ALEF NULA

DŮVĚŘUJTE SILNÝM

Útoky/síťová bezpečnost

Martin Biško

ALEF NULA, a.s. – Cisco Gold Partner

www.alefnula.com

ALEF NULA

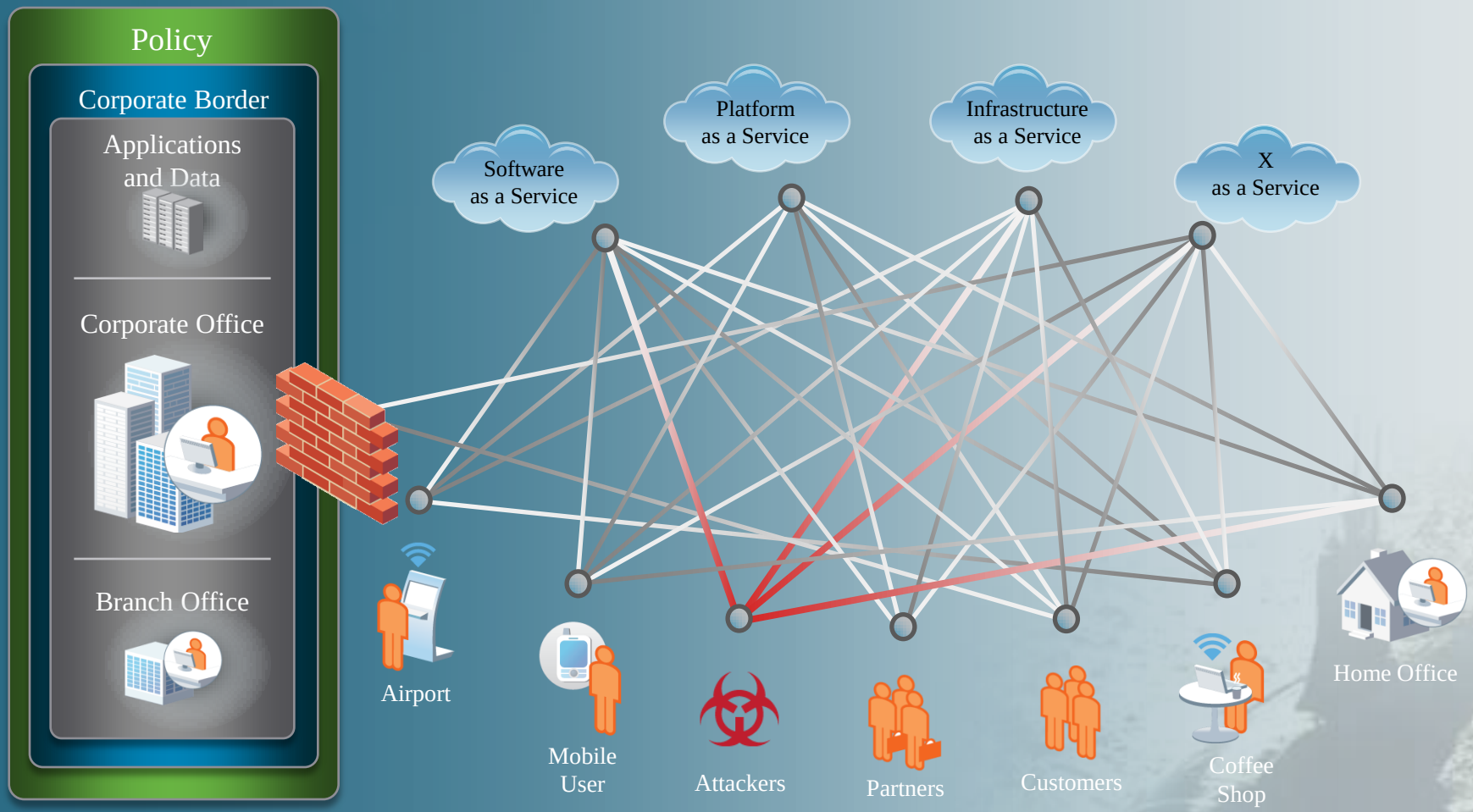
DŮVĚŘUJTE SILNÝM

Cisco Self-Defending Networks

Cisco Self-Defending Network

ALEF NULA
DŮVĚŘUJTE SILNÝM

Customers Want Business Without Borders



HTTP Is the New TCP

ALEF NULA
DŮVĚŘUJTE SILNÝM

Understanding Web Traffic

Cisco Global Correlation

SensorBase: World's Largest Traffic Monitoring Network

ALEF NULA
DŮVĚŘUJTE SILNÝM

LARGEST FOOTPRINT | GREATEST BREADTH | FULL CONTEXT ANALYSIS

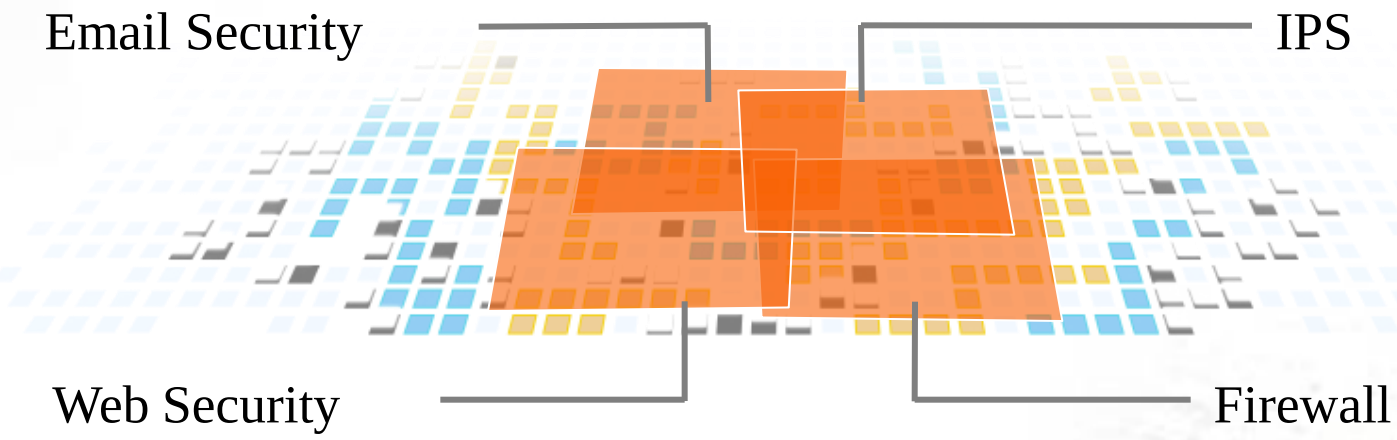
Cisco SensorBase

- 700,000+ sensors deployed globally
- 8 of the top 10 global ISPs
- Over 500GB of data per day
- 500 third party feeds
- Over 30% of the world's email traffic

Cisco Global Correlation
Unmatched Breadth

ALEF NULA
DŮVĚŘUJTE SILNÝM

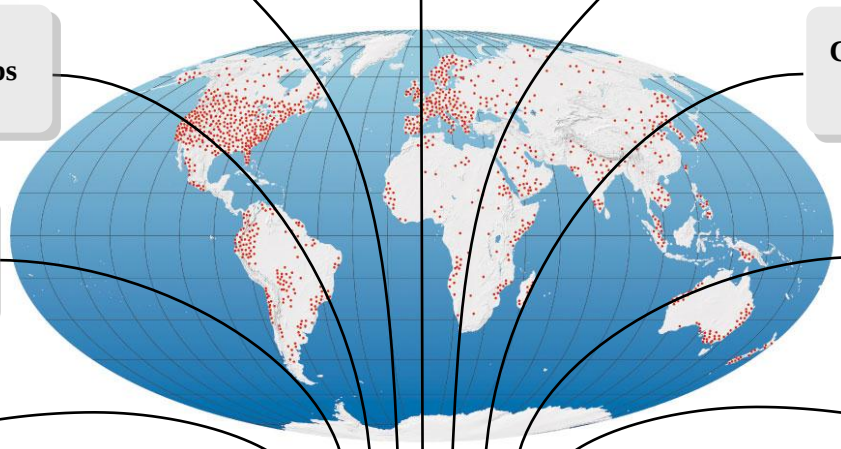
LARGEST FOOTPRINT | **GREATEST BREADTH** | FULL CONTEXT ANALYSIS



Identifying a global botnet requires complete visibility across all threat vectors

SenderBase

Breadth and Quality of Data Makes the Difference



SpamCop, SpamHaus (SBL), NJABL, Bonded Sender

IP Blacklists & Whitelists

Spam, phishing, virus reports

Complaint Reports

Domain Blacklist & Safelists

Spamvertized URLs, phishing URLs, spyware sites

SpamCop, ISPs, customer contributions

Spam Traps

Compromised Host Lists

SORBS, OPM, DSBL

Message size, attachment volume, attachment types, URLs, host names

Message Composition Data

Web Site Composition Data

Downloaded files, linking URLs, threat heuristics

Global Volume Data

Over 100,000 organizations, email traffic, web traffic

Other Data

Fortune 1000, length of sending history, location, where the domain is hosted, how long has it been registered, how long has the site been up

SenderBase

http://www.senderbase.org

ALEF NULA
DŮVĚŘUJTE SILNÝM

cisco | IronPort Email and Web Security

Blocked? | Help | Contac

HOME | THREAT OVERVIEW | TOP SENDERS | REPUTATION LOOK UP | HELP | ABOUT

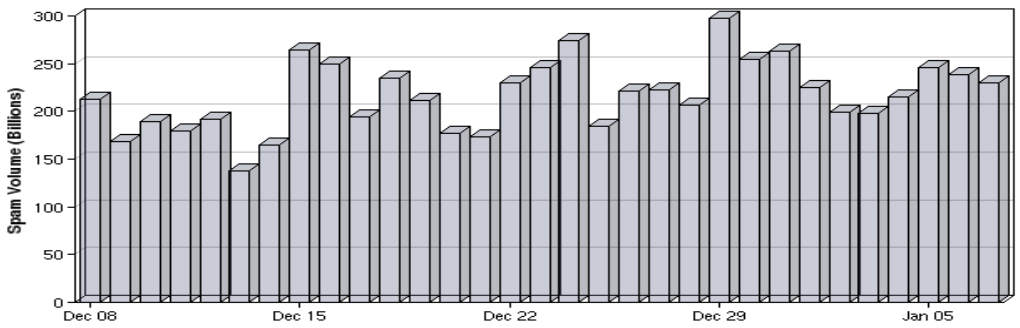
Cisco IronPort SenderBase Security Network

Since its inception, the IronPort Threat Operations Center has been tracking worldwide spam volume. Changes in spam volume can be attributed to numerous factors including the variety of methods used by spammers and capture rates due to the ability (or inability) of anti-spam solutions to keep up with rapidly changing techniques.

The graph below expresses the number of spam messages over a specified amount of time. The table contains additional vectors to help show how spam relates to global email volume and its own average statistics.

DISPLAYED Last Month OPTIONS: Print Export

GLOBAL SPAM VOLUME



Date	Spam Volume (Billions)	% of Global Email Volume	Spam Volume Change
2010 Jan 07	230.2	85.9%	-3% ↓
2010 Jan 06	238.3	86.9%	-3% ↓
2010 Jan 05	246.1	87.4%	15% ↑
2010 Jan 04	214.8	87.0%	8% ↑

Look up your network:

Look Up

Reputation Look Up

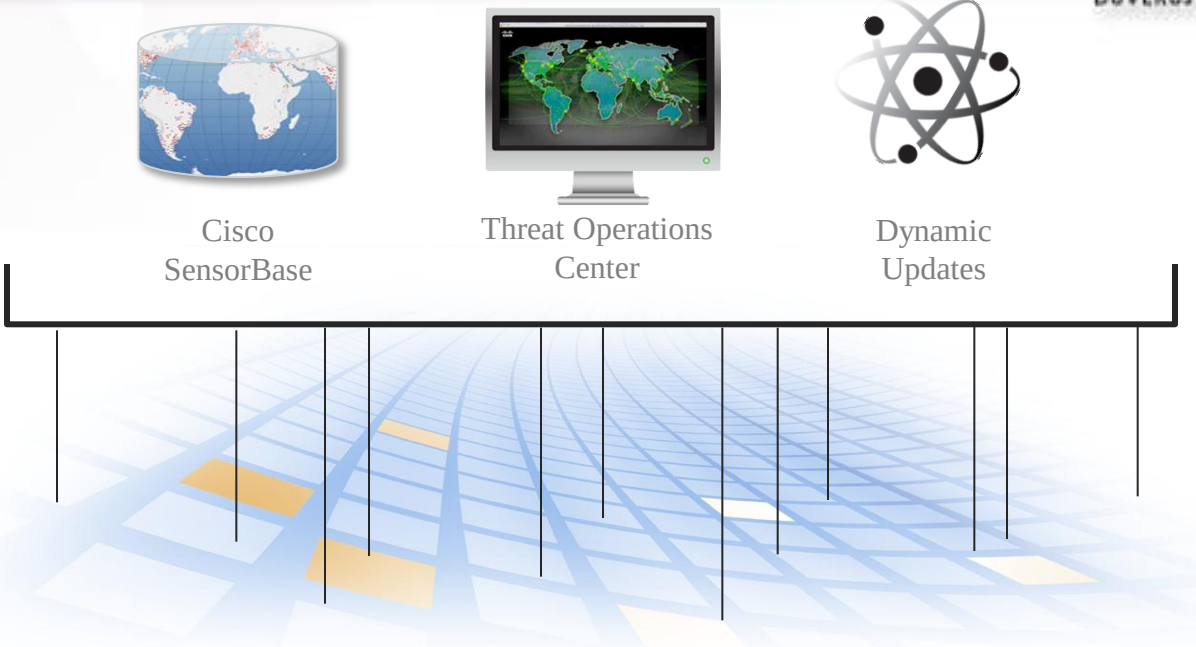
QUICK LINKS

+ Blocked?

EXTERNAL LINKS

+ Threat Operations Center
+ Web Reputation
+ Email Reputation

Cisco Security Intelligence Operations



Security Infrastructure That Dynamically Protect Against the Latest Threats Through:

Cisco SensorBase

The Most Comprehensive Vulnerability and Sender Reputation Database

Threat Operations Center

A Global Team of Security Researchers, Analysts, and Signature Developers

Dynamic Updates

Dynamic Updates and Actionable Intelligence

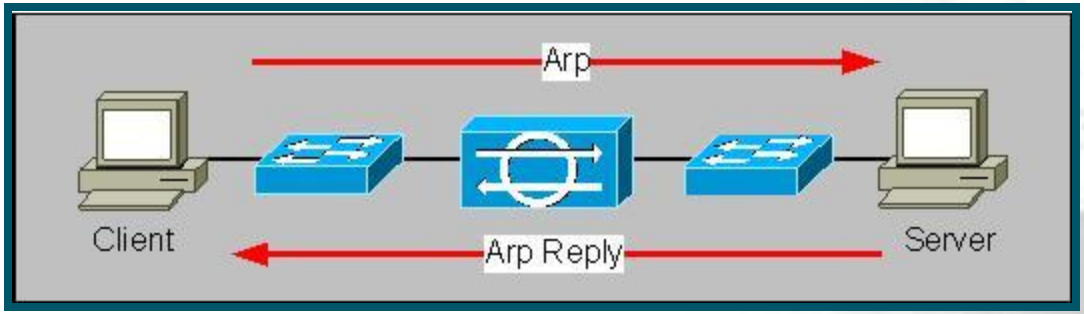
ALEF NULA

DŮVĚŘUJTE SILNÝM

Intrusion Prevention Solutions

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



IDS vs. IPS
Network-Based IDS—The Sensor

ALEF NULA
DŮVĚŘUJTE SILNÝM

- 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

ALEF NULA
DŮVĚŘUJTE SILNÝM

- 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

Types of IDS/IPS Systems

ALEF NULA
DŮVĚŘUJTE SILNÝM

Signature based

- e.g. more than 100 ICMP packets/minute

Policy based

- e.g. deny all UDP packets

Anomaly based

- e.g. packet contains invalid protocol options

Network or Host based

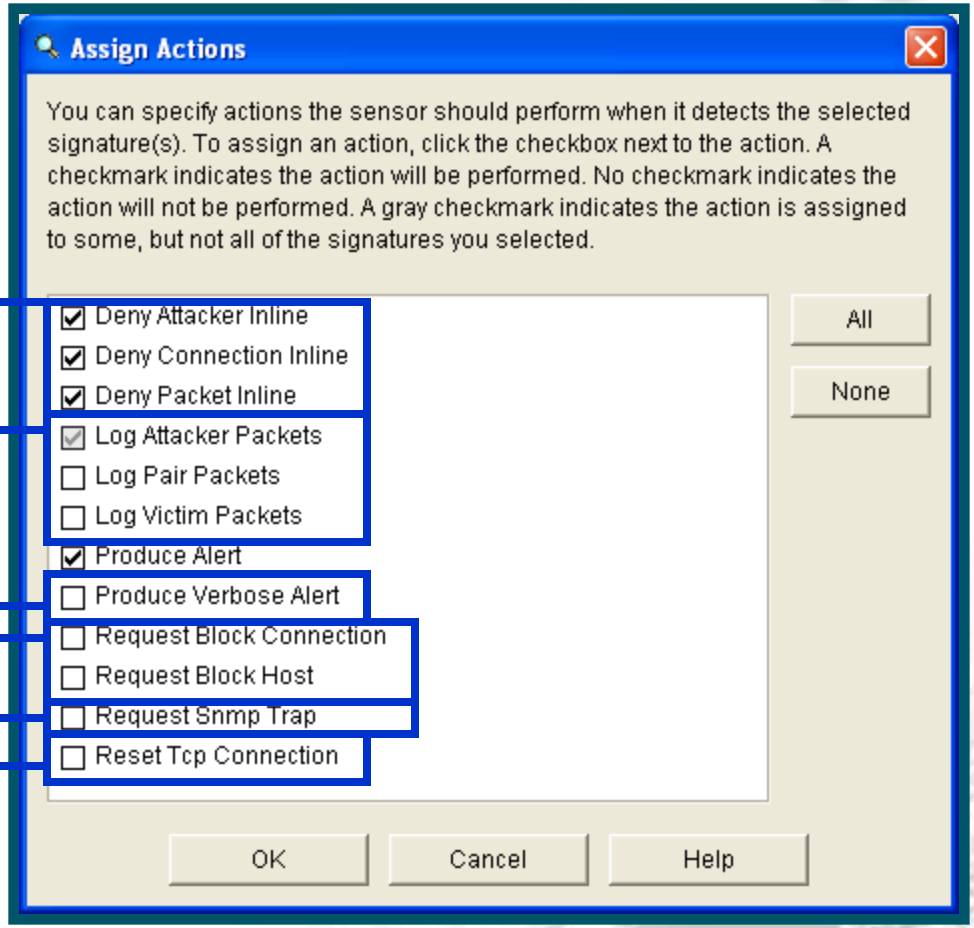
- HIDS/NIDS and HIPS/NIPS

Cisco IPS Software v6.x

Expanded Mitigation Actions to STOP Attacks

ALEF NULA
DŮVĚŘUJTE SILNÝM

- 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

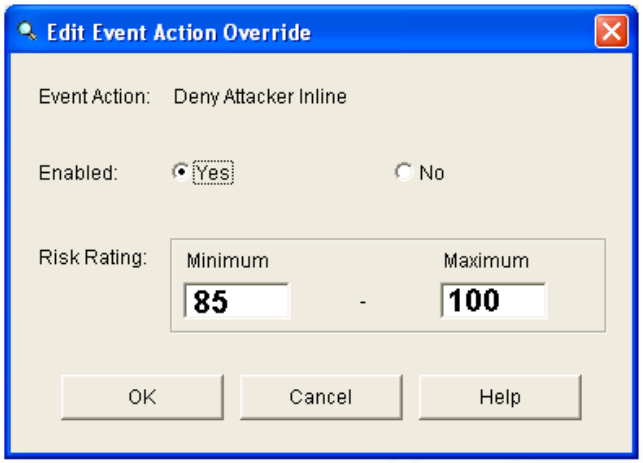


Cisco IPS Overview:
Risk-Management-based Security Policy

ALEF NULA
DŮVĚŘUJTE SILNÝM

Threat Rating

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

Customizable Risk Rating Thresholds :

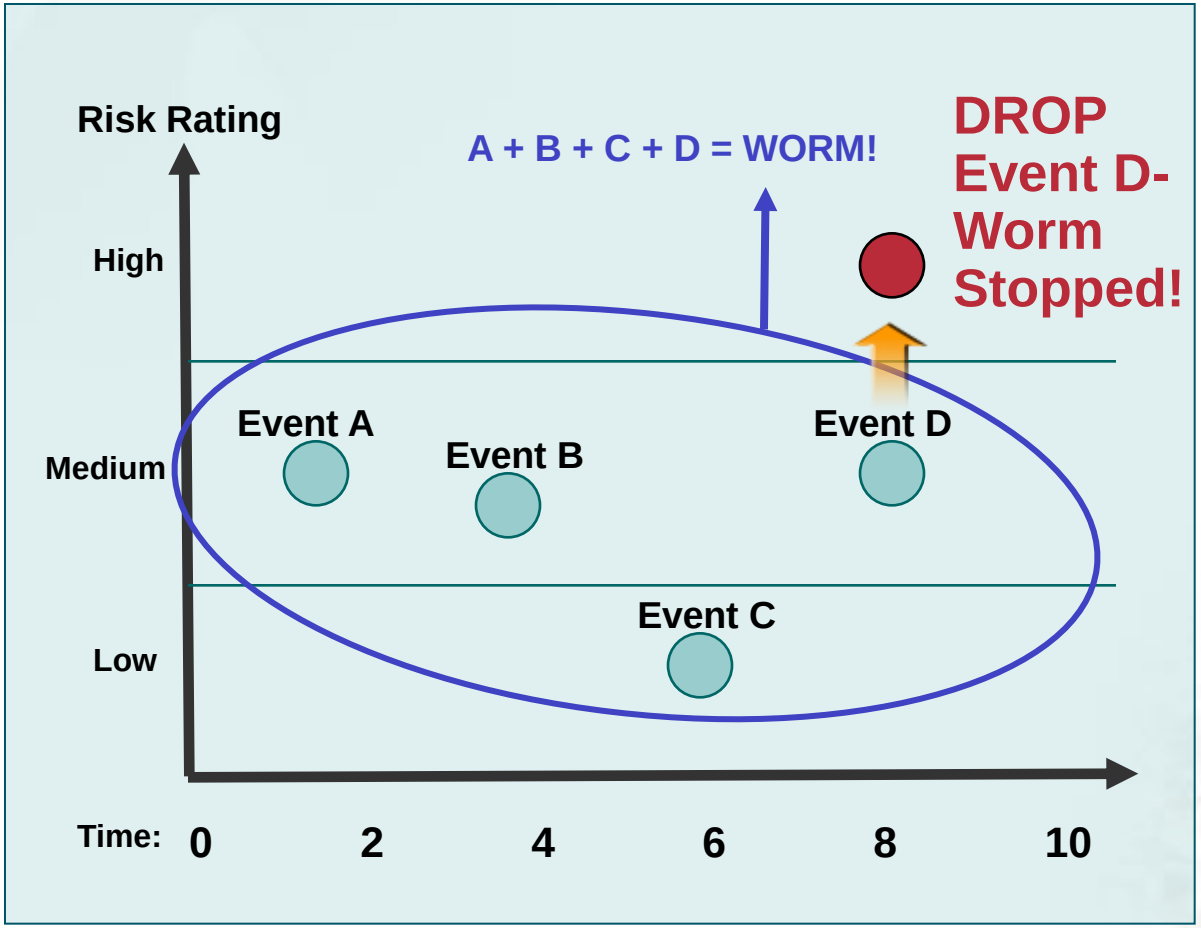
0 < RR < 35	Alarm
35 < RR < 85	Alarm & Log Packets
85 < RR < 100	Drop Packet

Result: Calibrated Risk Rating enables scalable management of sophisticated threat prevention technologies

Accurate Prevention Technologies

Meta Event Generator Delivers Advanced Correlation

On-box correlation allows adaptation to new threats in real-time without user intervention

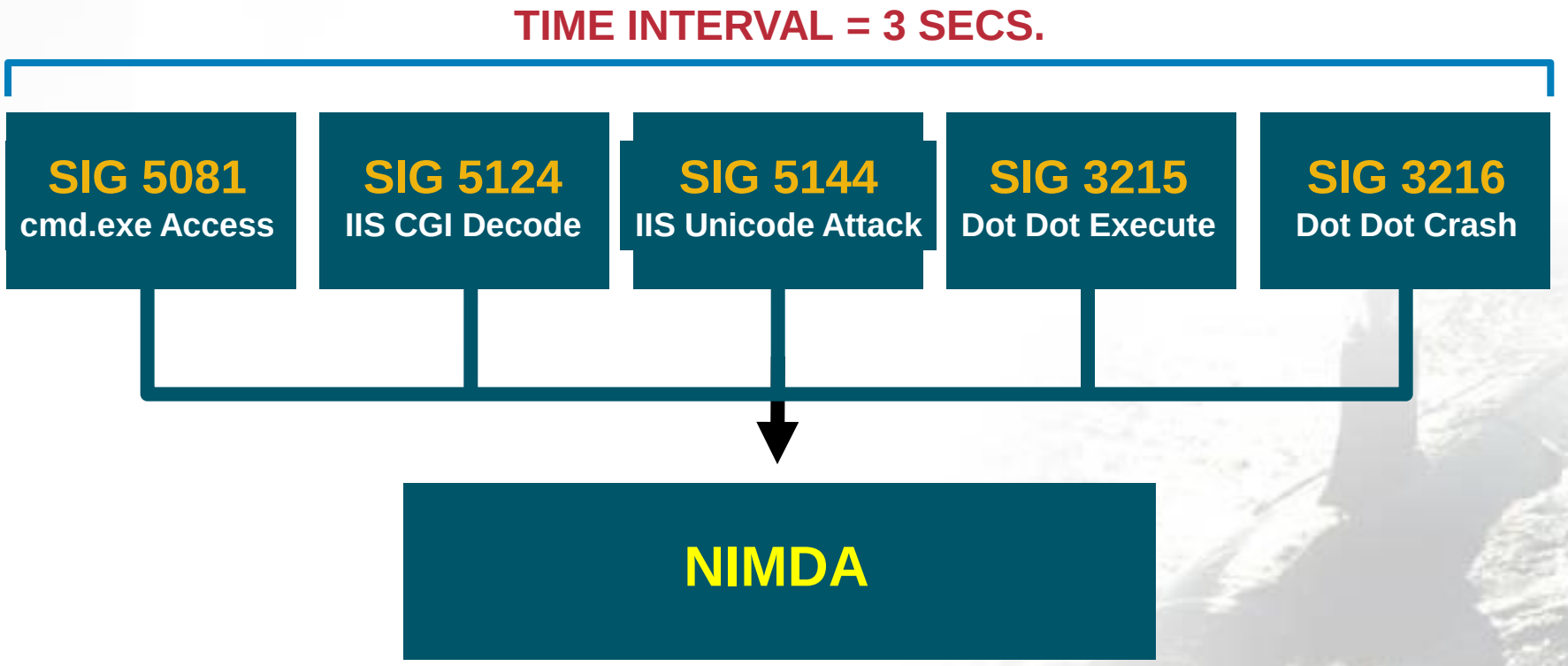


- Links lower risk events into a high risk meta-event, triggering prevention actions
- Models attack Behavior by Correlating:
  - Event type
  - Time span

Process for Accurate Threat Mitigation:
Integrated Event Correlation

ALEF NULA
DŮVĚŘUJTE SILNÝM

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

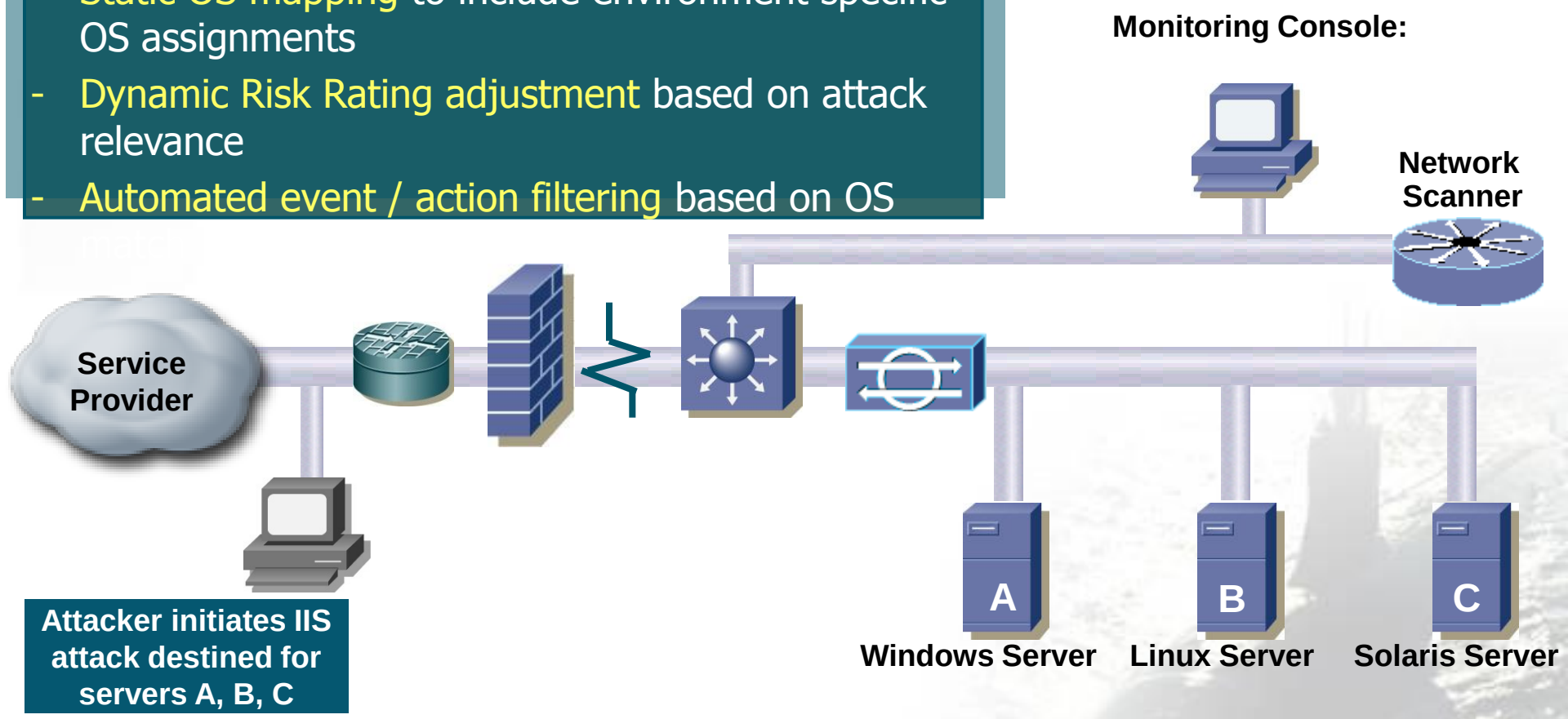


IPS

CTR & Network Scanner Integration

ALEF NULA
DŮVĚŘUJTE SILNÝM

- Visibility into endpoint context through passive OS fingerprinting
- Static OS mapping to include environment specific OS assignments
- Dynamic Risk Rating adjustment based on attack relevance
- Automated event / action filtering based on OS



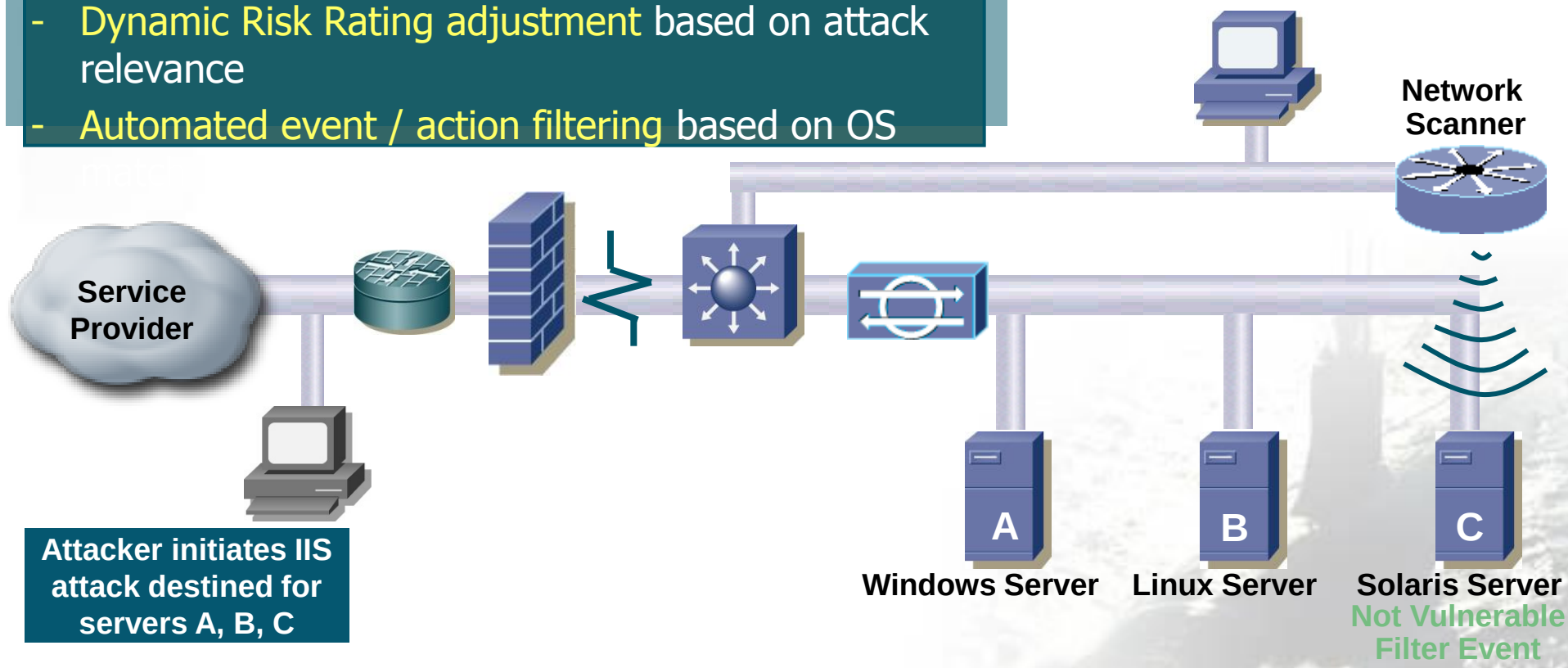
IPS

CTR & Network Scanner Integration

ALEF NULA
DŮVĚŘUJTE SILNÝM

- Visibility into endpoint context through passive OS fingerprinting
- Static OS mapping to include environment specific OS assignments
- Dynamic Risk Rating adjustment based on attack relevance
- Automated event / action filtering based on OS

Active Network Scanning



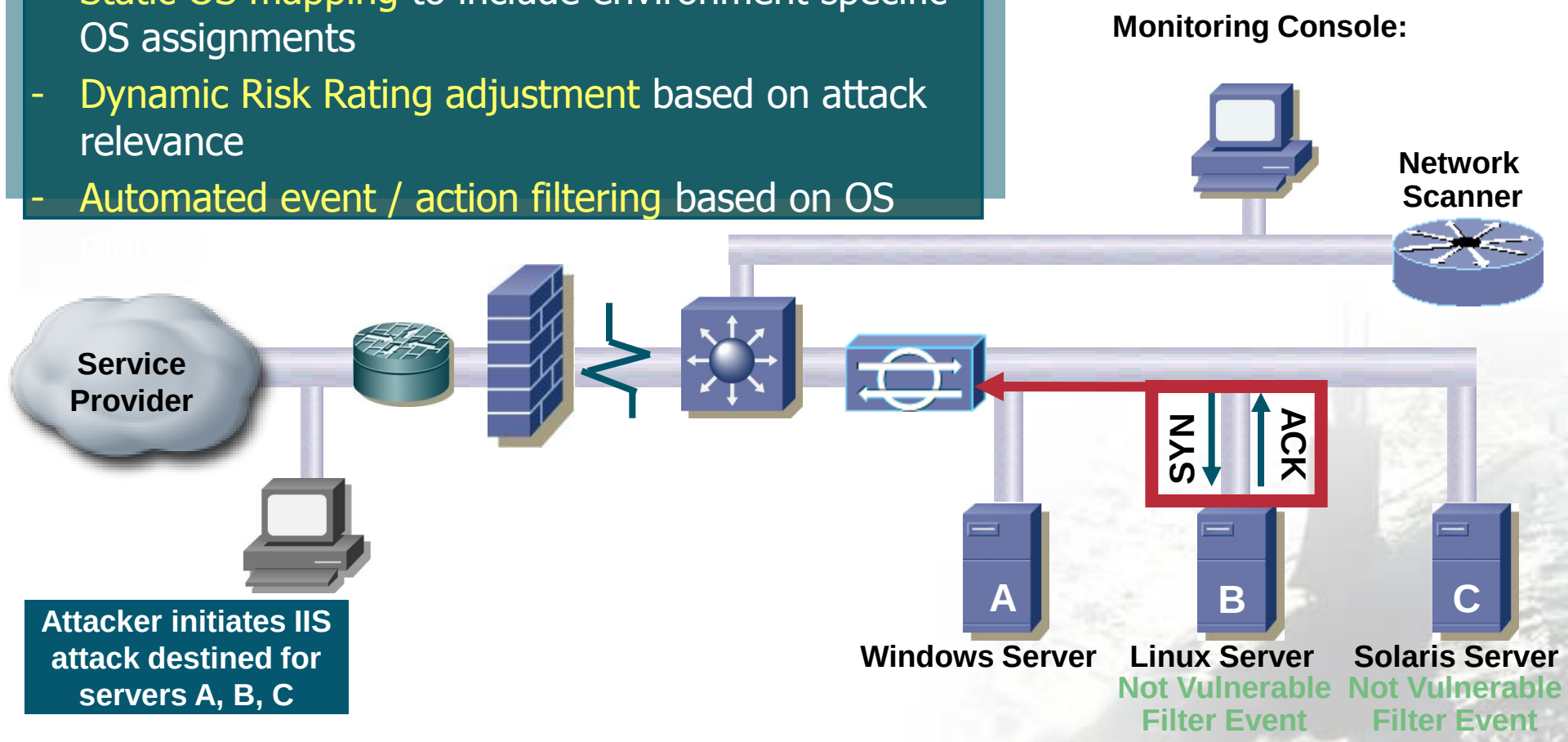
IPS

CTR & Network Scanner Integration

ALEF NULA
DŮVĚŘUJTE SILNÝM

- Visibility into endpoint context through passive OS fingerprinting
- Static OS mapping to include environment specific OS assignments
- Dynamic Risk Rating adjustment based on attack relevance
- Automated event / action filtering based on OS

Passive OS Fingerprinting



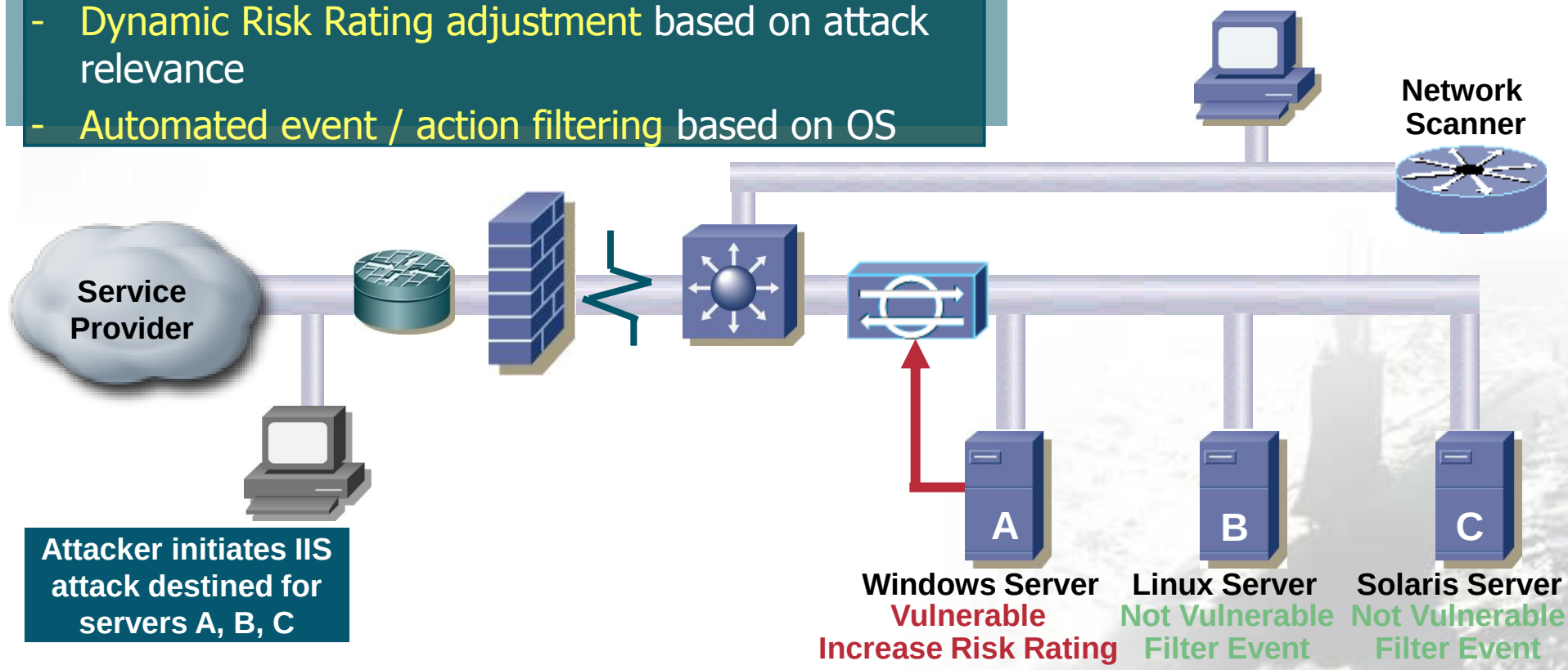
IPS

CTR & Network Scanner Integration

ALEF NULA
DŮVĚŘUJTE SILNÝM

- Visibility into endpoint context through passive OS fingerprinting
- Static OS mapping to include environment specific OS assignments
- Dynamic Risk Rating adjustment based on attack relevance
- Automated event / action filtering based on OS

Static OS Mapping

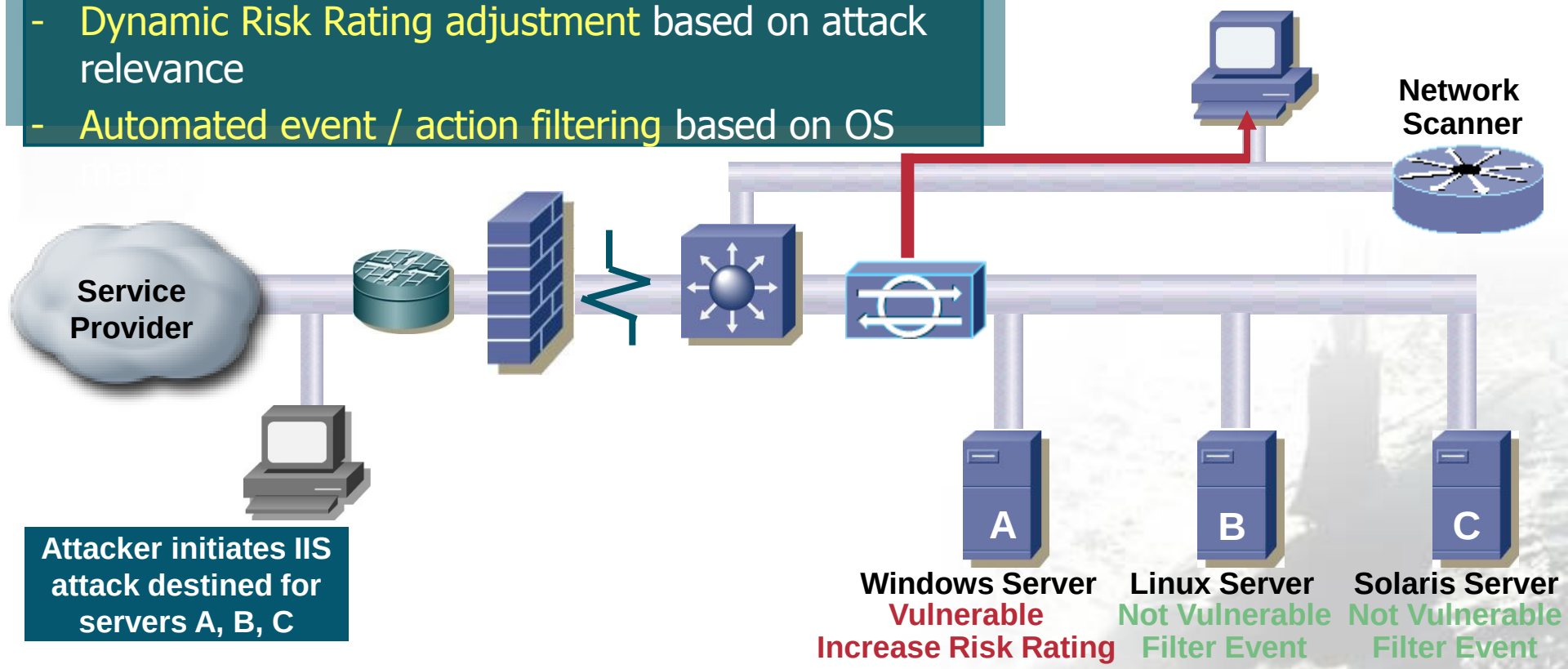


IPS

CTR & Network Scanner Integration

ALEF NULA
DŮVĚŘUJTE SILNÝM

- Visibility into endpoint context through passive OS fingerprinting
- Static OS mapping to include environment specific OS assignments
- Dynamic Risk Rating adjustment based on attack relevance
- Automated event / action filtering based on OS



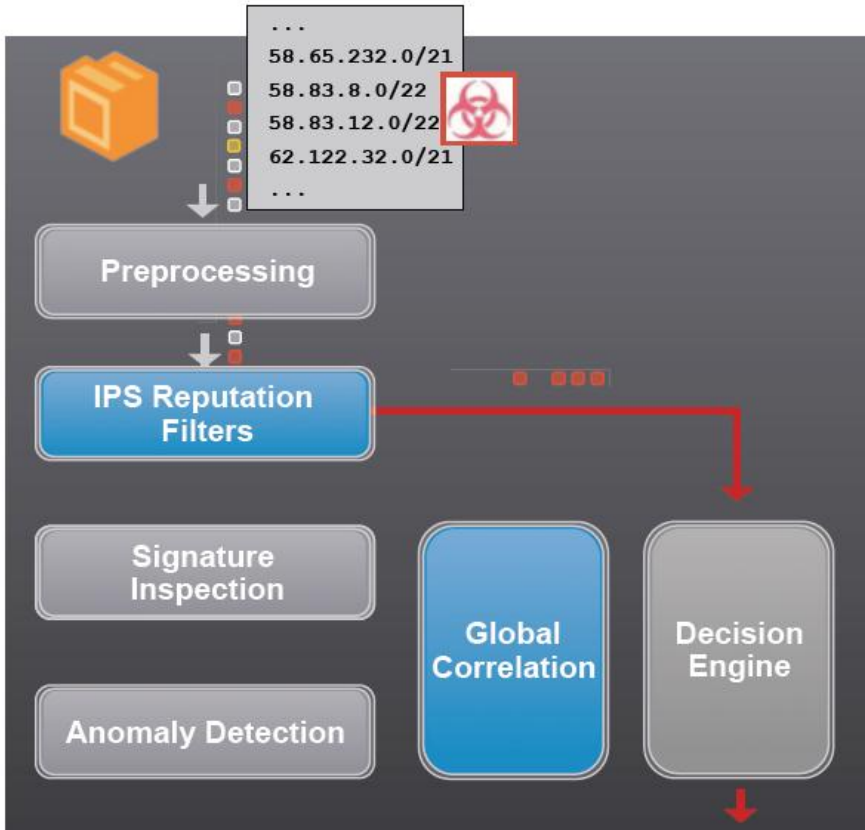
IPS

IPS-CSA Collaboration

ALEF NULA
DŮVĚŘUJTE SILNÝM

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- **Host Quarantining**

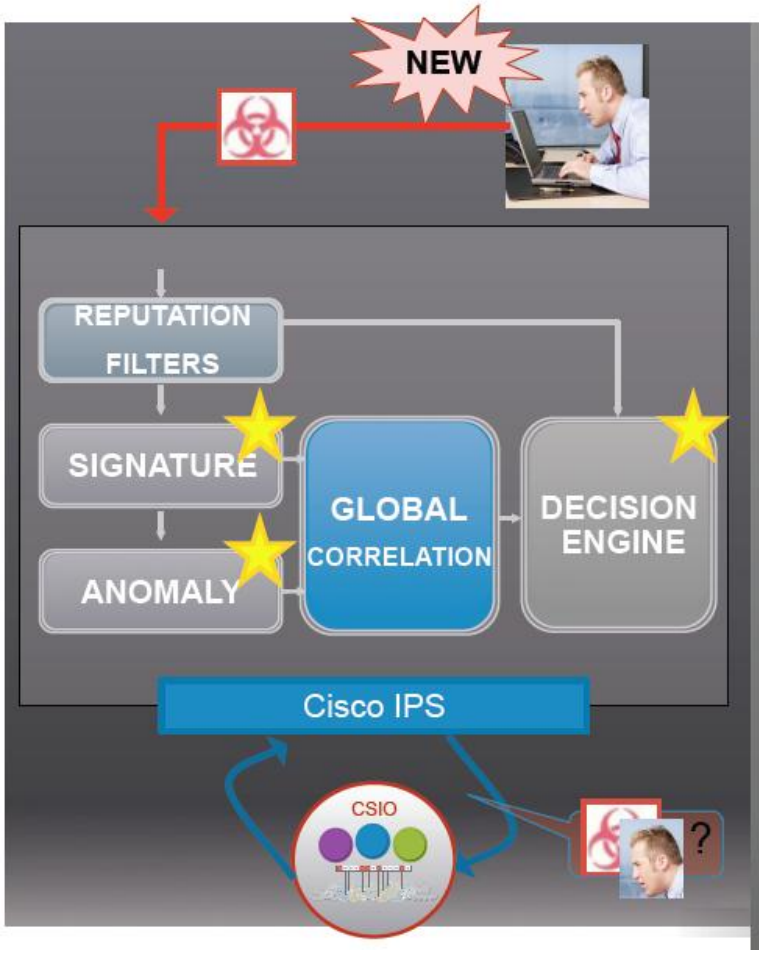
IPS Reputation Filter



- Some networks on the Internet are owned wholly by malicious organizations or are hijacked 'zombie' networks
- Reputation Filters block access to these networks like an ACL
- Individual IP addresses do not go on this list because of things they do (An IP does not go from -1 to -9 to being put on this list)

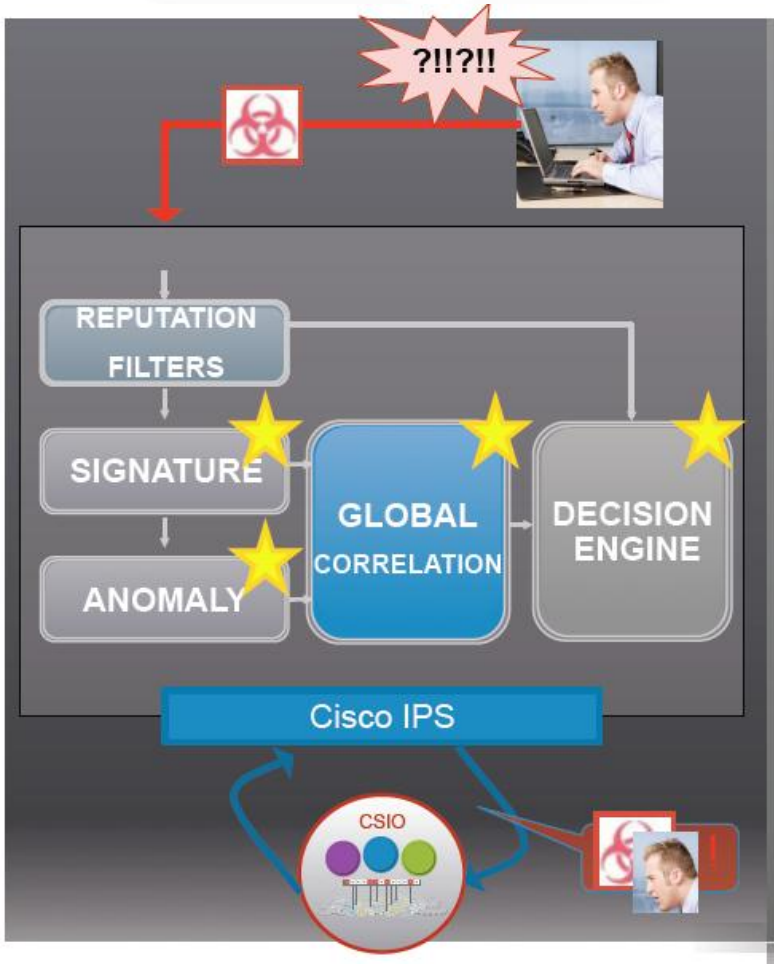
Global Correlation – Unknown attacker

ALEF NULA
DŮVĚŘUJTE SILNÝM



1. New Attacker hits the IPS
2. Attacker without a Reputation
3. Signatures or Anomaly Detection identify activity
4. The attack is handled according to the security policy implemented on the sensor (Deny if Risk Rating reaches threshold)
5. Information on the Attacker is sent back to CSIO to track his reputation (if configured)

Global Correlation – Suspicious attacker



1. Suspicious Attacker attacks
2. Has medium Reputation
3. Signatures identify suspicious activity and give this a medium Risk Rating
4. Global Correlation adds context of Attacker Reputation to Risk Rating
5. Decision Engine blocks
6. Information on NEW Reputation is sent back to CSIO.

ALEF NULA

DŮVĚŘUJTE SILNÝM

Cisco Security Agent

Specific Threats

Targeted at the Endpoint

ALEF NULA
DŮVĚŘUJTE SILNÝM

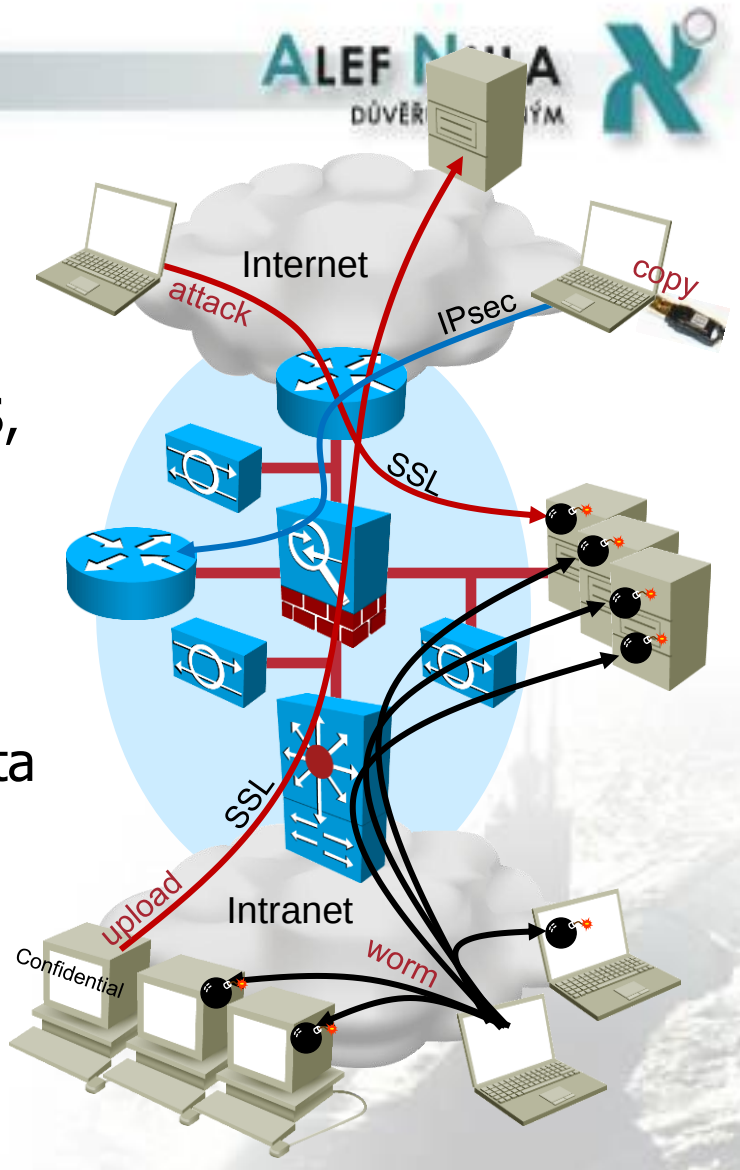
- Common security threats to end devices and data:
  - –Malware (e.g. worms, viruses, trojans, spyware, botnets)
  - –Malicious or careless users and attackers (accidental incidents or targeted attacks)
- Security incidents result in loss of business due to:
  - –Denial of service (loss due to downtime and repair)
  - –Theft or disclosure of sensitive data (financial and reputation loss)
  - –Integrity violation of sensitive data (financial and reputation loss)

Advanced Endpoint Security

Drivers

Challenges facing common security practices:

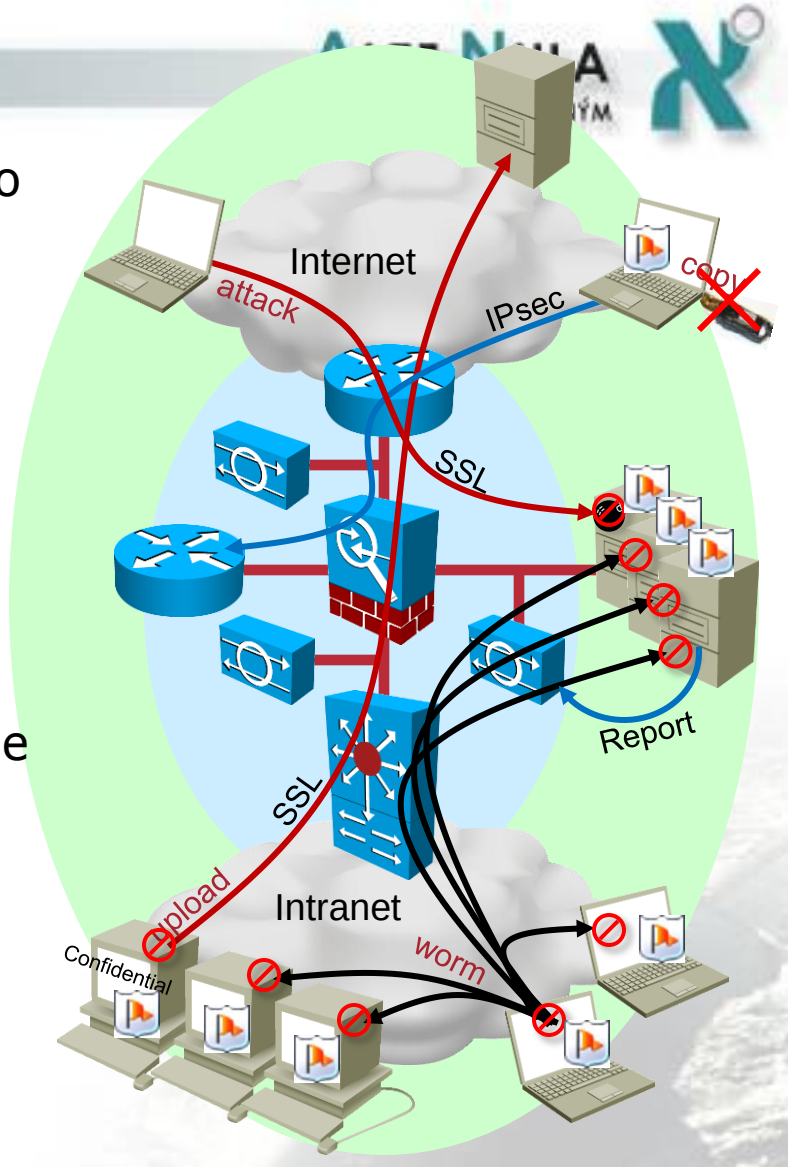
- New attacks that trick users into downloading malware cannot be stopped by signature-based mechanisms (e.g. IPS, AV)
- Encrypted end-to-end sessions (e.g. SSL) render firewalls and network IPS blind
- Network-based security devices cannot adequately control access to sensitive data (e.g. USB flash/disk, CD/DVD ROM, encrypted sessions)
- Security policies or regulatory requirements may be too demanding for the capabilities of network security solutions (e.g. PCI Compliance)



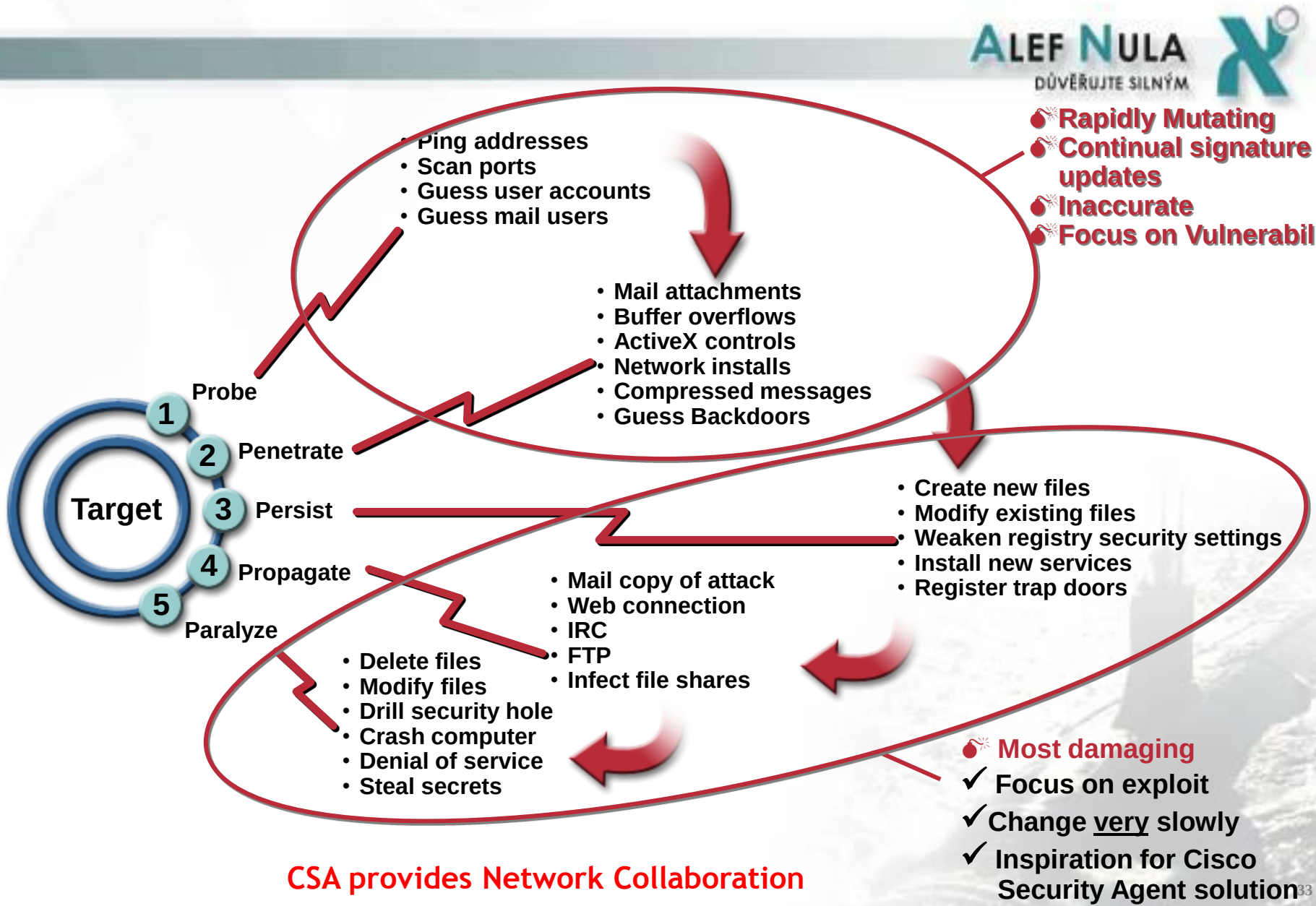
Advanced Endpoint Security

with Cisco Security Agent

- CSA extends network security solutions to end hosts
- Cisco Security Agent enhances security with:
  - **Zero Update protection** based on OS and application behavior
  - **Control of content** after decryption or before encryption (e.g. SSL, IPsec)
  - **Access control for I/O devices** based on process, network location and even file content
  - **Centralized management** and monitoring of events
  - **SDN Interaction** with other network solutions such as NAC, IPS, QoS, MARS, VOIP, etc



CSA Approach:
Behavioral Protection for Endpoints

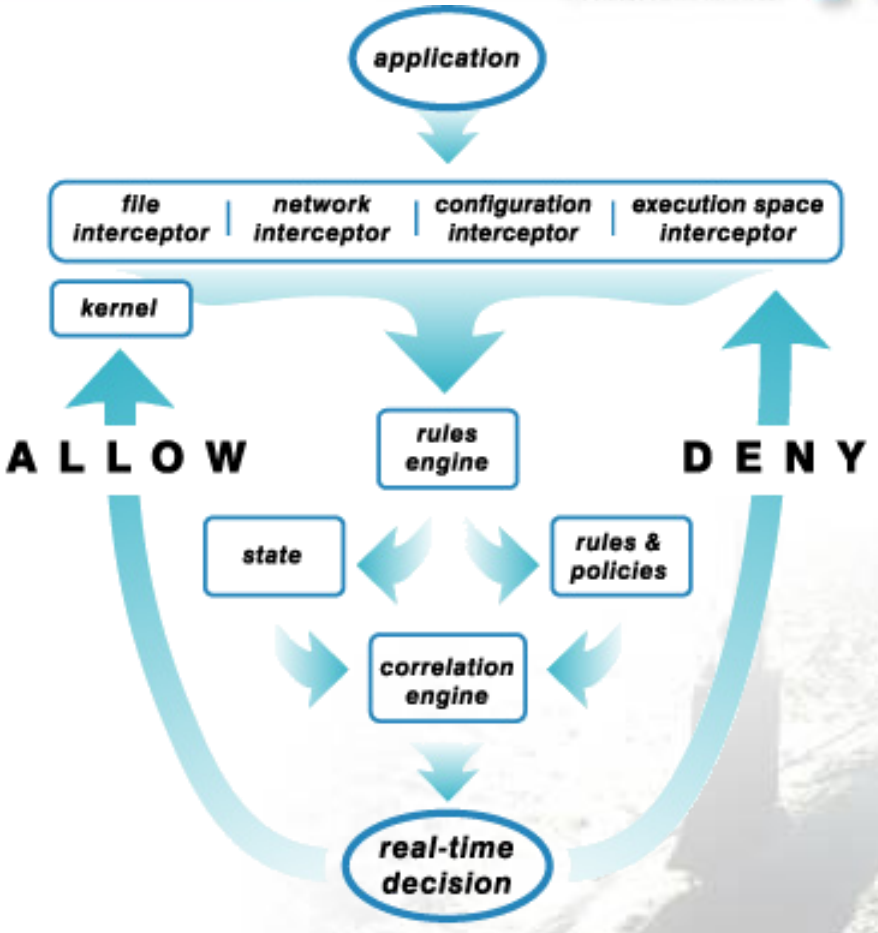


CSA provides Network Collaboration

INCORE™ Architecture – How to CSA works

ALEF NULA
DŮVĚŘUJTE SILNÝM

- The Cisco Security Agent intercepts application OS calls and invokes an allow/deny response through a technology called INCORE:
- **INCORE**
  INtercept
  COrrelate
  Rules
  Engine
- "Zero Update" architecture – you don't need a new signature to stop the next attack



CSA DayZero ScoreCard

ALEF NULA
DŮVĚŘUJTE SILNÝM

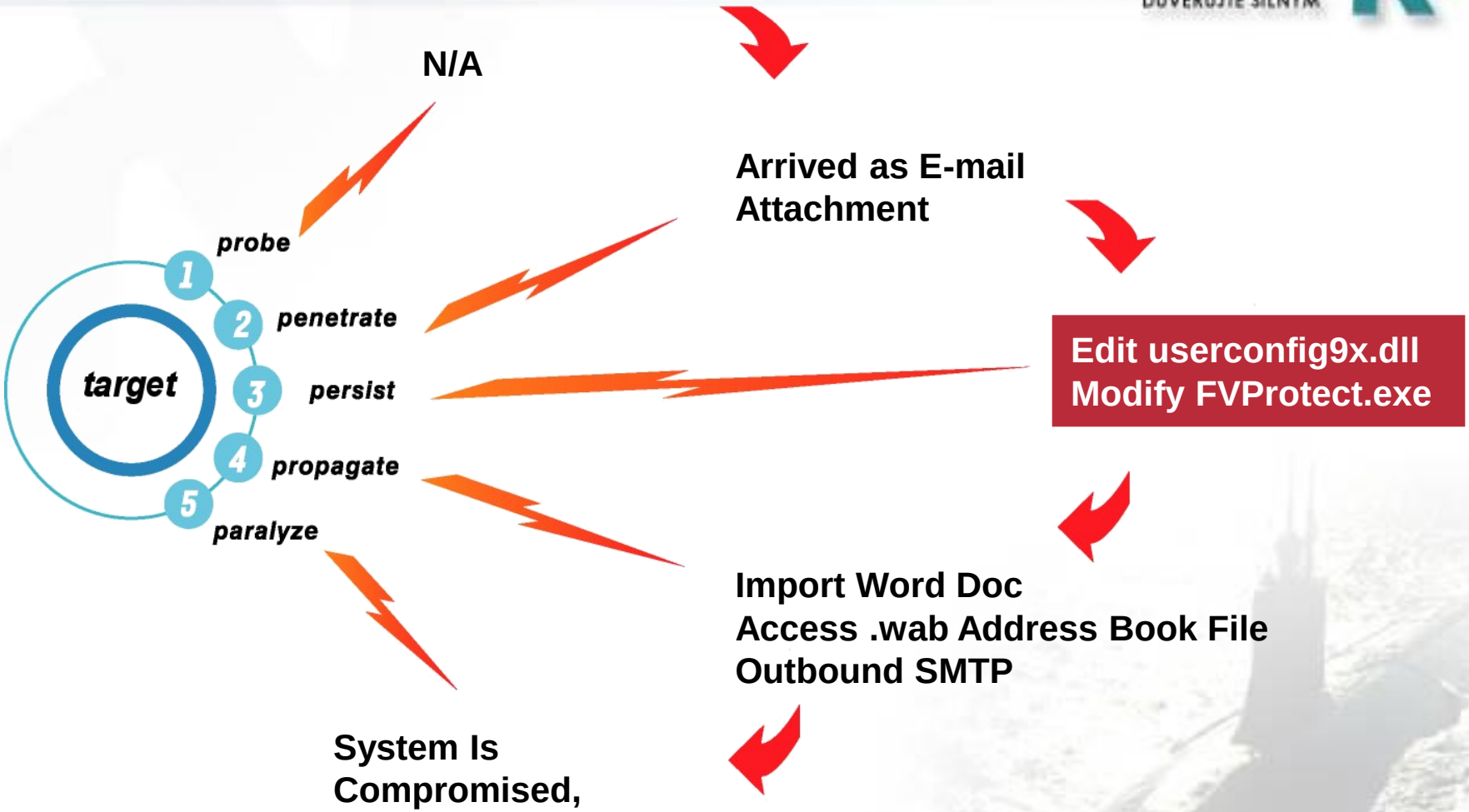
CSA successfully blocked the following known attacks with a default installation

- Non-Exhaustive List -

- Mydoom
- W32.Blaster
- Fizzer
- Bugbear
- Sobig.E

- **SQL Slammer**
- **Sircam.A**
- **WebDav Vulnerability**
- **Code Red**
- **Nimda**
- **Etc…**

CSA in Action: Protection Against Netsky Persist Phase



Data Loss Prevention (Cont.)

ALEF NULA
DŮVĚŘUJTE SILNÝM

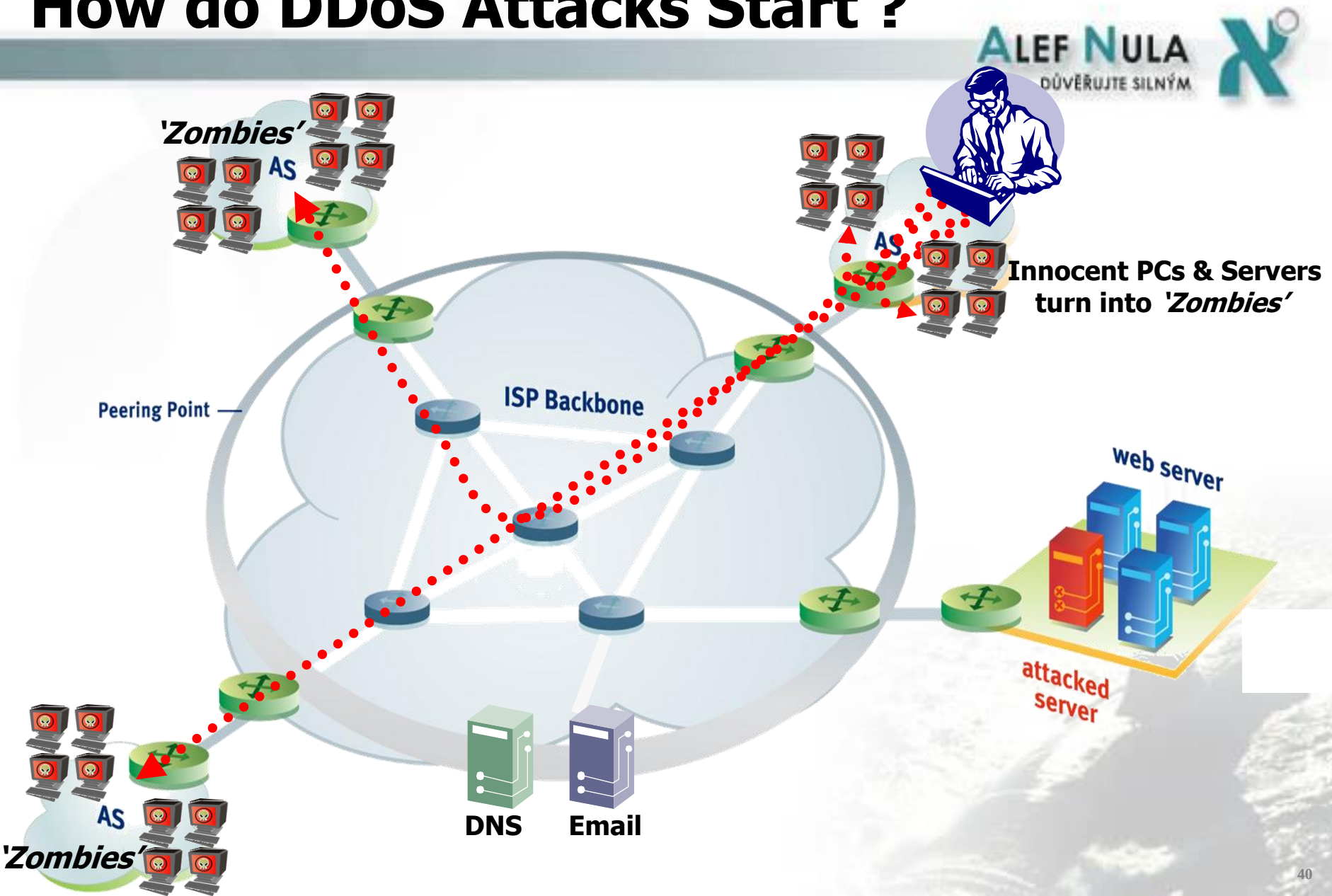
Data Theft Prevention Feature	CSA Capability
Control over removable media	– Dynamic tracking of applications that handle sensitive information – Prevents writing of sensitive information to removable media – USB, CD-ROM, floppy, etc.
Control over the Windows Clipboard	– Dynamic tracking of applications that copy and paste data – Prevents clipboard access to untrusted applications
Control over network transfers	– Dynamic tracking of applications that handle sensitive information – Prevents any network access for these applications

ALEF NULA

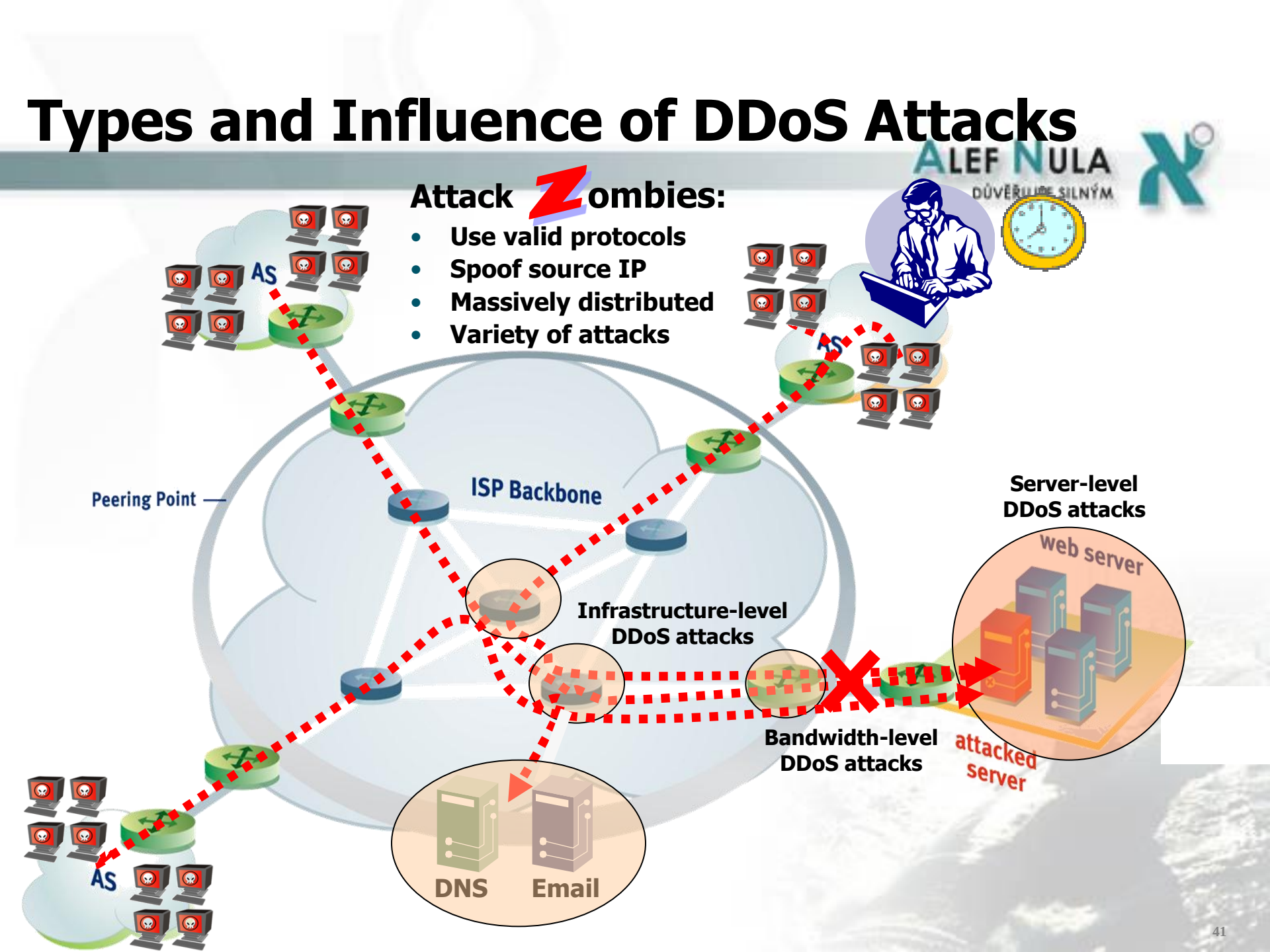
DŮVĚŘUJTE SILNÝM

CISCO DDoS MITIGATION SOLUTION

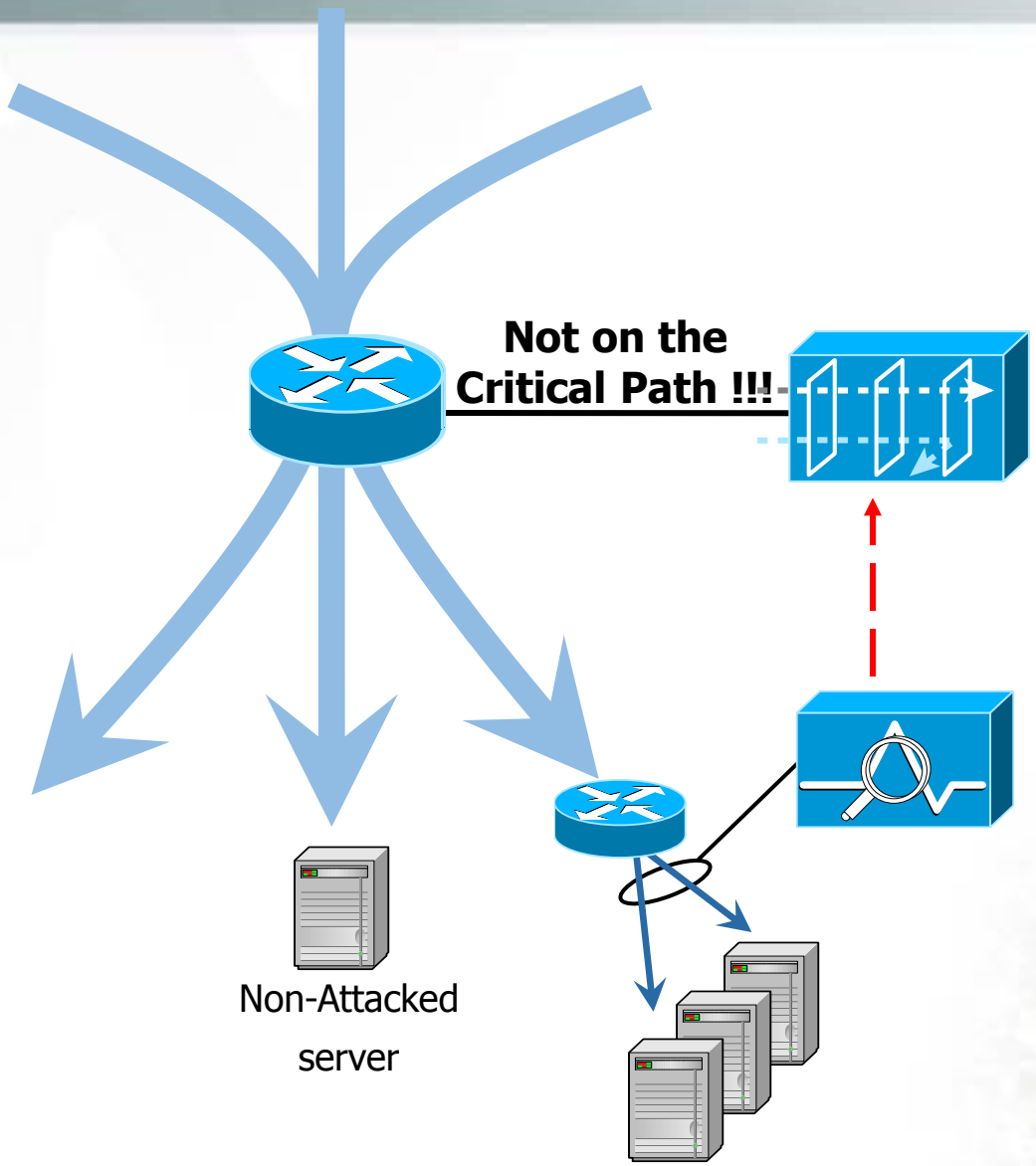
How do DDoS Attacks Start ?



Types and Influence of DDoS Attacks



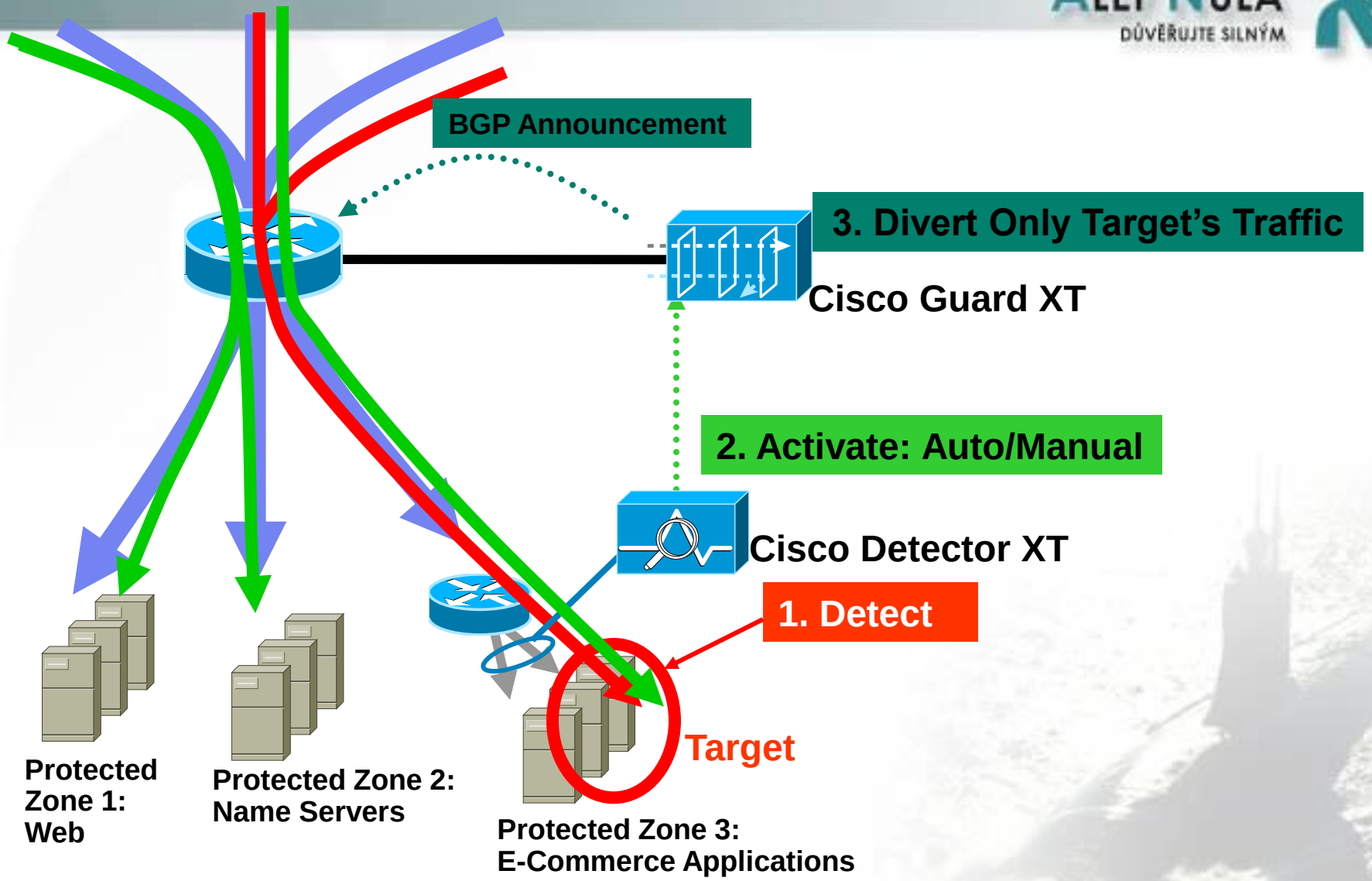
DDoS Solution Components



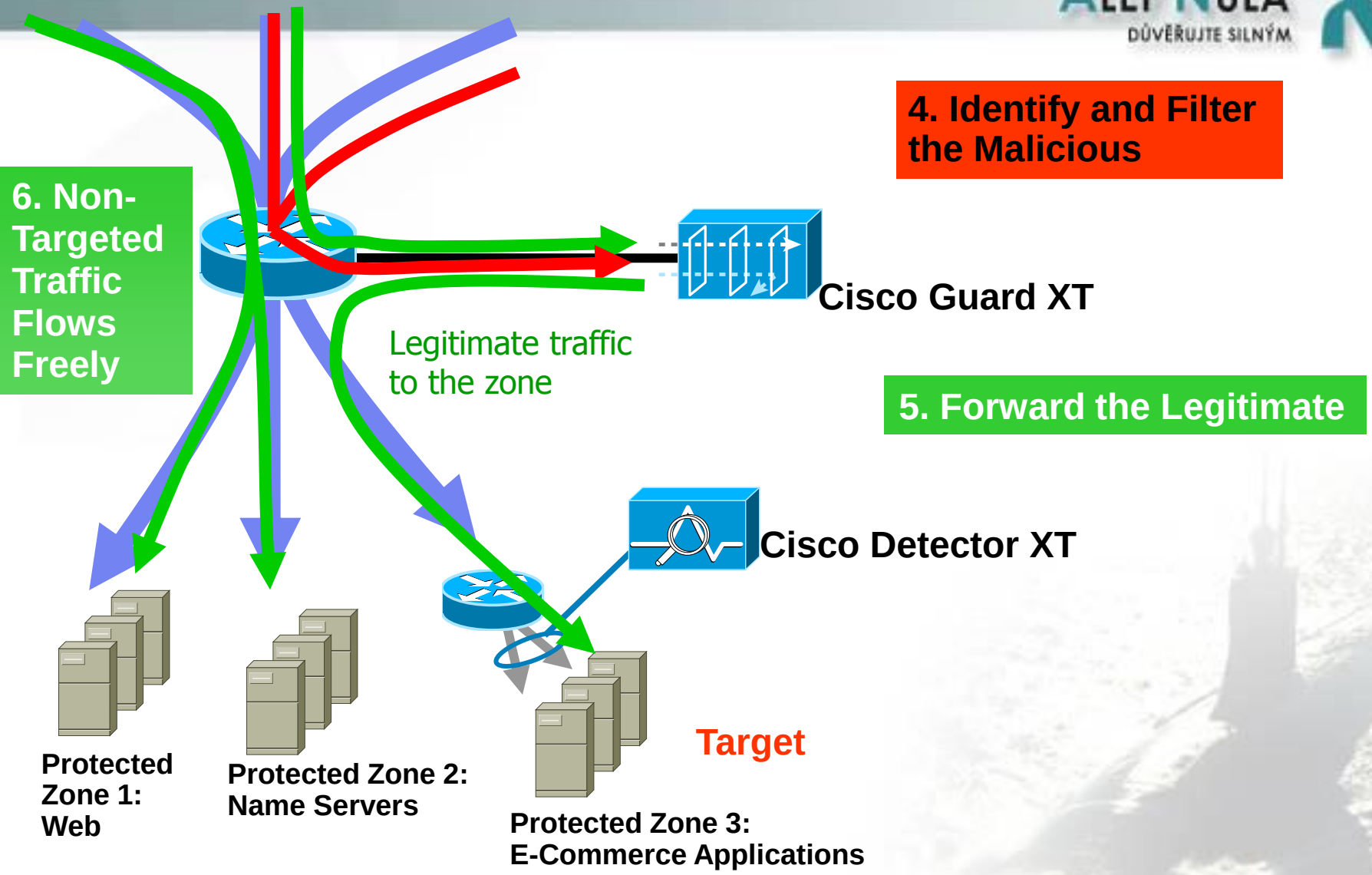
DDoS Mitigation by the
Cisco Guard

DDoS Detection by the
Cisco Traffic Anomaly Detector
or IDS/FW/3rd Party

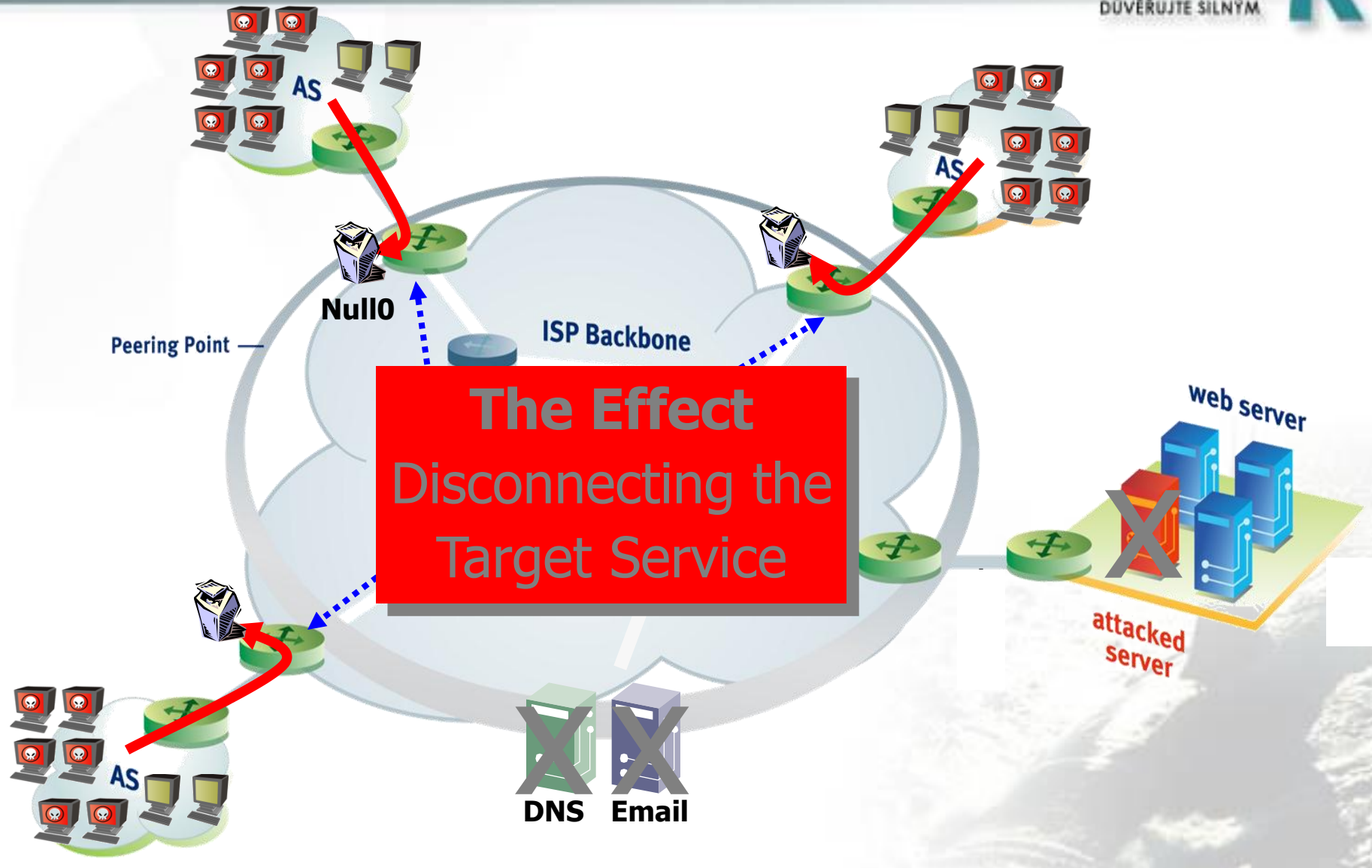
DDoS Solution Operation



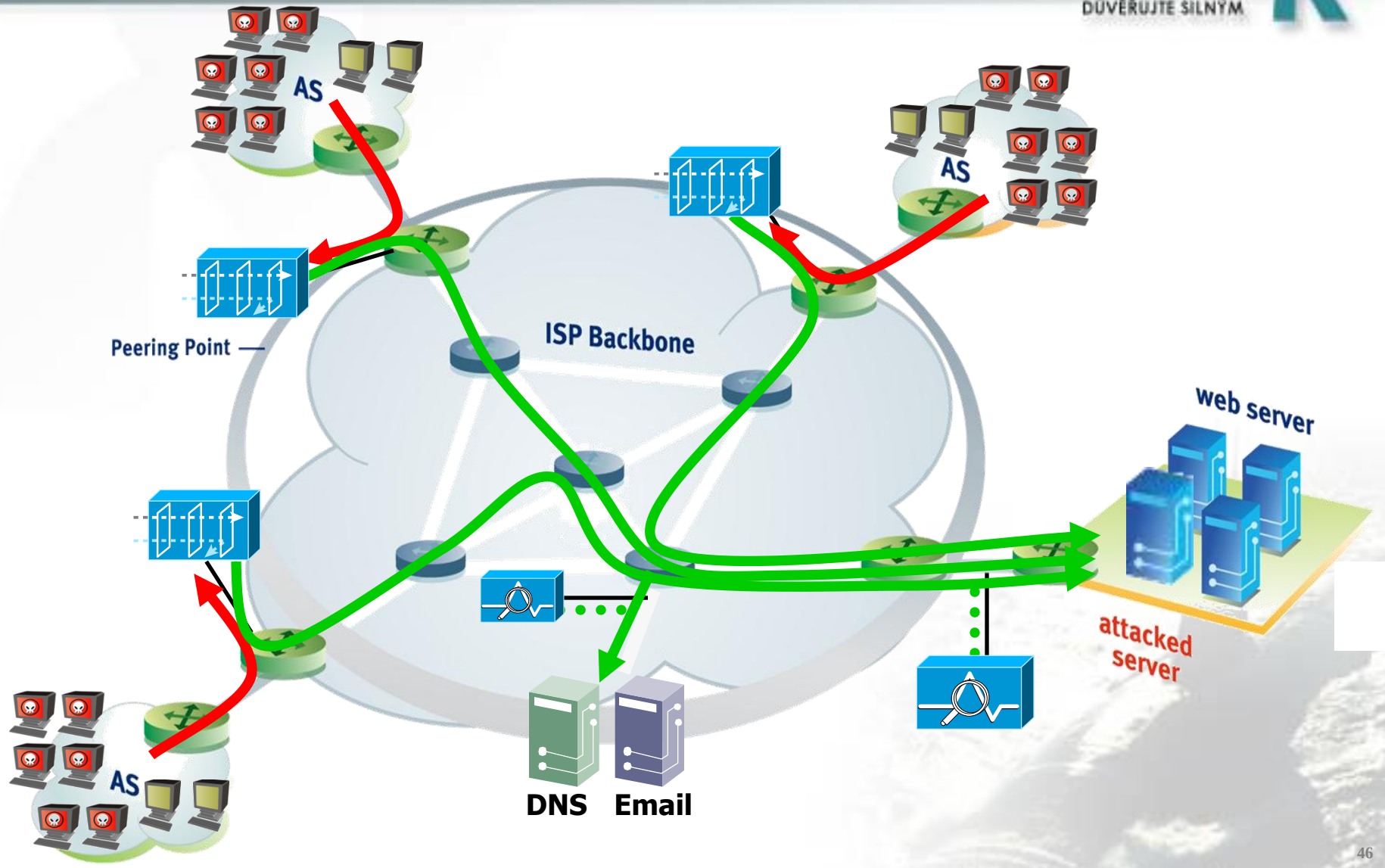
DDoS Solution Operation



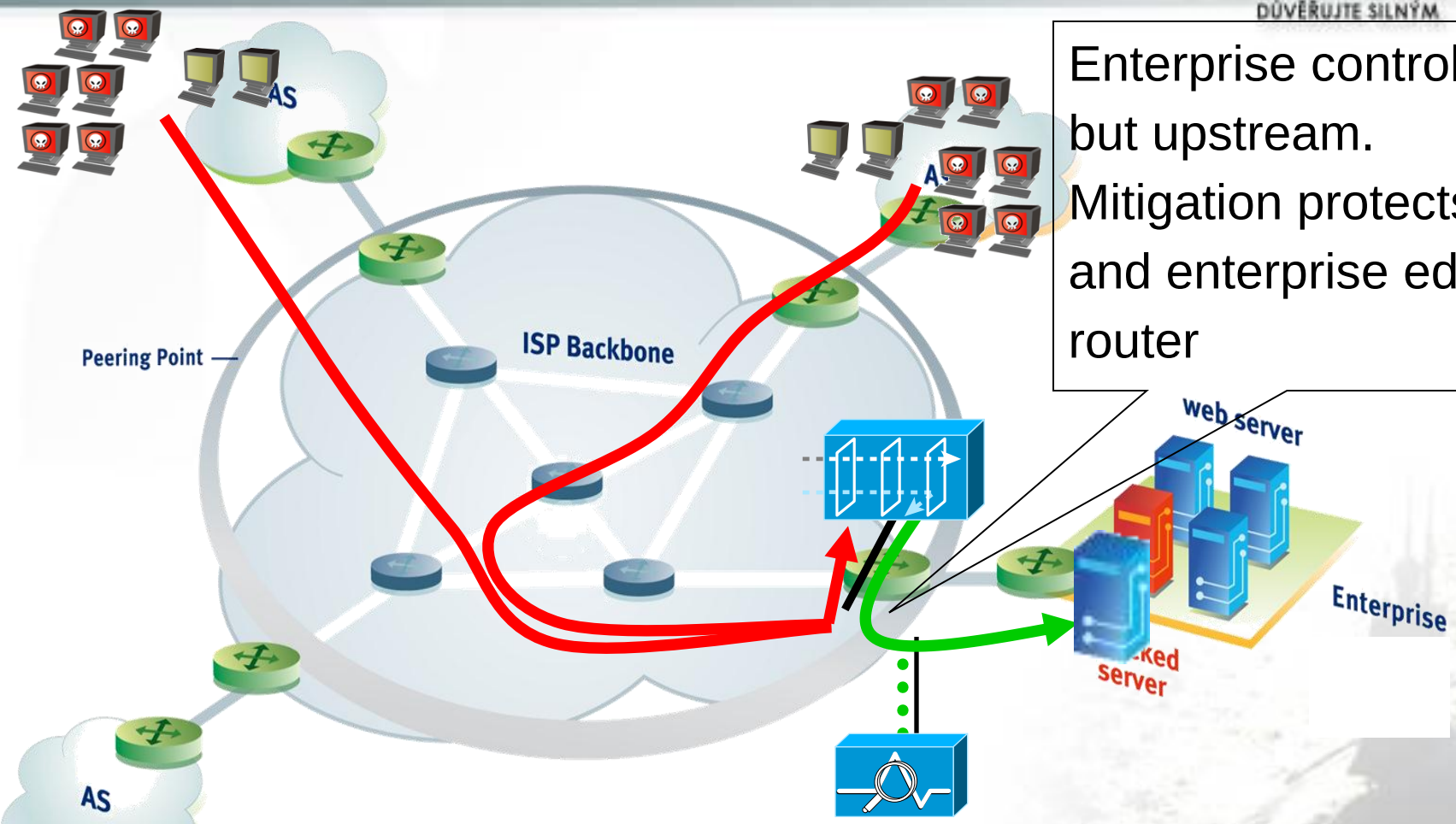
Today's Black-hole technique



Diversion at Peering Points



Enterprise Protection Upstream
Guard Co-Located at Provider Edge



Enterprise controlled, but upstream. Mitigation protects link and enterprise edge router

Detector activates the Guard via separate management circuit

ALEF NULA

DŮVĚŘUJTE SILNÝM

Bottnet Traffic Filter

ASA 8.2

Botnet Epidemic

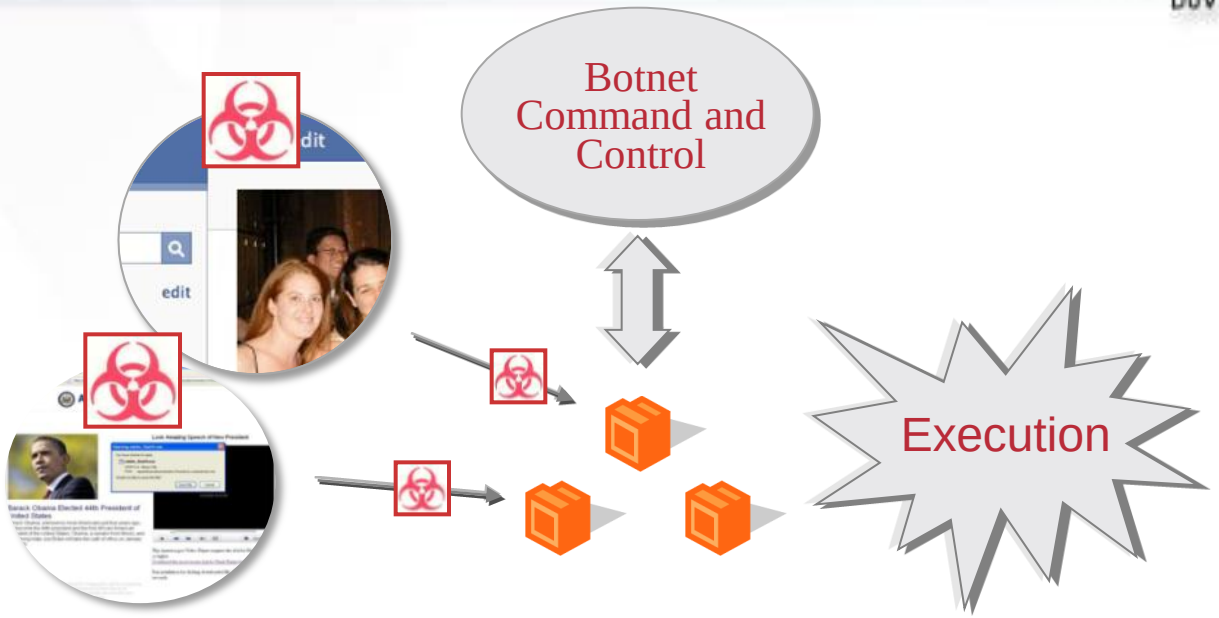
BBC Purchases Botnet Offered For Rent

CBS News Covers Conficker Worm, Malware Epidemic

Next-gen Botnet Armies Fill Spam Void

- Botnets (network of compromised computers) control approximately 25% of all personal computers
- Attacks include spam, identity theft, information harvesting and denial-of-service attacks to attacks on websites for profit
- More than 5 Million hosts infected in US alone
- Normal security mechanisms are only 75% effective against malware that are used to recruit bots

Botnet Stages of Attack



Step 1: Infection

Clients are infected by spyware, malware, and targeted attacks

Step 2: Control

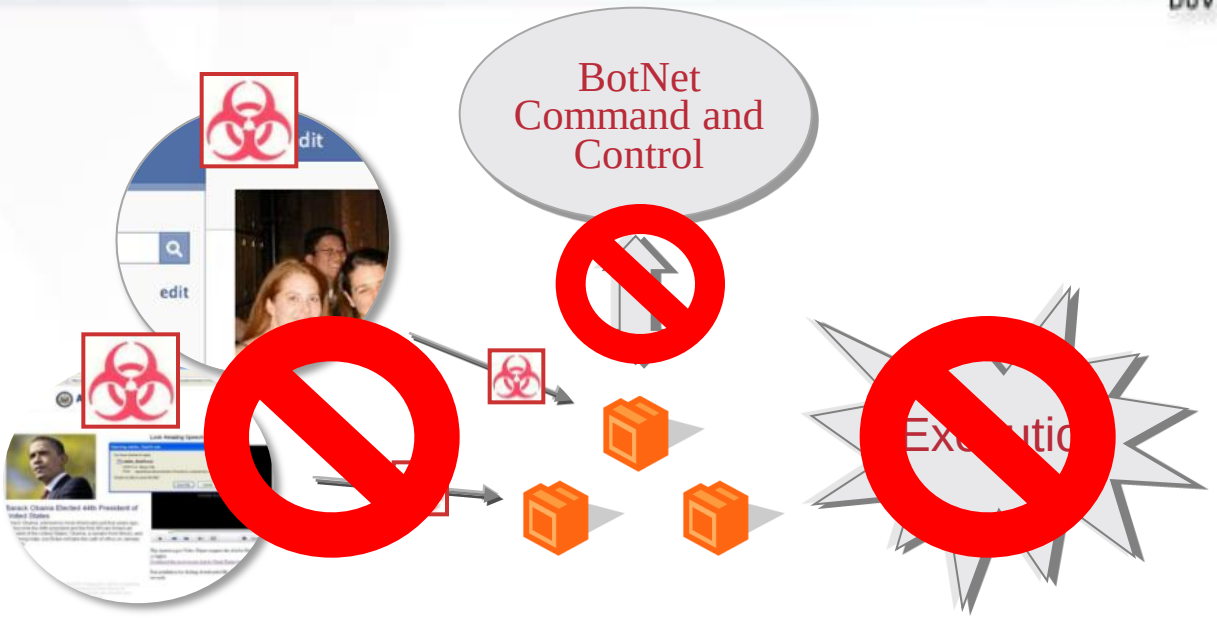
Infected clients communicate with botnet command and control

Step 3: Execution

Attacks are launched: data harvesting, ID theft, DDoS, spam, and click fraud

Cisco Anti-Botnet Solution

Defense in Depth



Step 1: Protection

Cisco Firewall,
Intrusion Prevention Systems,
Web Security Appliances,
Email Security Appliances

Step 2: Detection

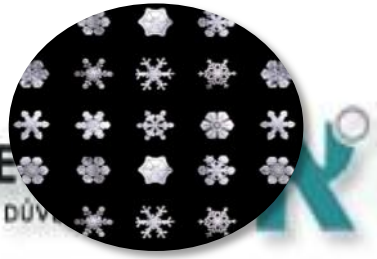
BotNet Traffic Filter

WSA Layer 4 Traffic Monitor

Step 3: Remediation

Cisco NAC

Profile of a BOTNET
Srizbi Botnet



- Computers infected by Srizbi trojan via spam
- 450,000 compromised machines to date

Large army of bots

- Fully-executed in kernel mode
- Employs rootkit technologies
- Patches NTFS file system drives to make files invisible to OS

Evades Normal Security Mechanisms

- Sends 60 billion spam messages a day (50% of total worldwide)
- “Ron Paul” incident – 3000 bot computers sent spam to 160 million email addresses

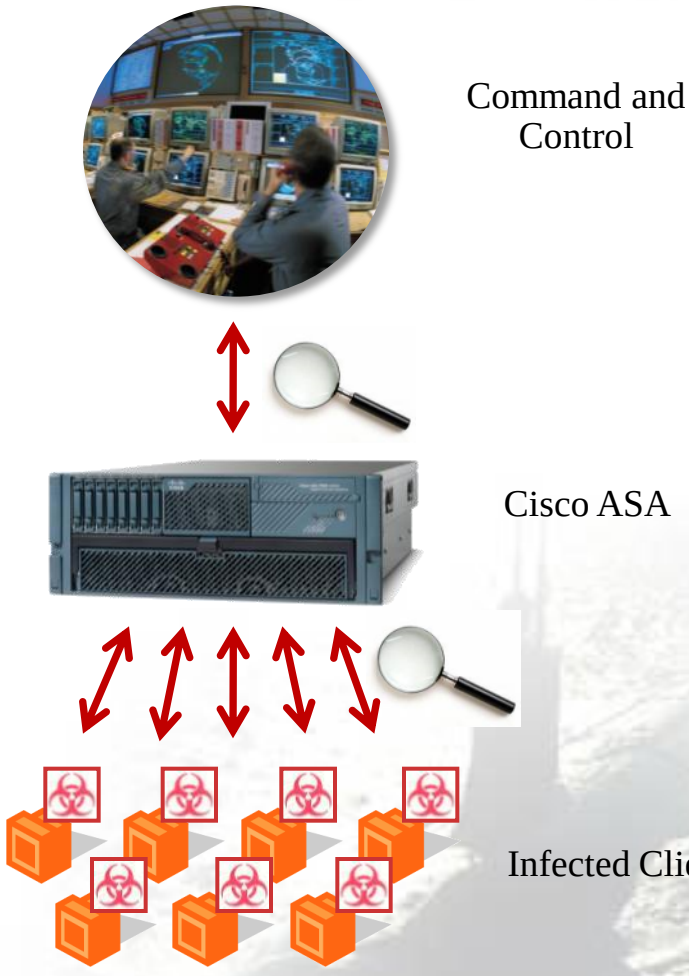
Massive attack scale

Detecting Client Infections

Botnet Traffic Filter on ASA 5500 Series

ALEF NULA
DŮVĚŘUJTE SILNÝM

- **Monitors malware traffic**
  - –Scans all traffic, ports & protocols
  - –Detects infected clients by tracking rogue "phone home" traffic
- **Highly accurate**
  - –Identifies100,000s of malware connections per week
  - –Automatic DNS lookups of addresses
  - –Dynamic database integrated into Cisco Security Intelligence Operations

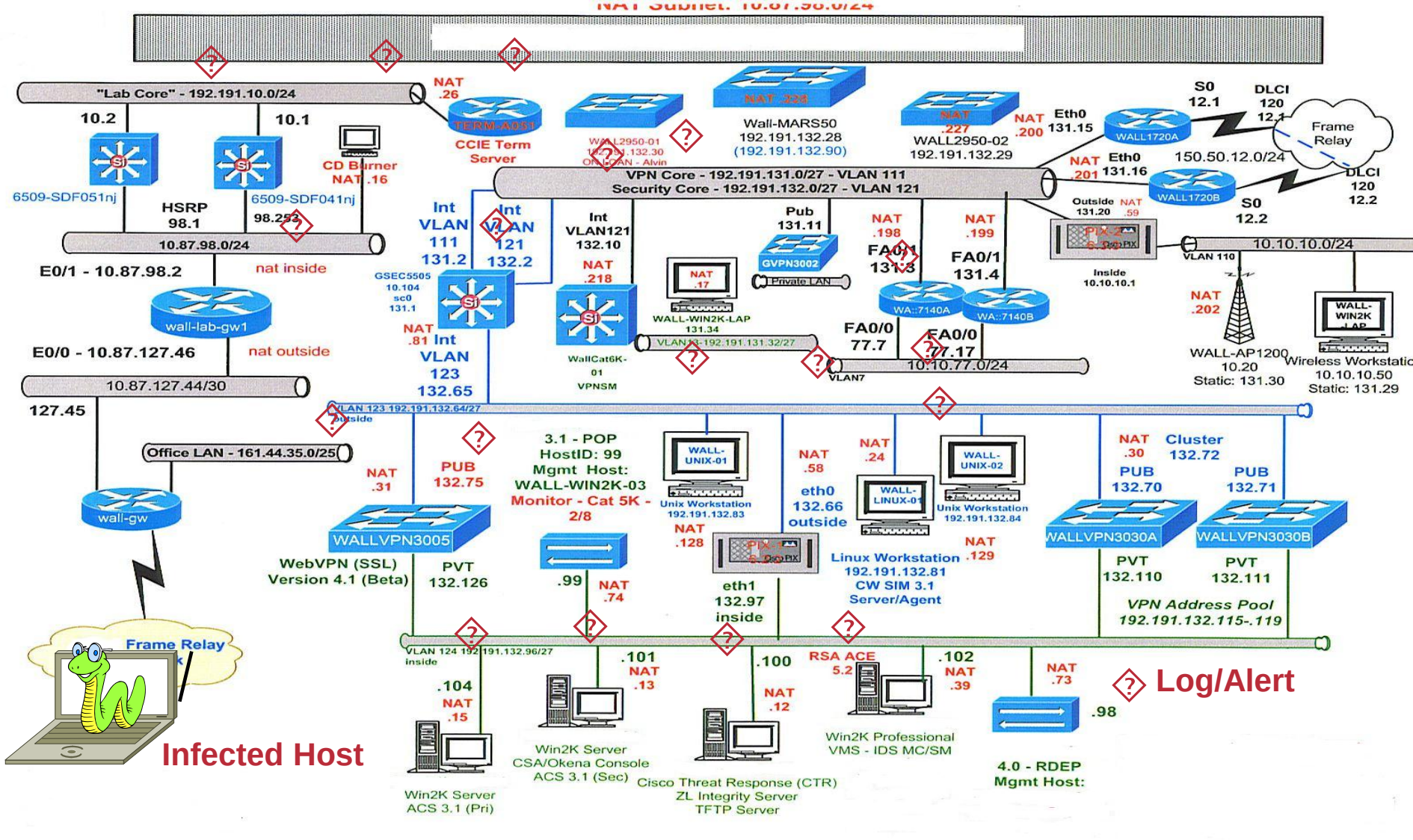


ALEF NULA

DŮVĚŘUJTE SILNÝM

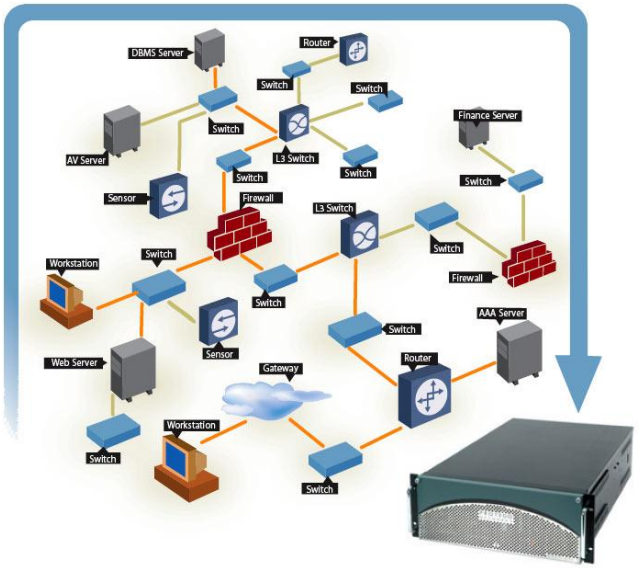
CISCO SECURITY MONITORING, ANALYSIS & RESPONSE SYSTEM (MARS)

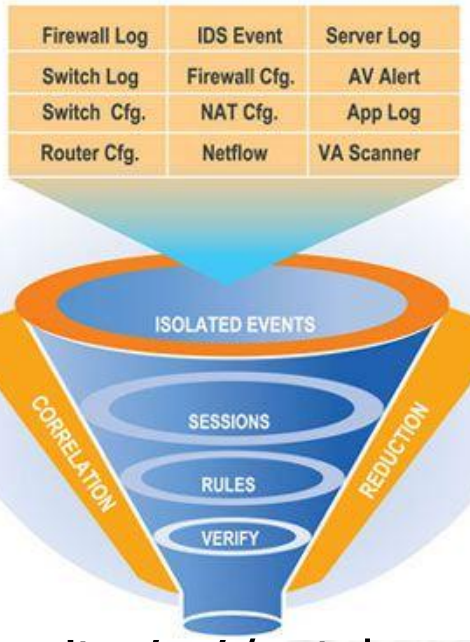
Defense-In-Depth = Complexity



Mitigation, Analysis, and Response System (MARS) *Next Generation SIM/STM*

- Leverage YOUR existing investment to build "pervasive security"
- Correlate data from across the Enterprise
  - NIDS, Firewalls, Routers, Switches, CSA
  - Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs, Multi-Vendor
- Rapidly locate and mitigate attacks

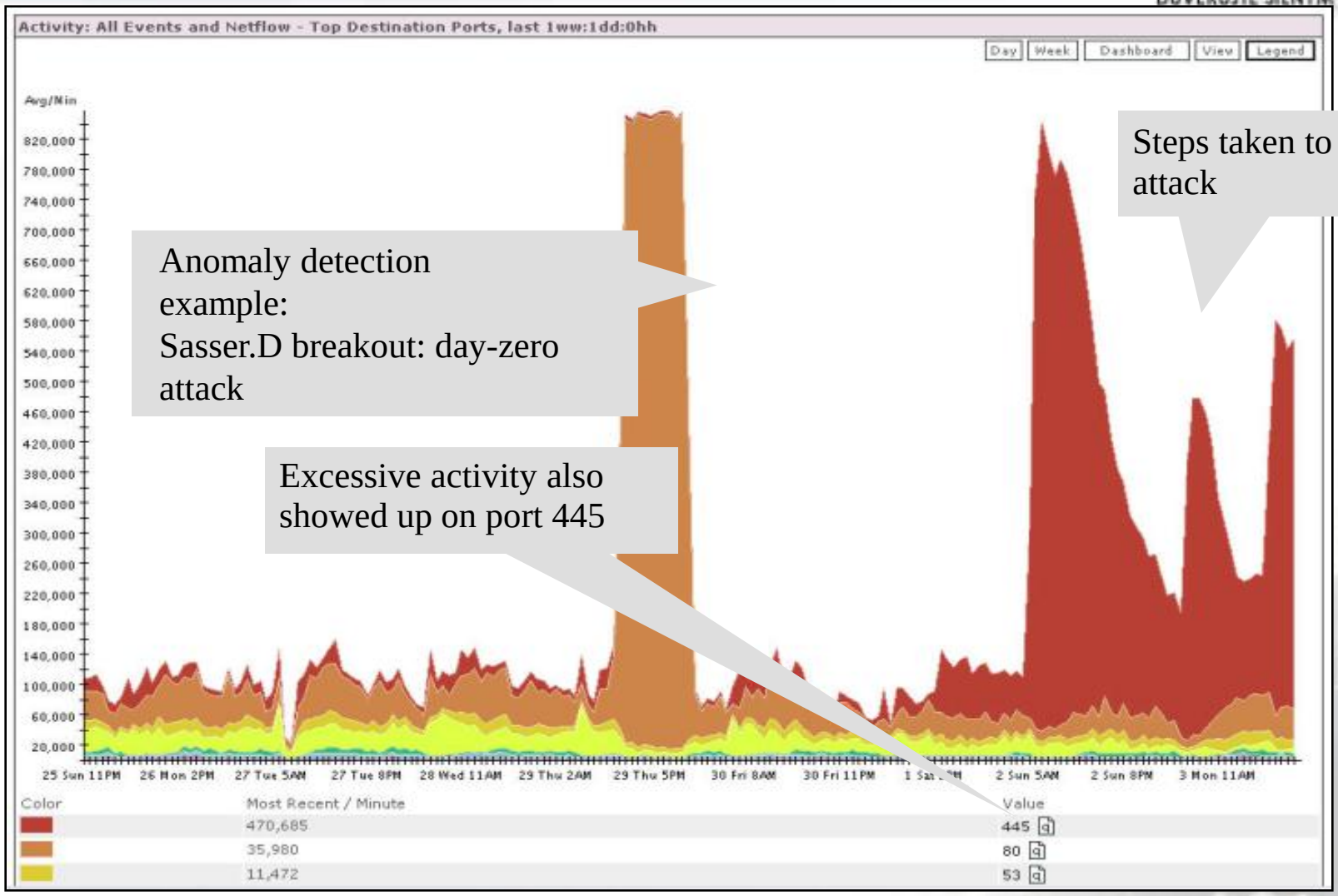




- Key Features
  - Determines security *incidents* based on device *messages*, *events*, and "*sessions*"
  - *Incidents* are topologically aware for visualization and replay
  - Mitigation on L2 ports and L3 chokepoints

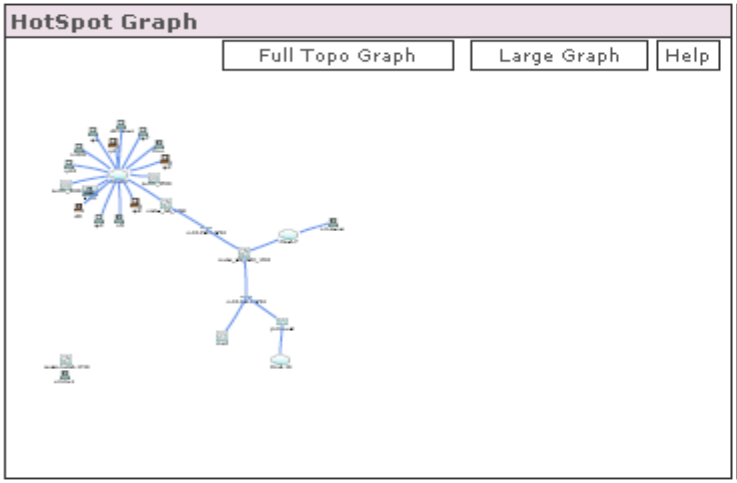
Anomaly Service: NetFlow Anomaly Detection Response to Sasser.D Attack

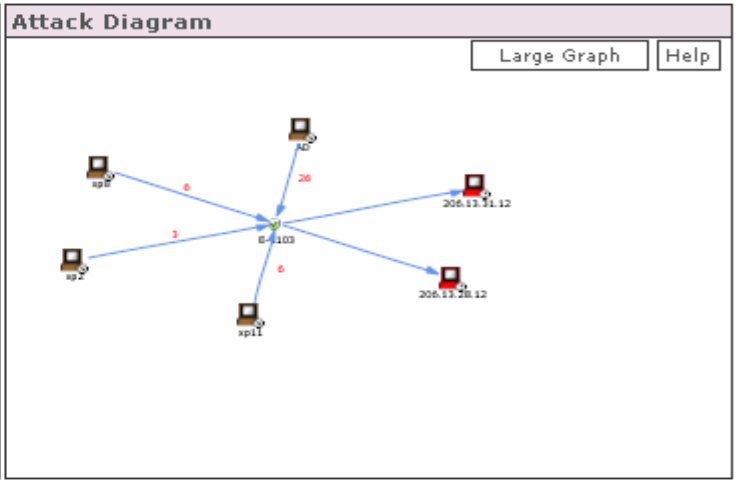
ALEF NULA
DŮVĚŘUJTE SILNÝM



Diagrams

- Diagrams
  - Hot Spot Graph (most recent incidents src/dest pairs)
  - Full Topology (displays the full network)
  - Attack Diagram (the last 500 events related to incidents for the past 24hrs)
- Generated by the configuration and topology discovery information that you provide.
- Drill-down into the diagrams by clicking the icons.
- Drill-down attack paths in the Attack Diagram by clicking the Path icon.
- Drilling-down into these diagrams is one of the fastest ways to uncover real-time information about your network.





CS-MARS Compliance Report

ALEF NULA
DŮVĚŘUJTE SILNÝM

Popular reports with customization and distribution options
Queries saved as rules or reports – intuitive framework (no SQL)

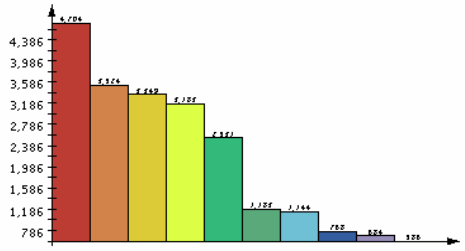
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

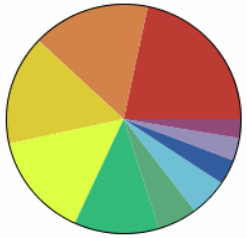
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

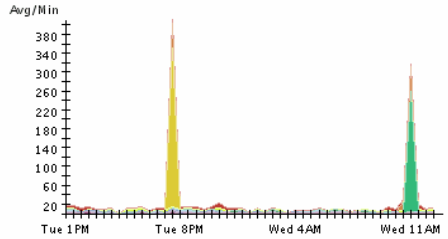
Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]

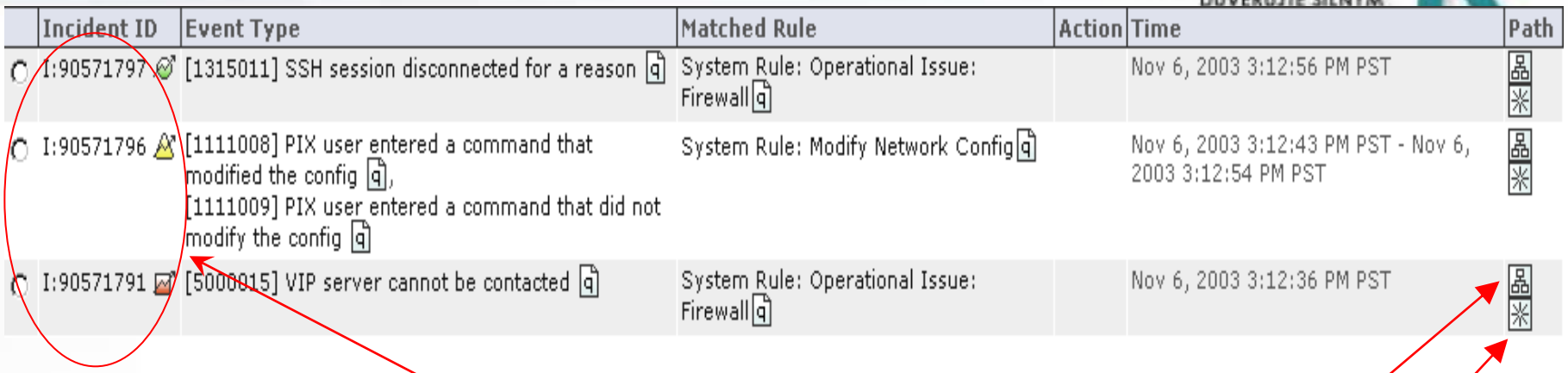






Rank		Count (# of sessions)	Raw Destination Port
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

The Incidents Page



	Incident ID	Event Type	Matched Rule	Action	Time	Path
○	I:90571797	[1315011] SSH session disconnected for a reason	System Rule: Operational Issue: Firewall		Nov 6, 2003 3:12:56 PM PST	
○	I:90571796	[1111008] PIX user entered a command that modified the config, [1111009] PIX user entered a command that did not modify the config	System Rule: Modify Network Config		Nov 6, 2003 3:12:43 PM PST - Nov 6, 2003 3:12:54 PM PST	
○	I:90571791	[5000015] VIP server cannot be contacted	System Rule: Operational Issue: Firewall		Nov 6, 2003 3:12:36 PM PST	

Drill down

- **Click the Incidents tab to navigate to the Incidents page.**
- **The Incident page's table:**
  - ***Incident ID***
  - An incident's unique ID
  - ***Severity***
  - Green, Yellow, and Red icons
  - ***Event Type***
  - The normalized signature sent from the reporting devices.
  - ***Matched Rule***
  - The rule whose criteria was met.

The Incident page's table (cont.):

- ***Action***

  The description of the notification taken when this rule fires.
- ***Time***

  A single time or a time range
- ***Incident Path***

  The icon that takes you to the incident's path diagram.
- ***Incident Vector***

  The icon that takes you to the source, event type, and destination diagram.

Incident Path

Incident ID	Event Type	Matched Rule	Action	Time	Path
I:81408011	IIS DOT DOT EXECUTE, IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	Nimda Rule		Mar 1, 2005 7:03:19 PM PST	

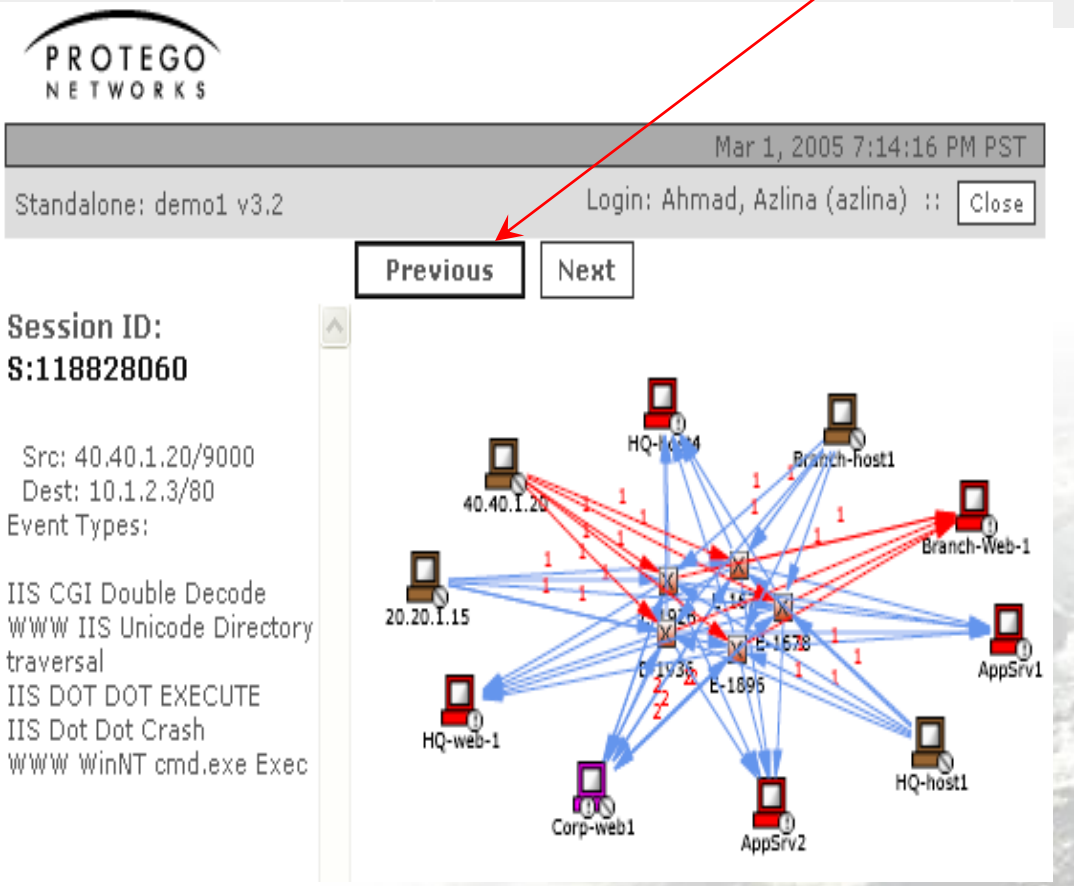
- Click on the PATH icon will display the attack path diagram of the incident
- It displays all the associated sessions of this incident as well as the event types of each session
- Toggle Topology display the Full Topology of the discovered network

Incident Attack Diagram

ALEF NULA
DŮVĚŘUJTE SILNÝM

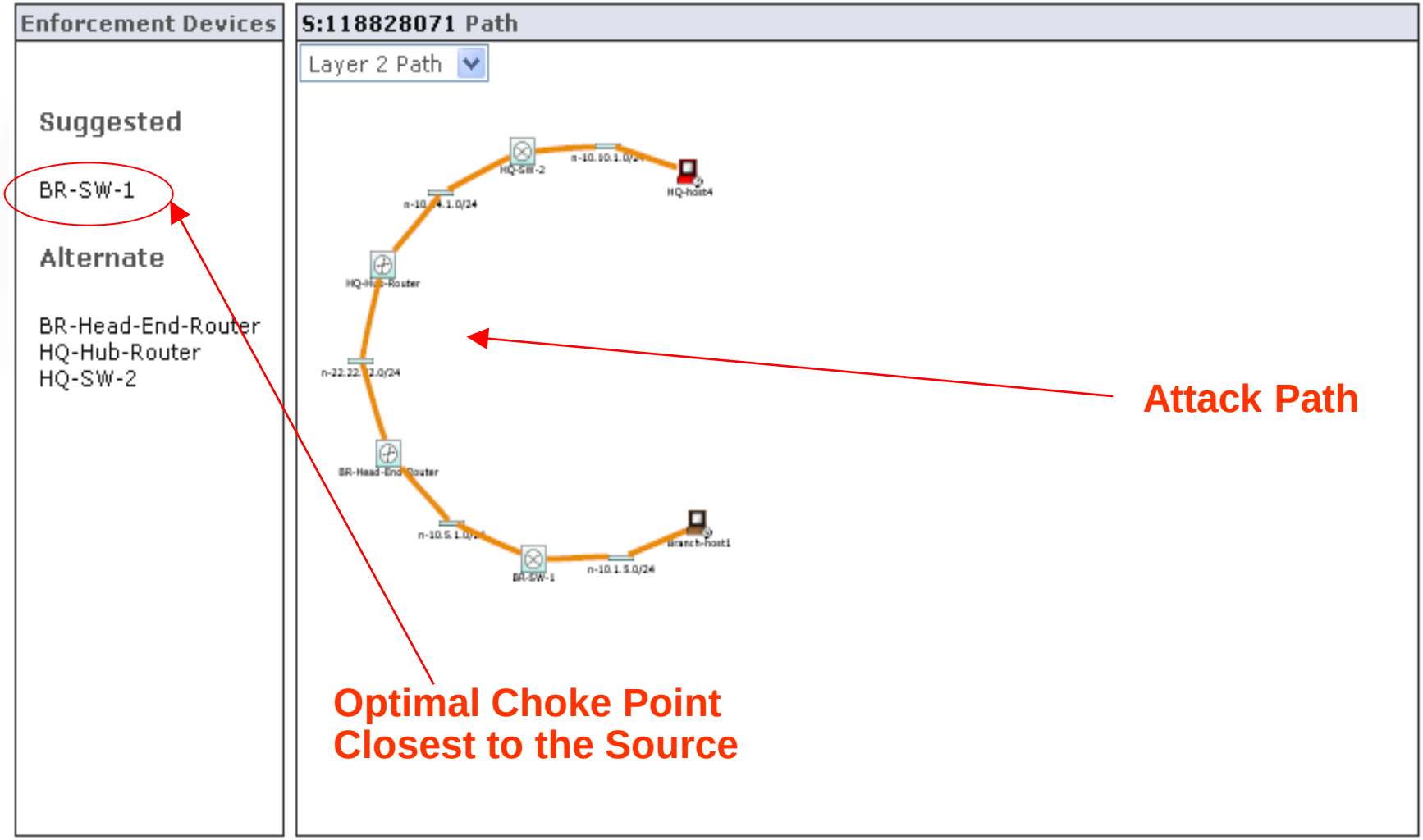
Incident ID	Event Type	Matched Rule	Action	Time	Path
I:81408011	IIS DOT DOT EXECUTE, IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	Nimda Rule		Mar 1, 2005 7:03:19 PM PST	

- Click on the Incident vector icon will display the attack diagram
- It displays each attack session and provides the Src & Dest IPs as well as the all the Event Type
- The color coded host indicates if it is compromised (red), attacker (brown) or both (purple)
- Each link is label with the no of occurrences



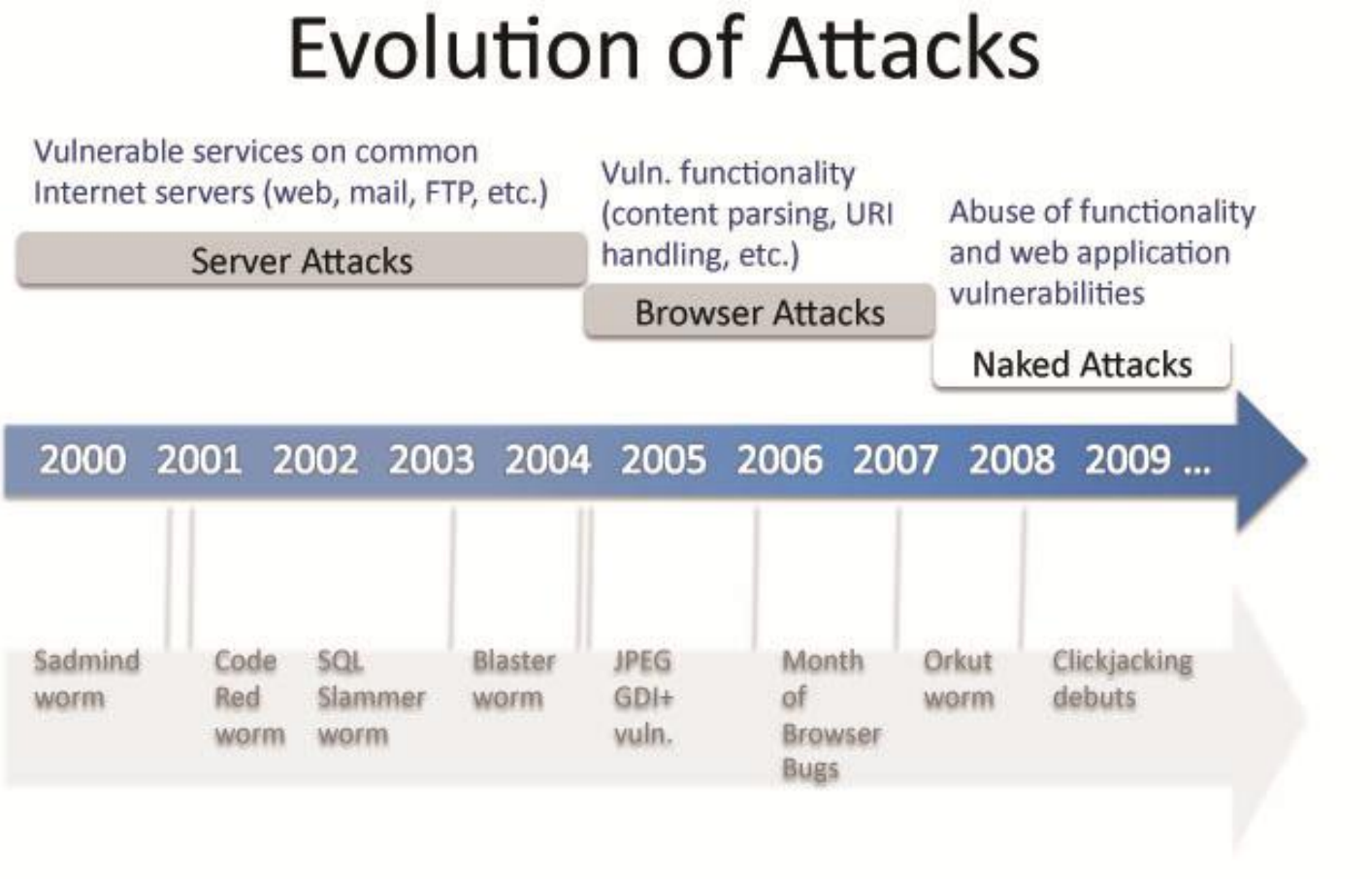
Mitigation Information Page

- **To mitigate an attack:**



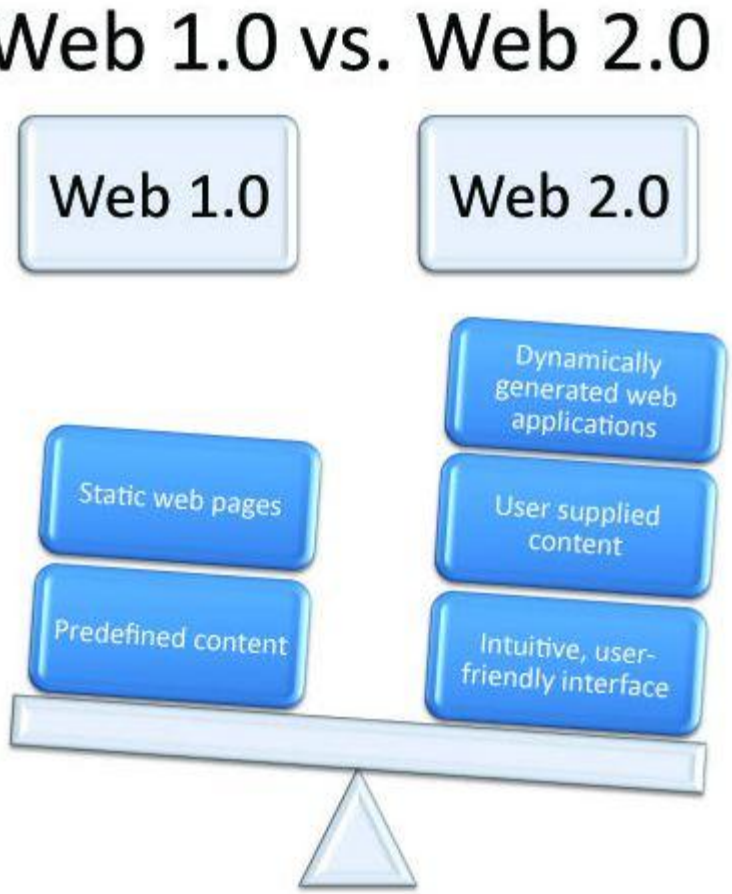
Útoky v čase

ALEF NULA
DŮVĚŘUJTE SILNÝM



Srovnání Web 1.0 vs. 2.0

ALEF NULA
DŮVĚŘUJTE SILNÝM



Web 2.0

ALEF NULA
DŮVĚŘUJTE SILNÝM

Obsah vytvářený uživatelem

- moderní webové stránky vybízí uživatele k vytváření vlastního obsahu
- z TOP100 stránek v angličtině:
    - 77 povoluje obsah vytvářený uživatelem (např. sociální sítě)
    - 55 povoluje sdílení souborů
    - 12 obsahuje „pochybné" zdroje (pornografie, gambling, …)
    - uživatelé považují populární weby za legitimní, bez ohledu na to, že může obsahovat obsah třetích stran, který nemusel být jakkoliv validován

Problematická bezpečnost

- Validují webové servery vkládaný obsah?
- Nejsou tyto servery prostředkem pro „data leakage"?

„Naked“ útoky

ALEF NULA
DŮVĚŘUJTE SILNÝM

ActiveX/Javascript

• zneužití chyby v implementaci skriptovacího jazyka

Formát souborů

• chybné zpracování souboru s modifikovaným obsahem umožní spustit kód s oprávněním uživatele

Cross-site Scripting/cross-site request forgery

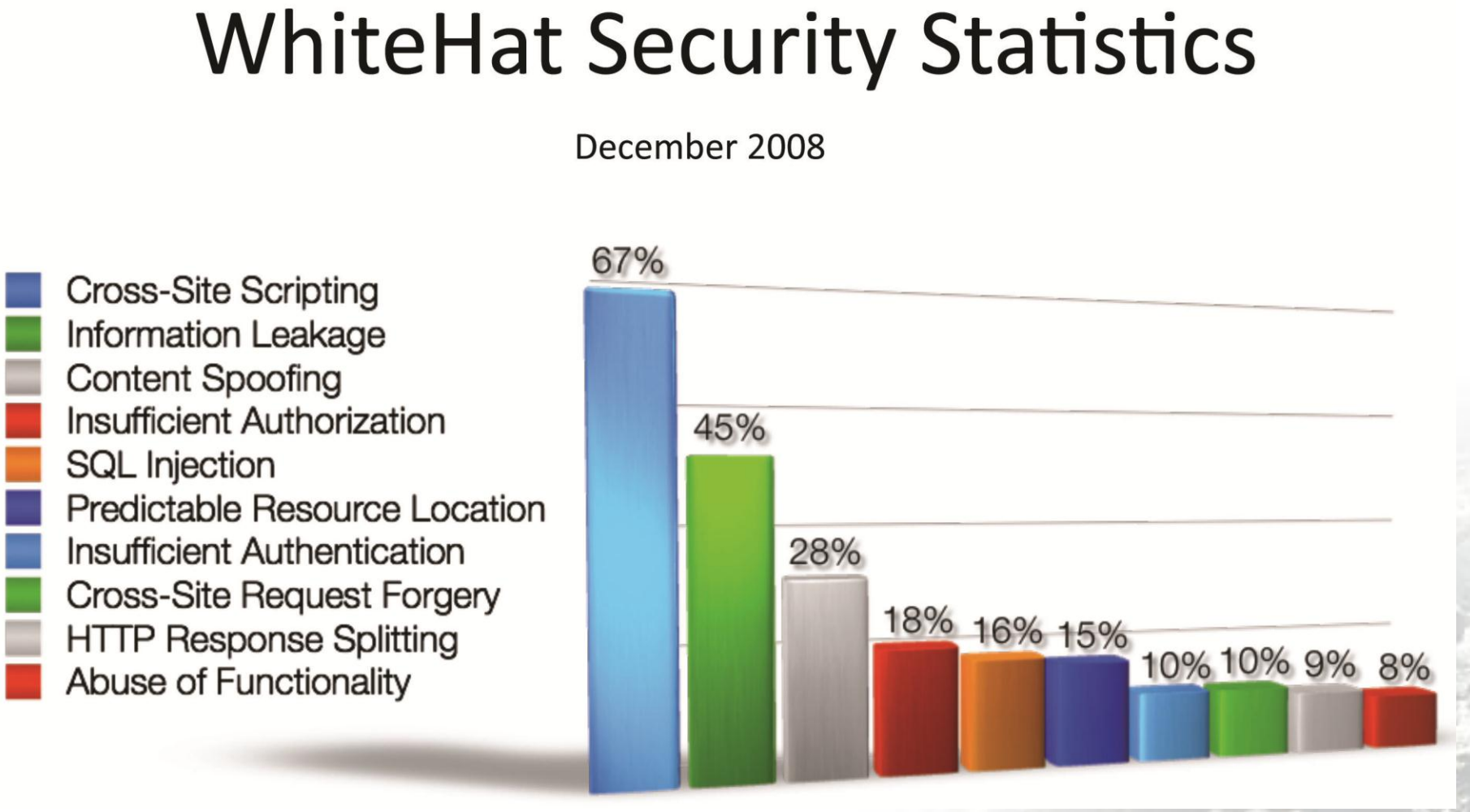
• útočník injektuje nežádoucí, typicky Javascript, do prohlížeče oběti

Clickjacking

• útočník přiměje oběť ke kliknutí na webové stránce tak, aby se provedla útočníkem požadovaná akce

Statistika dle WhiteHat

ALEF NULA
DŮVĚŘUJTE SILNÝM



Cross-site scripting (XSS)

ALEF NULA
DŮVĚŘUJTE SILNÝM

Co je XSS?

- zneužití nedostatečné kontroly vstupů webových aplikací
- útočníkova data jsou zobrazena v dynamicky generované stránce
- útočníkův skript je spuštěn v prohlížeči oběti
- oběť typicky vůbec neví, že je útok tohoto typu spuštěn

Rizika

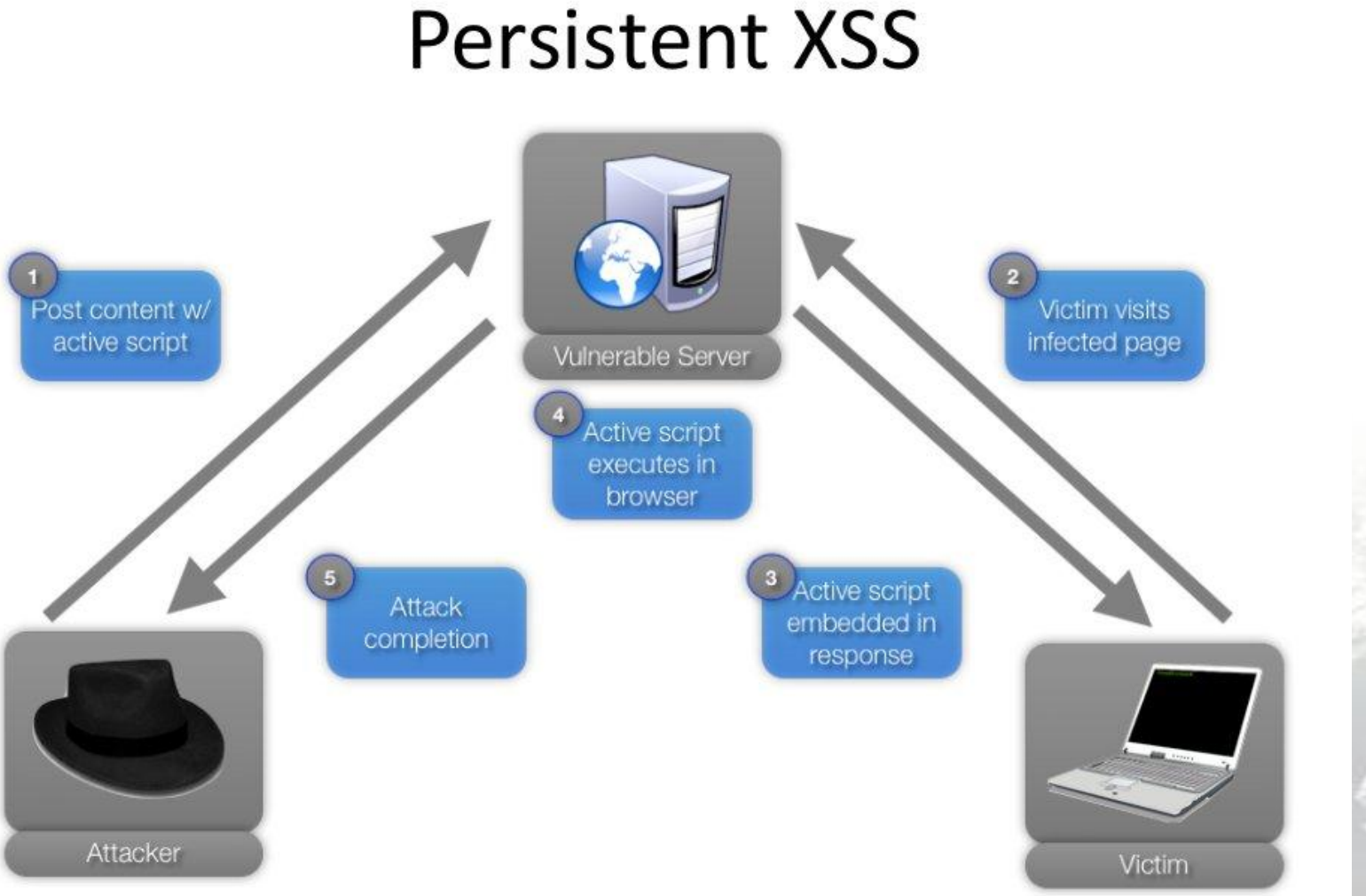
- zcizení autentizačních údajů oběti
- přepisování obsahu stránek
- vykonávání nechtěných akcí na straně oběti

Typy XSS

- persistent
- non-persistent (reflected)

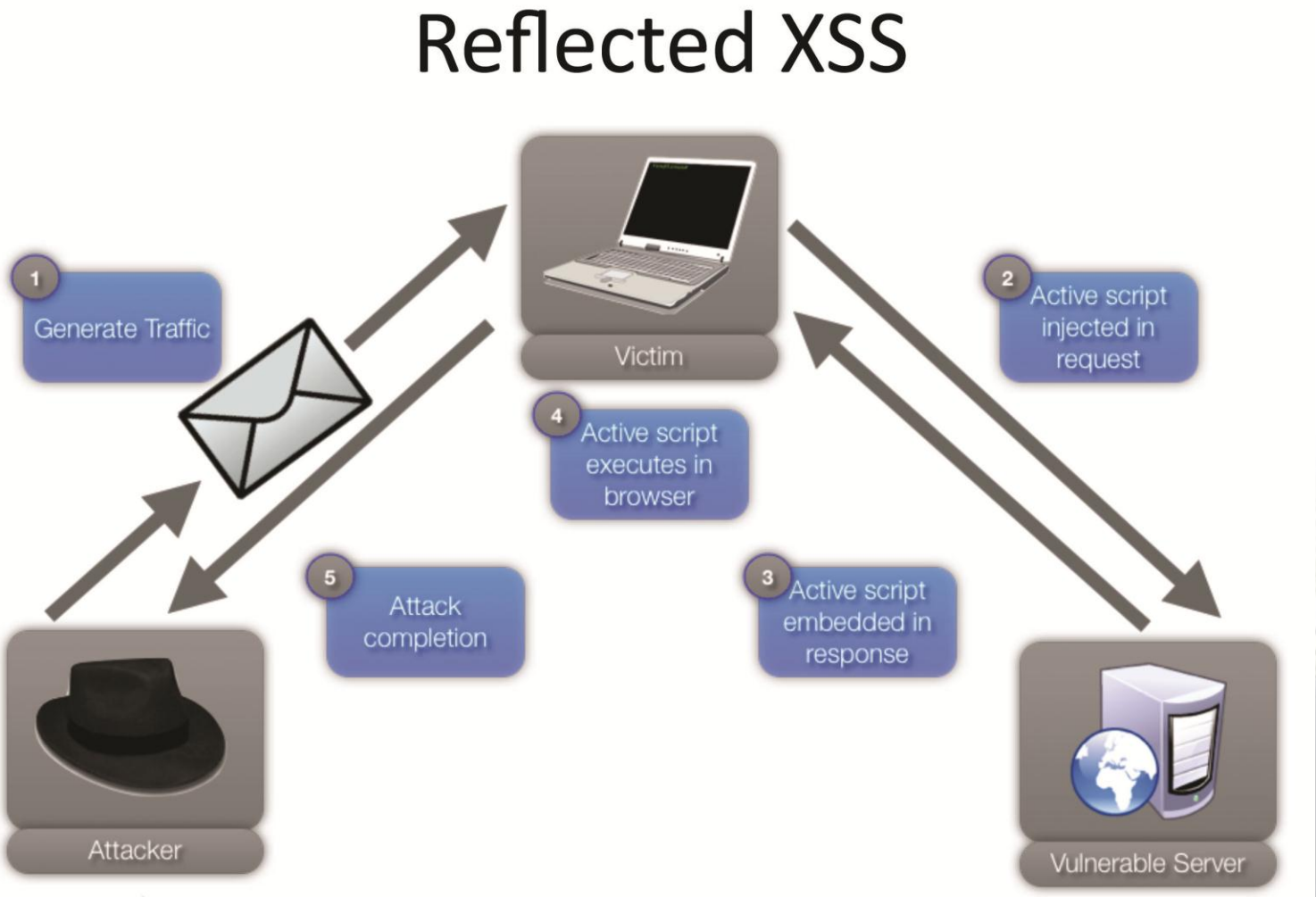
Persistent XSS

ALEF NULA
DŮVĚŘUJTE SILNÝM



Reflected XSS

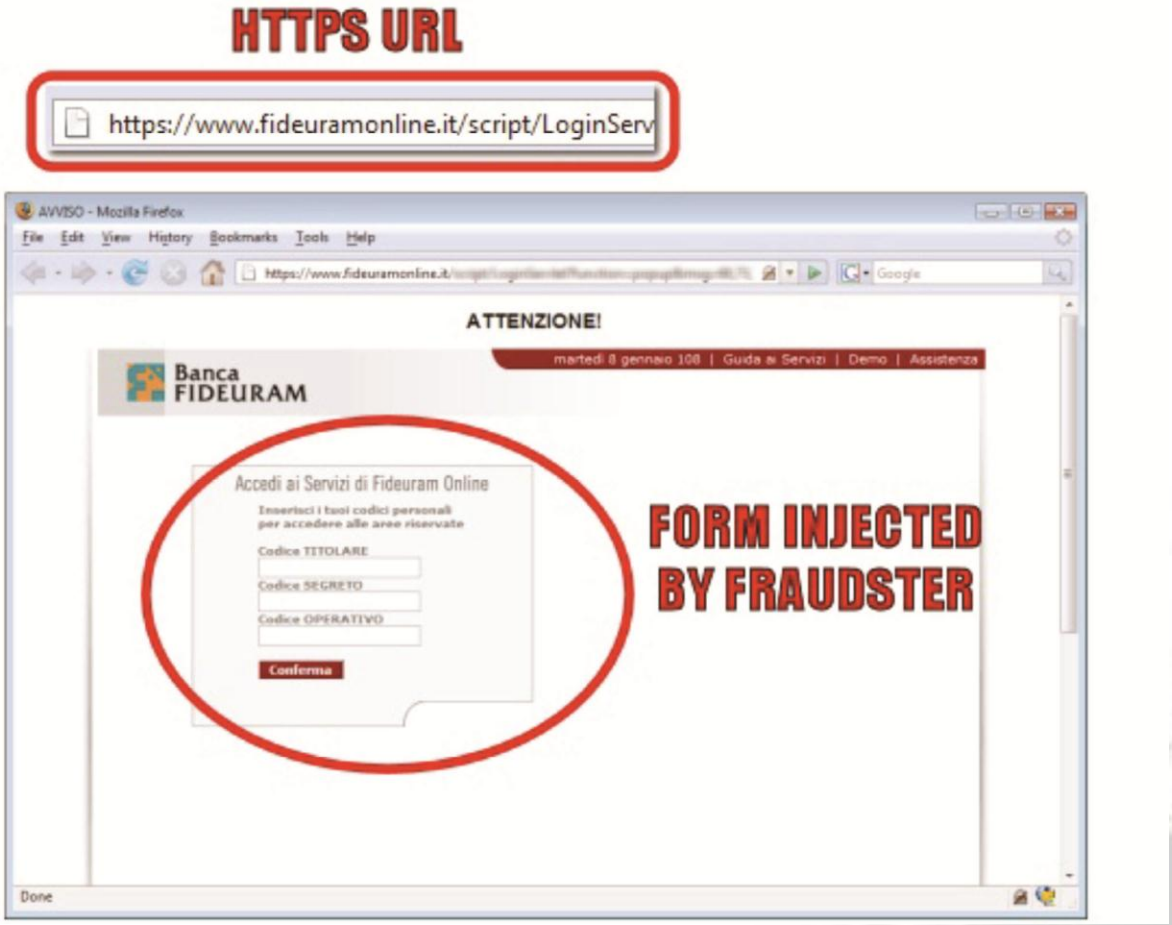
ALEF NULA
DŮVĚŘUJTE SILNÝM



Útok na banku Fideraum

ALEF NULA
DŮVĚŘUJTE SILNÝM

Case Study: Banca Fideuram



Útok na banku Fideraum

ALEF NULA
DŮVĚŘUJTE SILNÝM

Popis útoku

- použití spamu k rozšíření útočníkova skriptu
- nainjektování IFRAME do přihlašovací stránky (+zamlžení injektovaného kódu)
- původní login přepsán útočníkovým loginem
- autentizační údaje odeslány útočníkovi na Taiwanu
- autentizační údaje redirektovány zpět na původní stránky

Rizika

- XSS na „důvěryhodné" stránce, zabezpečené pomocí SSL
- tradiční bezpečnostní informace prohlížeče klamou
    - SSL zabezpečení, SSL certifikát v pořádku
    - adresa v pořádku
- autentizace proběhla v pořádku a oběť nic netuší

Clickjacking

ALEF NULA
DŮVĚŘUJTE SILNÝM

Co je Clickjacking?

- zneužití legitimního formátování webové stránky
- přimění oběti, aby klikla tam, kam potřebuje útočník

Rizika

- vykonání nechtěných uživatelských akcí
- hijacking webkamery/mikrofonu

Clickjacking

ALEF NULA
DŮVĚŘUJTE SILNÝM

Popis útoku, použité techniky

- server pod kontrolou útočníka
- útočník vloží vlastní obsah pomocí tzv. IFRAME HTML tagu
- útočníkův obsah se zobrazí nad obsahem legitimním pomocí z-indexu
- útočník nastaví pro svůj obsah průhlednost na 100%, čímž se stane pro oběť neviditelným