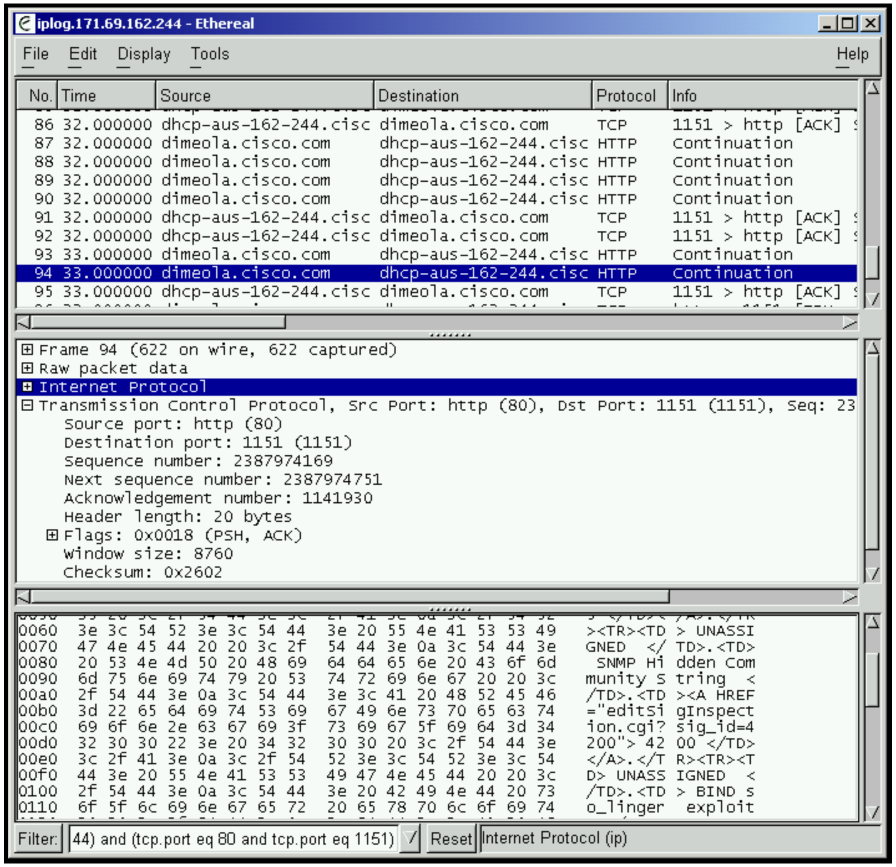
You can specify actions the sensor should perform when it detects the selected signature(s). To assign an action, click the checkbox next to the action. A checkmark indicates the action will be performed. No checkmark indicates the action will not be performed. A gray checkmark indicates the action is assigned to some, but not all of the signatures you selected.

☑ Deny Attacker Inline
☑ Deny Connection Inline
☑ Deny Packet Inline
☑ Log Attacker Packets
☐ Log Pair Packets
☐ Log Victim Packets
☑ Produce Alert
☐ Produce Verbose Alert
☐ Request Block Connection
☐ Request Block Host
☐ Request Snmp Trap
☐ Reset Tcp Connection

# Logging: Session Capture

Cisco.com

- Logs traffic associated with a signature trigger (in pcap format)
- Generally, only trigger and subsequent packets logged
- Does impact sensor performance



```
No. Time      Source                  Destination             Protocol Info
 86 32.000000 dhcp-aus-162-244.cisc dimeola.cisco.com       TCP      1151 > http [ACK]
 87 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 88 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 89 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 90 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 91 32.000000 dhcp-aus-162-244.cisc dimeola.cisco.com       TCP      1151 > http [ACK]
 92 32.000000 dhcp-aus-162-244.cisc dimeola.cisco.com       TCP      1151 > http [ACK]
 93 33.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 94 33.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 95 33.000000 dhcp-aus-162-244.cisc dimeola.cisco.com       TCP      1151 > http [ACK]
```

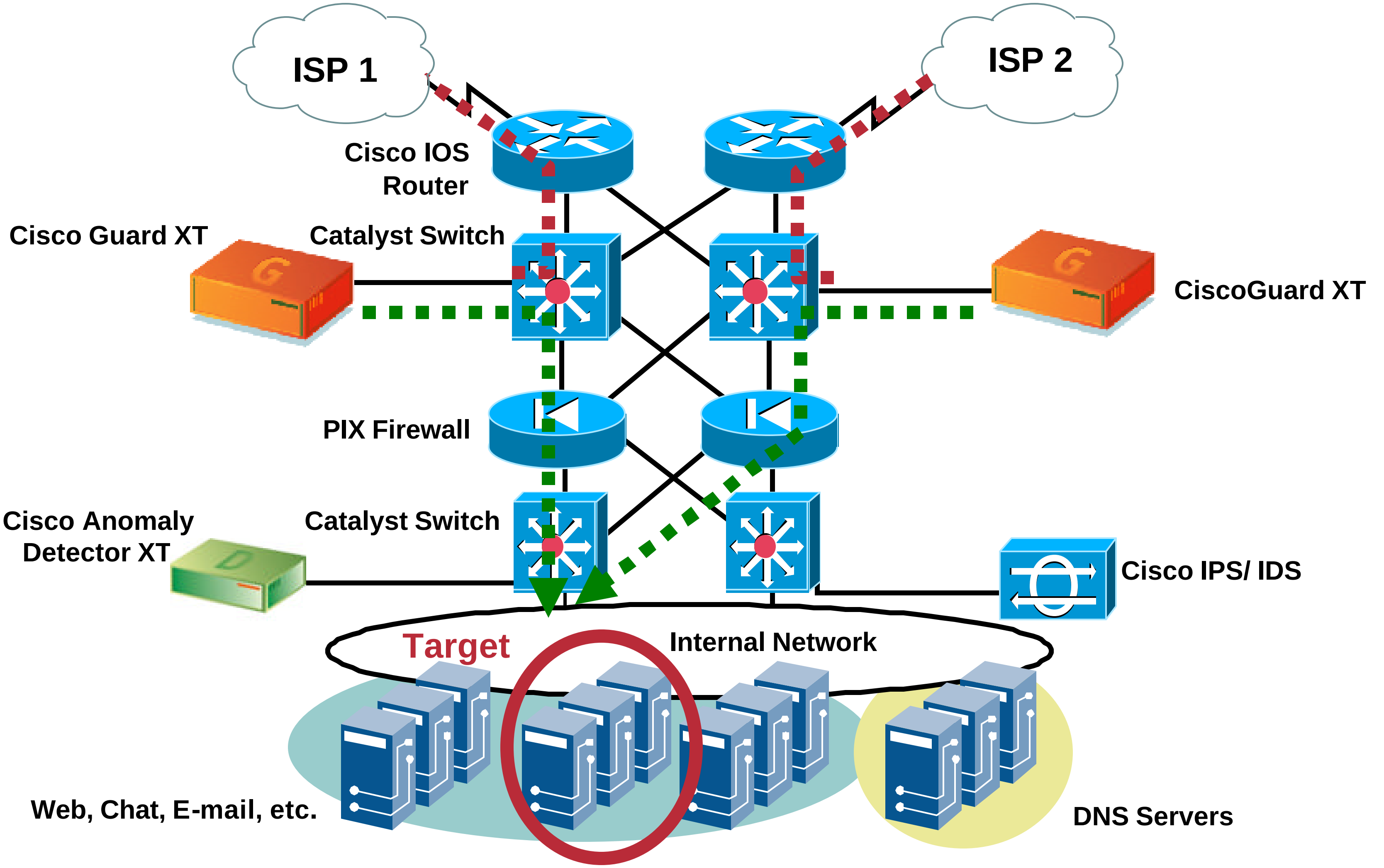
```
⊞ Frame 94 (622 on wire, 622 captured)
⊞ Raw packet data
⊞ Internet Protocol
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 1151 (1151), Seq: 23
    Source port: http (80)
    Destination port: 1151 (1151)
    Sequence number: 2387974169
    Next sequence number: 2387974751
    Acknowledgement number: 1141930
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 8760
    Checksum: 0x2602
```

```
0060  3e 3c 54 52 3e 3c 54 44  3e 20 55 4e 41 53 53 49   ><TR><TD > UNASSI
0070  47 4e 45 44 20 20 3c 2f  54 44 3e 0a 3c 54 44 3e   GNED  </ TD>.<TD>
0080  20 53 4e 4d 50 20 48 69  64 64 65 6e 20 43 6f 6d    SNMP Hi dden Com
0090  6d 75 6e 69 74 79 20 53  74 72 69 6e 67 20 20 3c   munity S tring  <
00a0  2f 54 44 3e 0a 3c 54 44  3e 3c 41 20 48 52 45 46   /TD>.<TD ><A HREF
00b0  3d 22 65 64 69 74 53 69  67 49 6e 73 70 65 63 74   ="editSi gInspect
00c0  69 6f 6e 2e 63 67 69 3f  73 69 67 5f 69 64 3d 34   ion.cgi? sig_id=4
00d0  32 30 30 22 3e 20 34 32  30 30 20 3c 2f 54 44 3e   200"> 42 00 </TD>
00e0  3c 2f 41 3e 0a 3c 2f 54  52 3e 3c 54 52 3e 3c 54   </A>.</T R><TR><T
00f0  44 3e 20 55 4e 41 53 53  49 47 4e 45 44 20 20 3c   D> UNASS IGNED  <
0100  2f 54 44 3e 0a 3c 54 44  3e 20 42 49 4e 44 20 73   /TD>.<TD > BIND s
0110  6f 5f 6c 69 6e 67 65 72  20 65 78 70 6c 6f 69 74   o_linger  exploit
```

Filter: 44) and (tcp.port eq 80 and tcp.port eq 1151)

Internet Protocol (ip)

# DoS/DDoS Attack Mitigation



# High Availability for IPS

Deploying an IPS sensor into the traffic stream introduces a new device to possibly fail and prevent traffic from flowing (It will be the first thing blamed for any problems).

High Availability is defined as building into the network, the ability to cope with the loss of a component of that network to ensure that network functionality is preserved

Solutions:

•Failopen techniques: Hardware or software that functions to detect problems and pass packets through the device without inspection when required

•Failover: One or more paths through the network to allow packets, in the event of a device failure, to either go through a backup IPS sensor or through a plain wire

•Load Balancing: Using devices or software features to split a traffic load up across multiple devices. This can achieve both higher data rates and redundant paths in case of failure

# IPS Fail-open

## IPS Fail-open Mechanisms

**Hardware based fail-open functions by closing a circuit when either power is removed, a link fails, or potentially when triggered by software.**

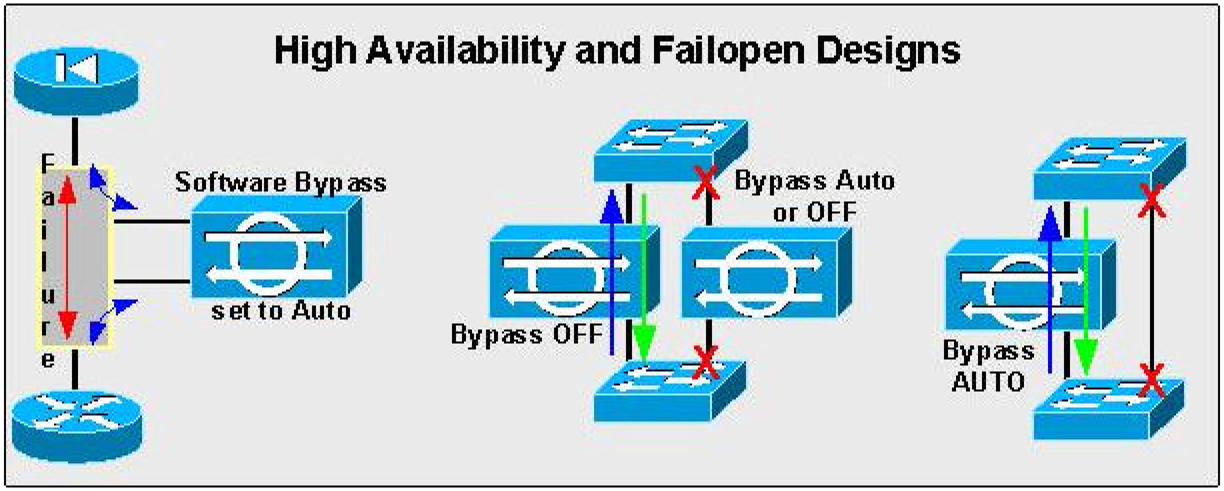
**Software based fail-open functions by building some software feature to pass packets when a failure is detected or packets are not flowing normally for any reason.**

**→ Best case is reliance on Fail-open strategies leaves you with no protection and, at worst, can bring down your entire network ←**

# Fail-open and Failover Deployments

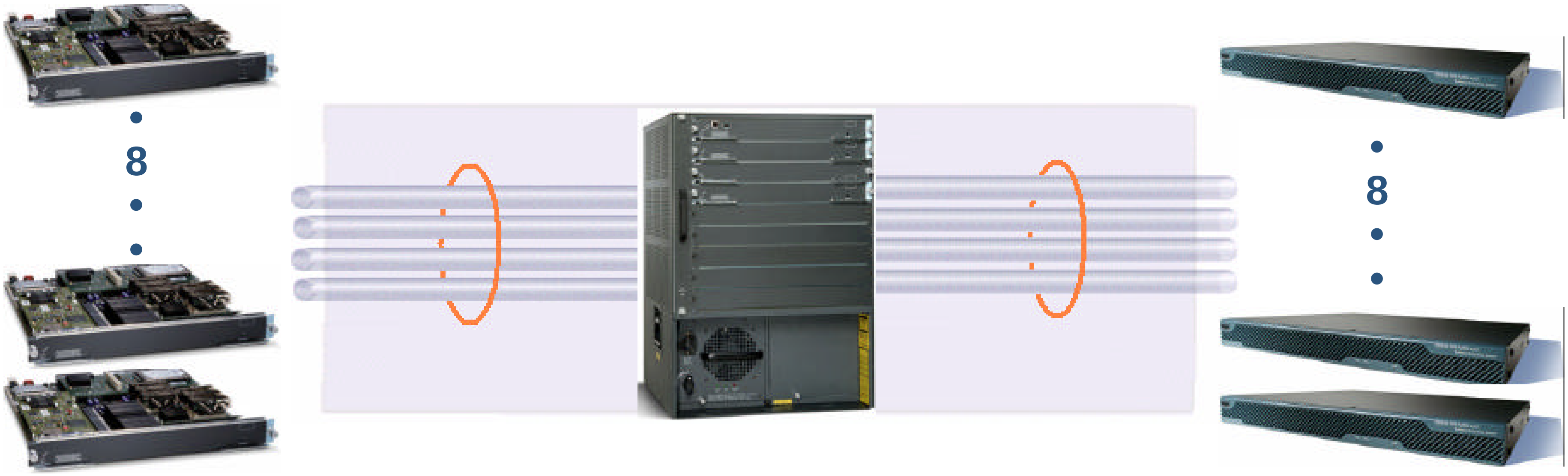
## IPS Appliance Sensor Solutions:

- Standalone Sensor in Hardware Bypass Deployment
- Redundant Deployment using Spanning Tree for Active/Passive Failover
- Redundant Deployment using Spanning Tree for High Availability (along with plain wire)



# EtherChannel Load Balancing

- that dynamically reconfigures the cluster on a HW or SW failure
- Allows up to 8 sensors deployed inspecting the same data set
- Relies on Etherchannel algorithm to split flows amongst the different blades



# Agenda

- Intrusion Prevention Systems (IPS)
- IPS Architecture
- Attack Classification Algorithms / Evasion Techniques
- Contextual Analysis and Alarm Correlation
- Day in the Life of a Packet
- Deploying Network Sensors
- Management Considerations

# Management Paradigms

## Device-Level Management

- Small deployments

  1–5 sensors

- Low alarm rates

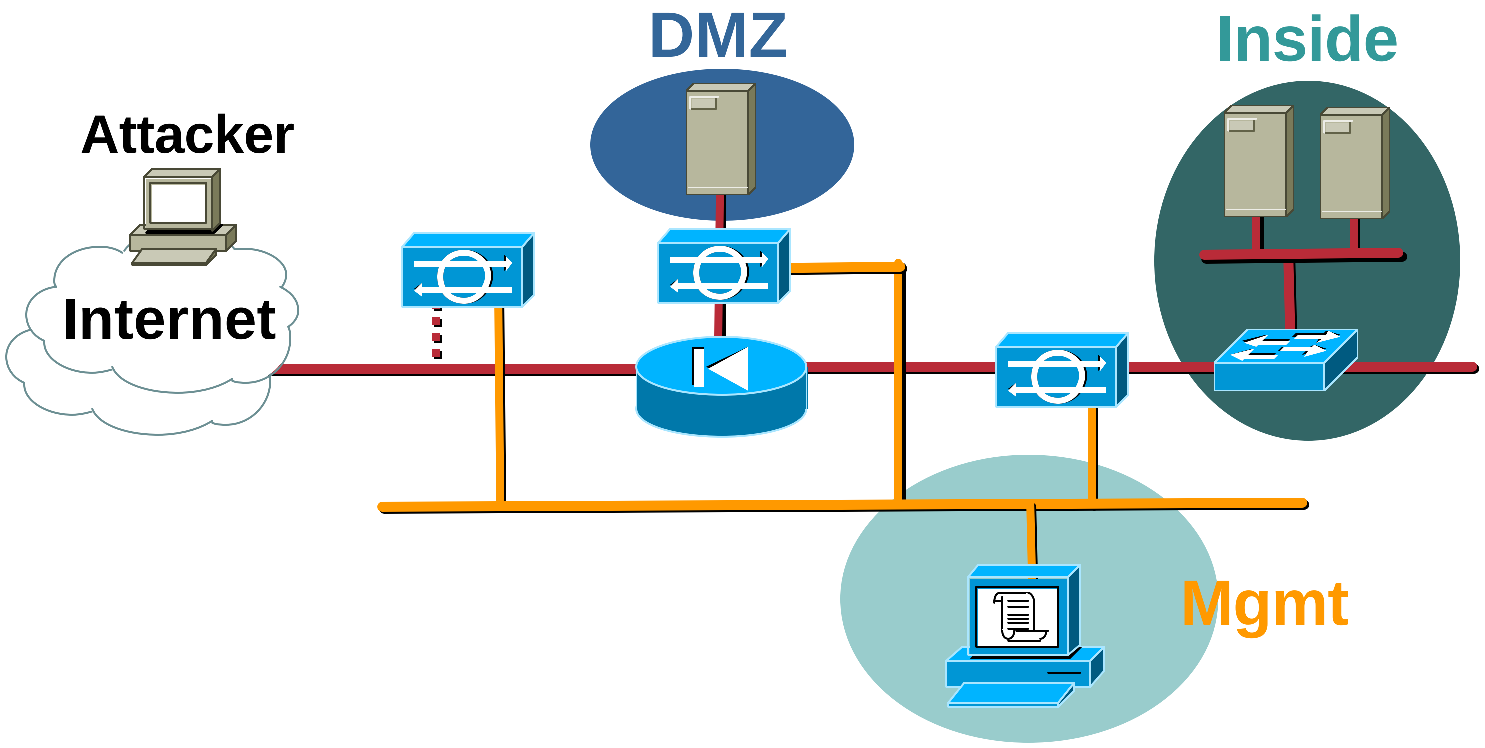
## Multi-Device Management

- Medium/large deployments

  Many sensors

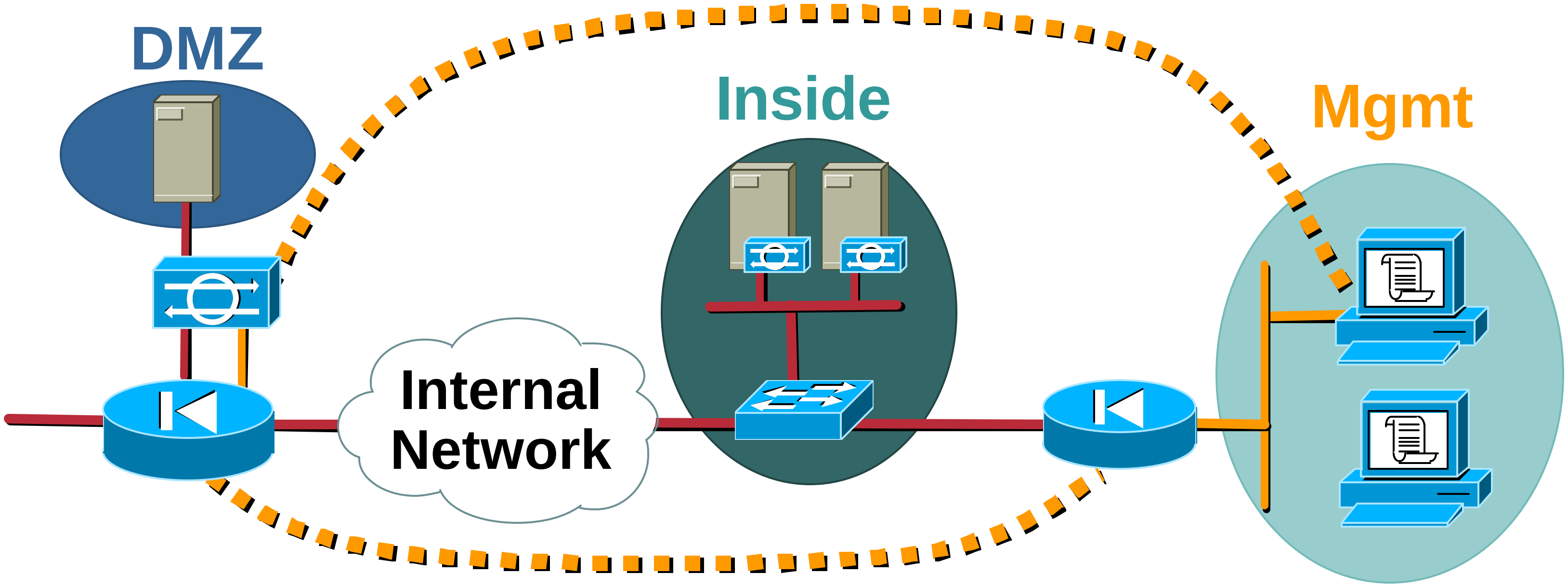
- High alarm rates

# Secure Management Guidelines: Out of Band Management



- Monitoring and Management Network Segment
- A conceptual air gap between IPS and Management segment provides the most security

# In-Band Management Through Tunnels



- **Firewall brokers** **connection from inside to Management Segment**
- **Encrypted tunnels** **terminated at firewall or at Management Station**

# Security Logging

| | Events/Sec | MB/Hr |
|---|---|---|
| Small VPN Gateway | 50 | 27.4 |
| Entry Firewall | 100 | 54.8 |
| High Router | 200 | 109.6 |
| Mid IPS | 400 | 219.2 |

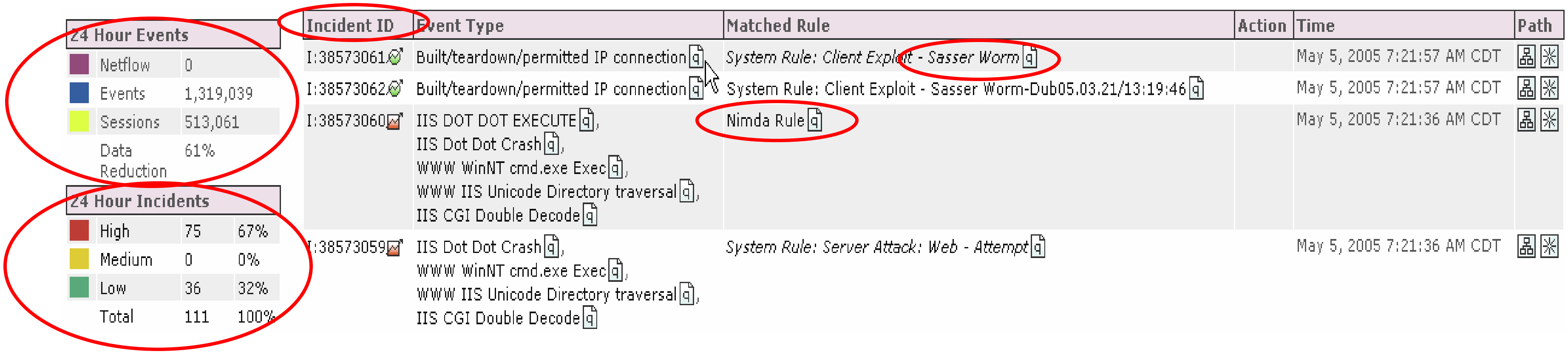
## What are the strategies:

- I don’t need it, so I don’t log it
- I don’t look at it, but still log it, if I need it in the future
- I log only what I am interested in
- I am logging for legal reasons

Too Many Devices, Too Much Data...
All to Find a Needle in a Haystack

# Correlation

- Statistical – Summarization or anomaly based
- Rules Based – Finite state machine
- Vulnerability – Automatic verification
- Session Based – Automatic investigation



| 24 Hour Events | | |
|---|---|---|
| 🟪 | Netflow | 0 |
| 🟦 | Events | 1,319,039 |
| 🟨 | Sessions | 513,061 |
| | Data Reduction | 61% |

| 24 Hour Incidents | | | |
|---|---|---|---|
| 🟥 | High | 75 | 67% |
| 🟨 | Medium | 0 | 0% |
| 🟩 | Low | 36 | 32% |
| | Total | 111 | 100% |

| Incident ID | Event Type | Matched Rule | Action | Time | Path |
|---|---|---|---|---|---|
| I:38573061 | Built/teardown/permitted IP connection | *System Rule: Client Exploit - Sasser Worm* | | May 5, 2005 7:21:57 AM CDT | ⊞ ✳ |
| I:38573062 | Built/teardown/permitted IP connection | System Rule: Client Exploit - Sasser Worm-Dub05.03.21/13:19:46 | | May 5, 2005 7:21:57 AM CDT | ⊞ ✳ |
| I:38573060 | IIS DOT DOT EXECUTE,<br>IIS Dot Dot Crash,<br>WWW WinNT cmd.exe Exec,<br>WWW IIS Unicode Directory traversal,<br>IIS CGI Double Decode | Nimda Rule | | May 5, 2005 7:21:36 AM CDT | ⊞ ✳ |
| I:38573059 | IIS Dot Dot Crash,<br>WWW WinNT cmd.exe Exec,<br>WWW IIS Unicode Directory traversal,<br>IIS CGI Double Decode | *System Rule: Server Attack: Web - Attempt* | | May 5, 2005 7:21:36 AM CDT | ⊞ ✳ |

# Mitigation

- Layer 2

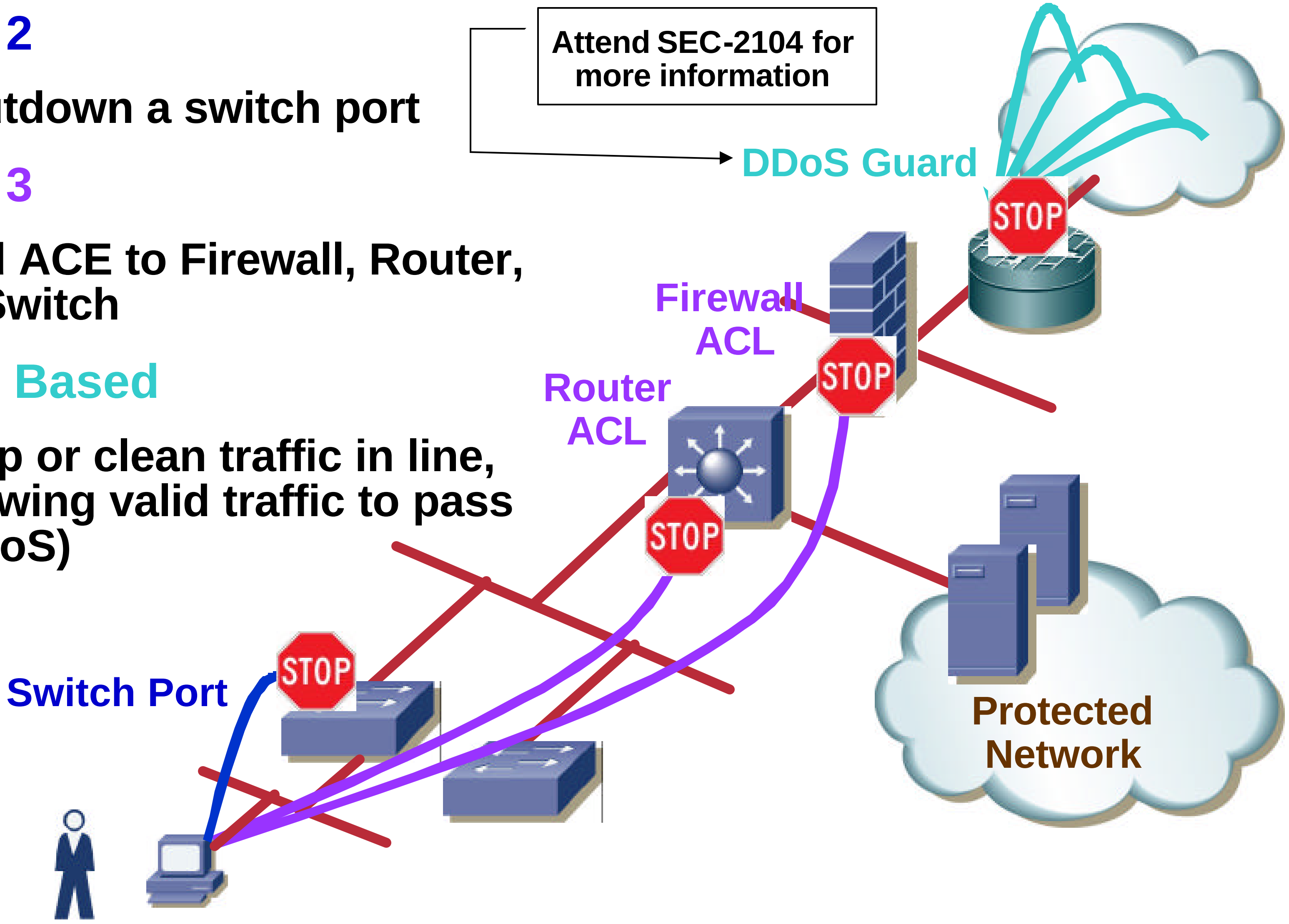
  Shutdown a switch port

- Layer 3

  Add ACE to Firewall, Router, or Switch

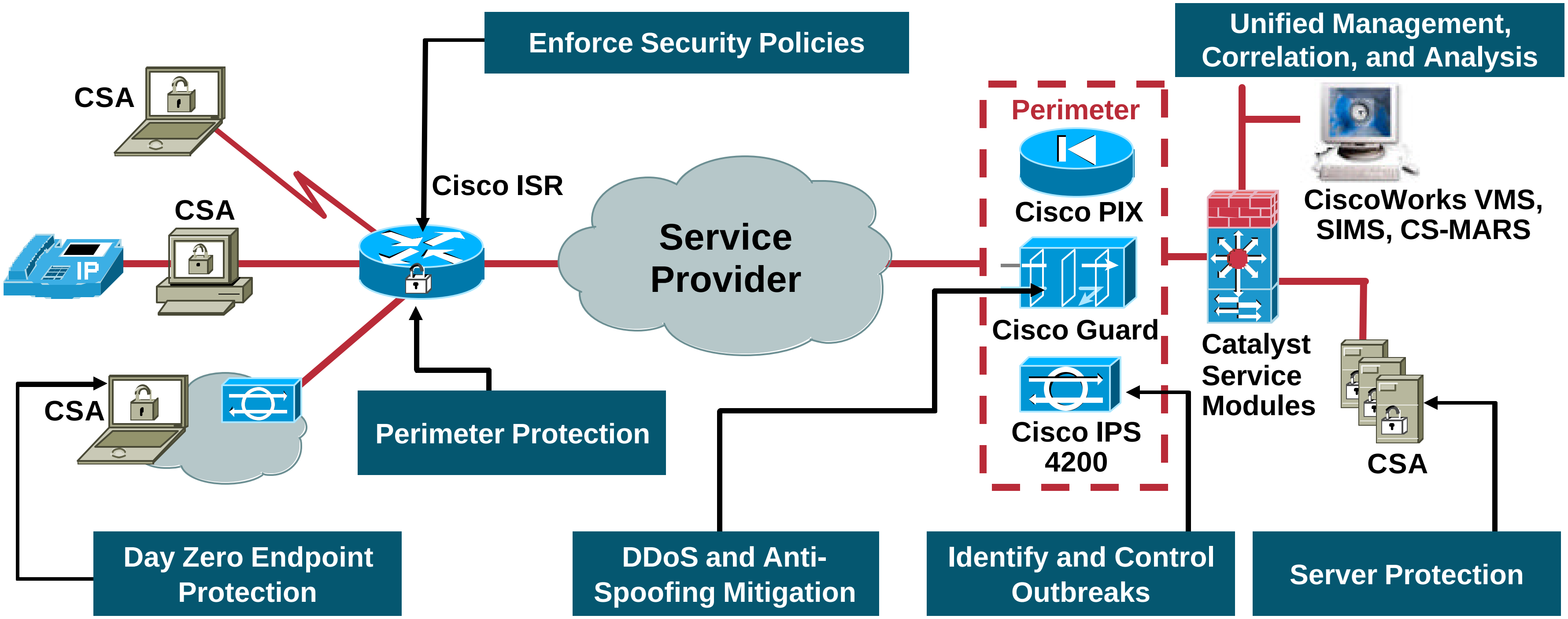
- Route Based

  Drop or clean traffic in line, allowing valid traffic to pass (DDoS)



# Cisco’s Intrusion Prevention Solution
## Summary

**A complete end-to-end prevention solution is required to deliver a defense in depth approach to attack  mitigation**


Enforce Security Policies
Unified Management, Correlation, and Analysis
CSA
CSA
CSA
Cisco ISR
Service Provider
Perimeter
Cisco PIX
Cisco Guard
Cisco IPS 4200
CiscoWorks VMS, SIMS, CS-MARS
Catalyst Service Modules
CSA
IP
Perimeter Protection
Day Zero Endpoint Protection
DDoS and Anti-Spoofing Mitigation
Identify and Control Outbreaks
Server Protection

**www.cisco/com/go/ips**

# Complete Your Online Session Evaluation!

**Por favor, complete el formulario de evaluación.**

**Muchas gracias.**

**Session ID: SEC-2030**

**Deploying IPS Solutions**