



Towards Impact Assessment Automation for Multi-Stage Cyber Attacks

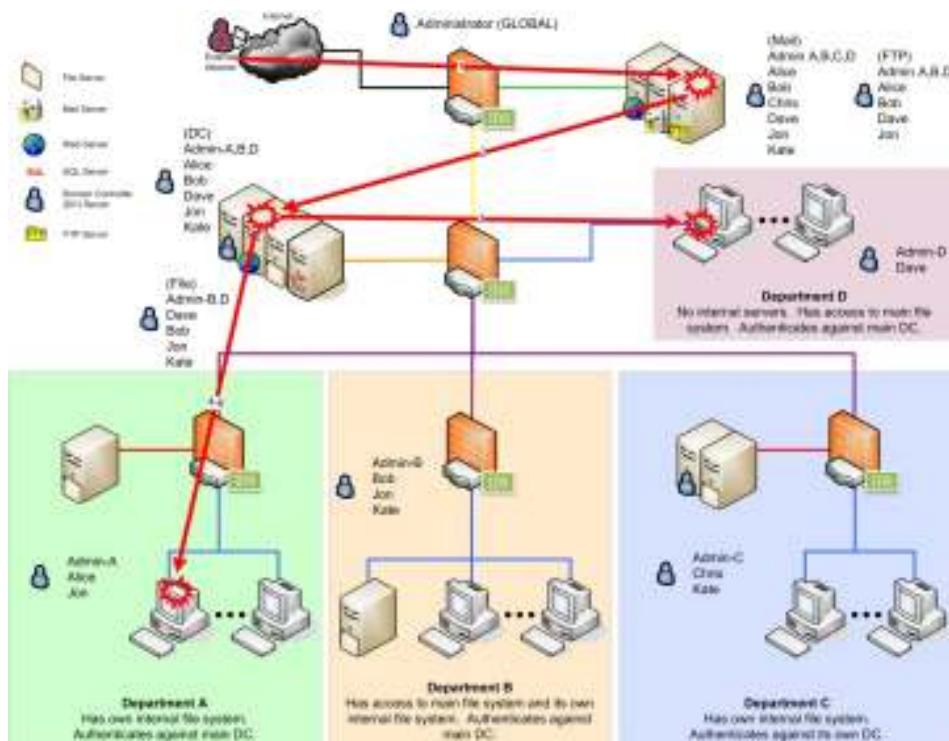
Adam Stotz
Moises Sudit
Jared Holsopple

September 2007

- Introduction/Motivation
- Cyber Attack Background
- Challenges
- Overall Impact/Situation Assessment Framework
 - Virtual Terrain
 - INFERD*
 - TANDI
 - VTAC

- **Computer networks**
 - Can contain sensitive information
 - Can perform critical missions
 - Are constantly targeted by hackers
 - Contain vulnerabilities
- **Hackers**
 - Think “outside the box”
 - Constantly find new ways to attack
 - Vary widely in skill, but even inexperienced hackers can cause damage
- **Many speculate that the next major terrorist attack will be executed via the Internet**
 - At a minimum, critical information and/or missions would be compromised

“Typical” Execution of Cyber Attacks



Originate from one or more computers outside of network

- Attacks originating internal to the network are “insider threats”
- Web servers, FTP servers, VPN servers usually most vulnerable to initial attack

Compromised computers can be used as “stepping stones”

- Detecting attacks
 - Intrusion Detection Sensors (IDS)
 - Analyze network traffic for attack signatures
 - Generate alerts for suspicious traffic
 - Placed throughout network
 - System logs
 - Size can make them unmanageable
 - In-house tools

Analyzing incoming attacks

6/37

- IDS Alerts/Log messages typically presented in spreadsheet format

ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigation	
10316, 1390	Sudden increase of traffic to a port	0.0.0.0	0	0.0.0.0	445	IP	May 3, 2004 6:00:03 AM EDT	NJIT	deimos	Tune	Mitigate
	AAA authorization denied due to no prior authentication	Total: 25									
	AAA authorization denied due to no prior authentication	5.130.120		Total: 3							
	AAA authorization denied due to no prior authentication	5.131.142		Total: 2							
16544, 1390	AAA authorization denied due to no prior authentication	5.136.85	4049	55.128	445	N/A	May 3, 2004 5:40:05 AM EDT	NJIT	cerberus2	Tune	Mitigate
	AAA authorization denied due to no prior authentication	5.136.104		Total: 3							

http://www.cisco.com/application/pdf/en/us/guest/products/ps6241/c1161/cdcont_0900aecd802677aa.pdf

- **Information Overload**
- Automated tool would allow analyst to quickly assess the location and severity of threat

UNCLASSIFIED

Challenges for Automated Impact Assessment

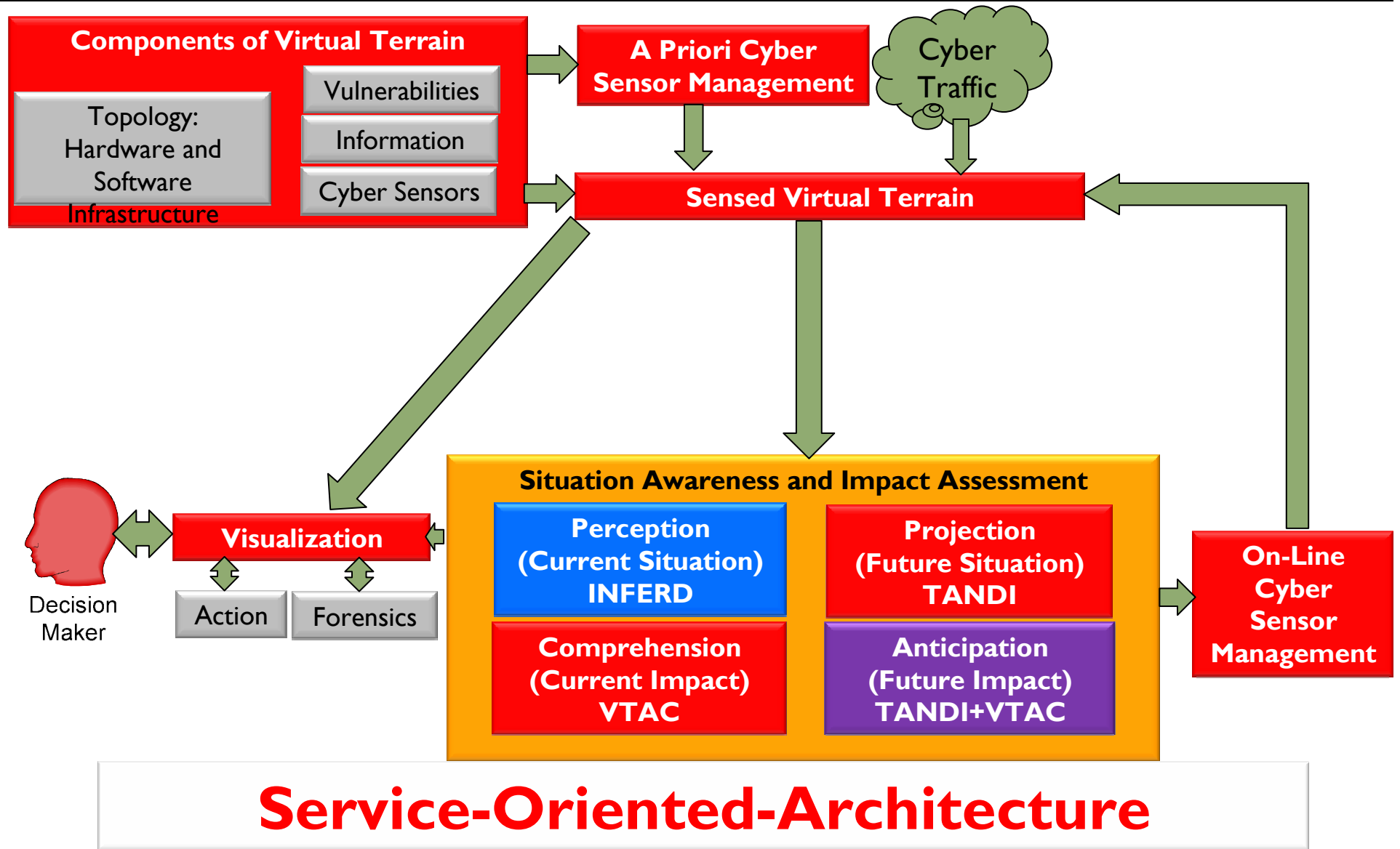
Slide 7

- No “common” representation of a computer network
 - Contextual information (services, operating systems) is valuable for automation
- Lack of Public Data
 - Companies/agencies will not release Cyber Attack data
- Current data
 - Is usually simulated
 - Does not contain important contextual information
 - (Near) complete list of services, operating systems
 - Firewall rules
 - Mission information

UNCLASSIFIED

Overall Architectural Vision

Slide 8



UNCLASSIFIED

INFERD Design

- **Hierarchical Fusion Framework**

- Allows for bottom-up and top-down information analysis
- Multiple levels of aggregation

- **Operational and Computational Efficiencies**

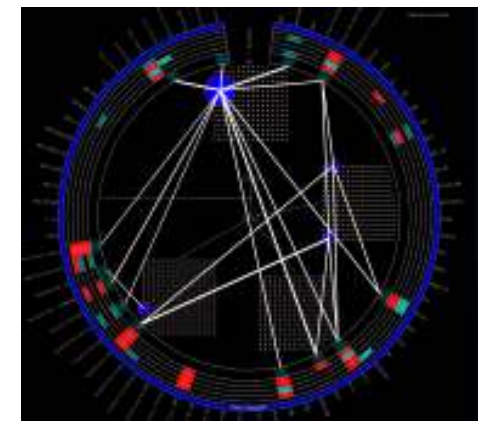
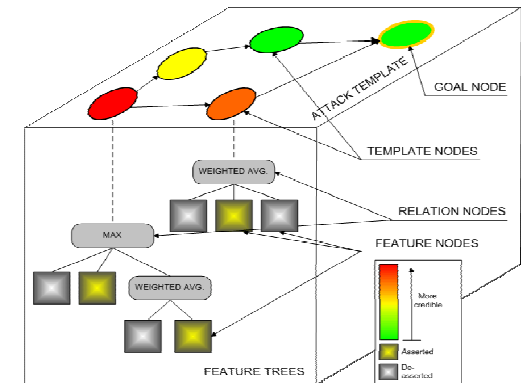
- Minimize *a priori* knowledge
- Distributed Architecture makes System Scalable to Varying Size Networks
- System performs streaming on-line processing
- Exact amount of information (no more and no less) at each stage of decision-making

- **Human-in-the-loop drives Fusion Process**

- Avoid the overflow of raw data and maximize relevant information/knowledge
- Situational Assessment (what is happening?) - ECCARS
- Impact Assessment (what could happen?) – Future Programs

- **Interoperability with other Systems**

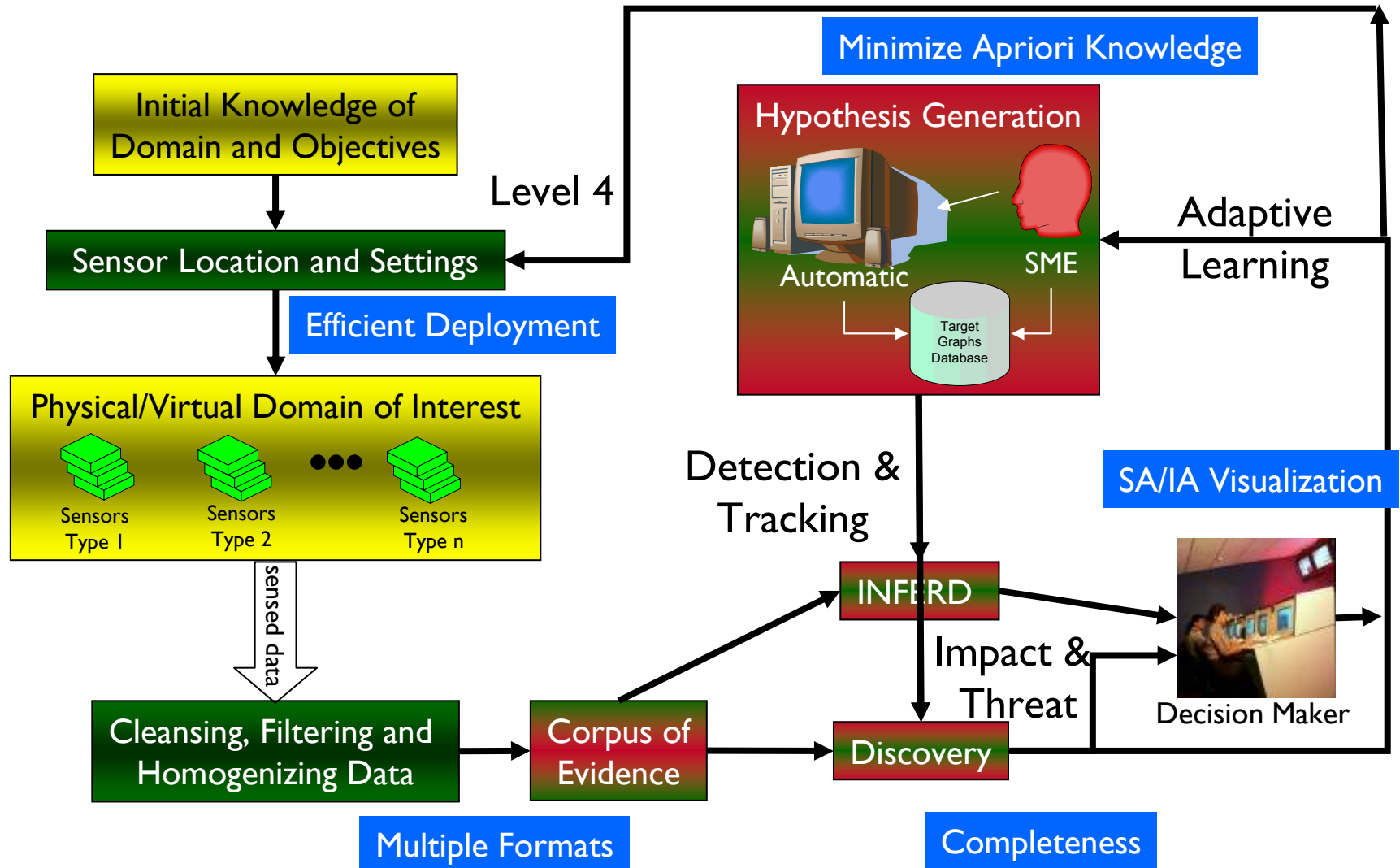
- General Visualization Interface
- Input interface for multiple sensor types & formats
- Connectivity to Forensics for Adaptive Learning



UNCLASSIFIED

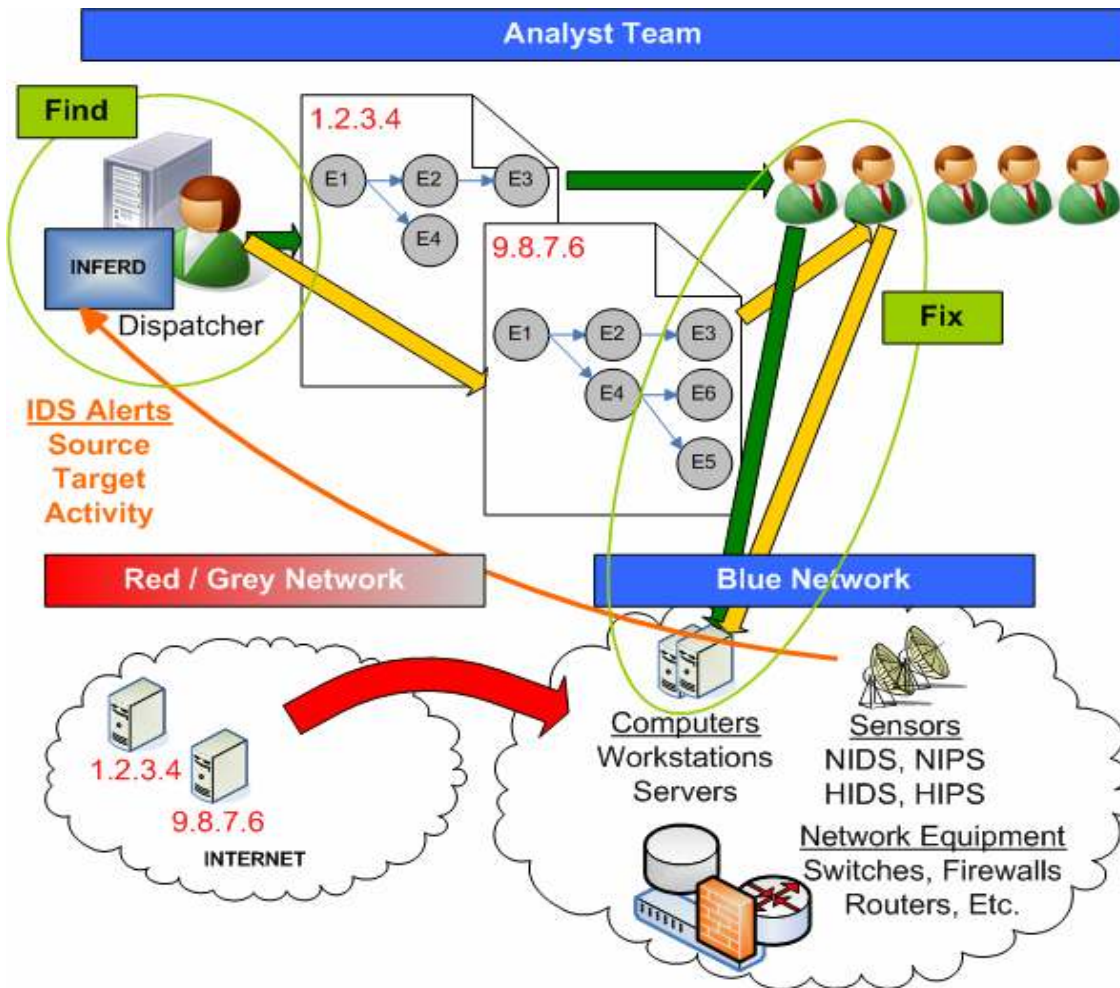
Introduction and Motivation

10

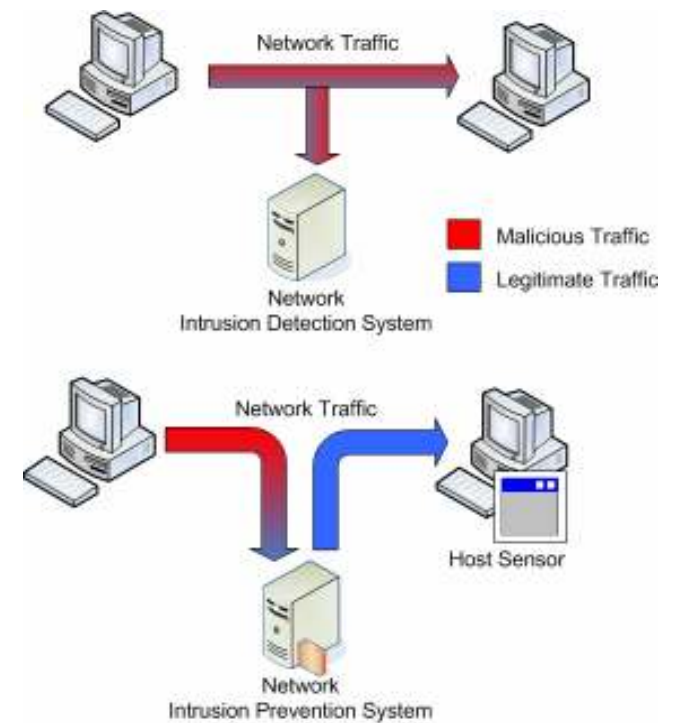


UNCLASSIFIED

Cyber Kill Chain

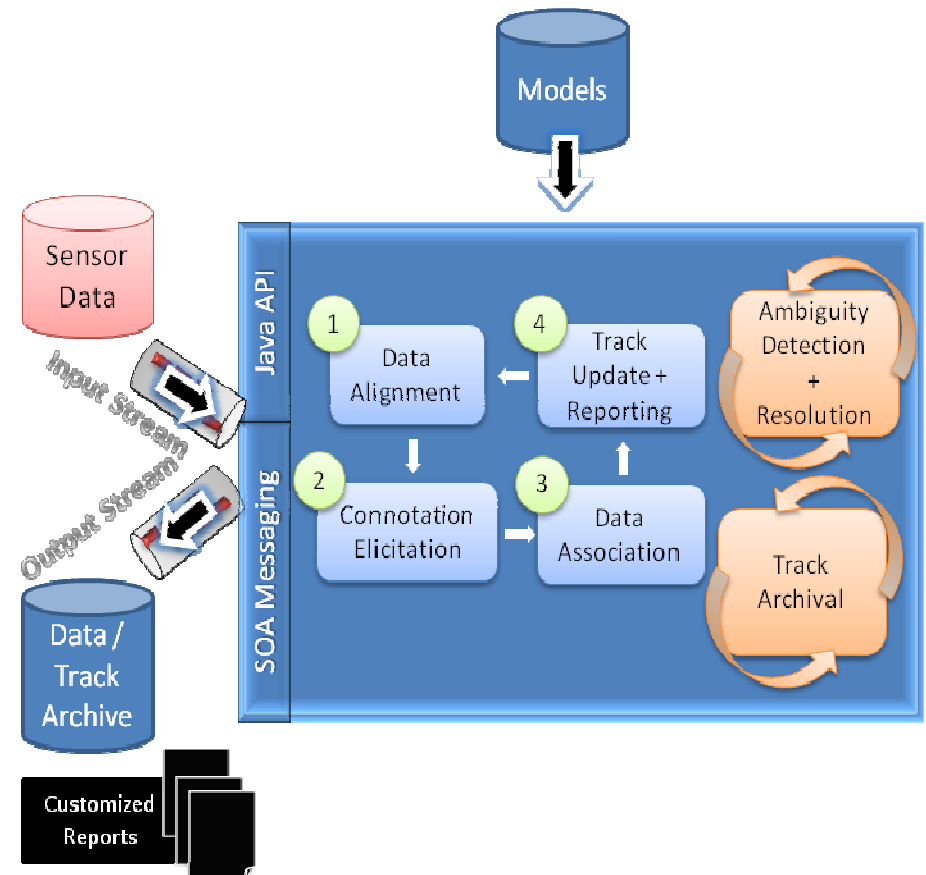


Detection vs. Prevention



INFERD Architecture

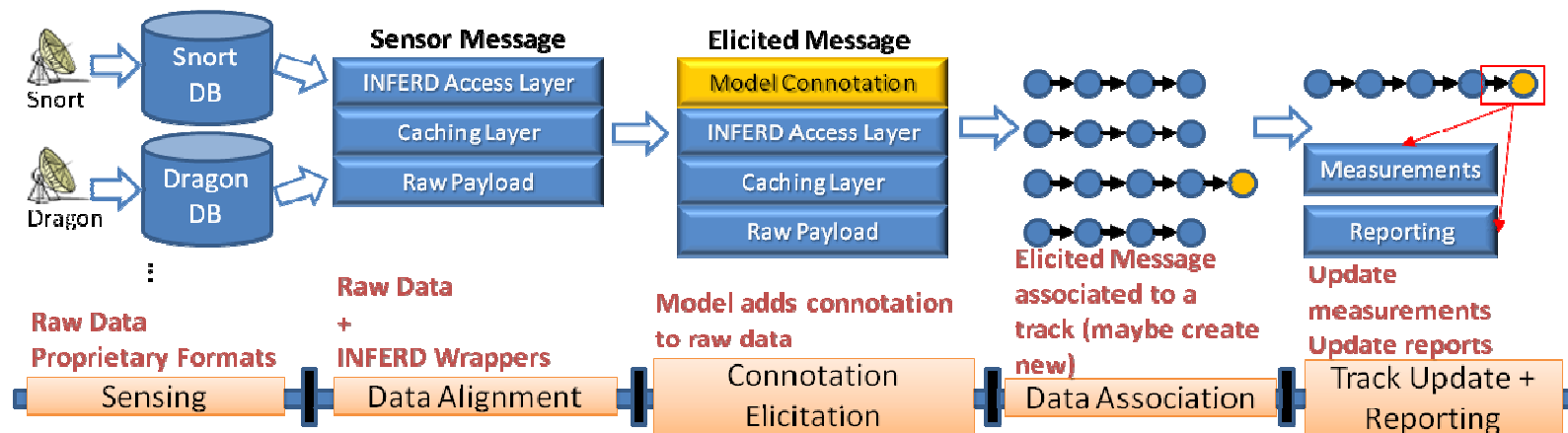
- Designed for stream-based tracking of *non-traditional* sensed events
 - non-traditional = sensor observations other than position/velocity on physical moving targets
 - *Context* plays an important role
- Accomplished by 6 main processing modules
 - **Data Alignment** 1
 - **Connotation Elicitation** 2
 - **Data Association** 3
 - **Track Update + Reporting** 4
 - **Ambiguity Detection and Resolution**
 - **Track Archival**



■ New tracking process stage necessitated by non-traditional data

■ Present in traditional tracking systems

- **Sensing**
 - Input: Network / host activity
 - Process: Cyber IDS(s) calculate anomalous or malicious patterns/signatures
 - Output: Alerts in their own heterogeneous formats in distributed network locations
- **Data Alignment**
 - Input: Heterogeneous / distributed alert data bases
 - Process: Ingests the heterogeneous / distributed alerts via network messaging services and provides a common access language for the INFERD fusion models to leverage
 - Output: Sensor Message = the alert with homogenized data access layer
- **Connotation Elicitation**
 - Input: Sensor Message
 - Process: Fusion model applies a contextual model-based understanding to the Sensor Message
 - Output: Elicited Message = Sensor Message with added model-based meaning
- **Data Association**
 - Input: Elicited Message
 - Process: Uses elicited information to associate the Elicited Message with information track(s) of relevance. Relevance determination is model defined.
 - Output: Information Track(s) of relevance
- **Track Update + Reporting**
 - Input: Elicited Message + Relevant Information Tracks
 - Process: Updates track structure with newly associated information. This update is model based.
 - Output: Report updates to publish to INFERD clients.



Sample Cyber Model

1. Multi-layer definition tying fusion process to specific fusion problem environments.
2. Defines how dynamic hypotheses are generated from data stream and what their content will be.

- **Events of Interest (Eoi)**

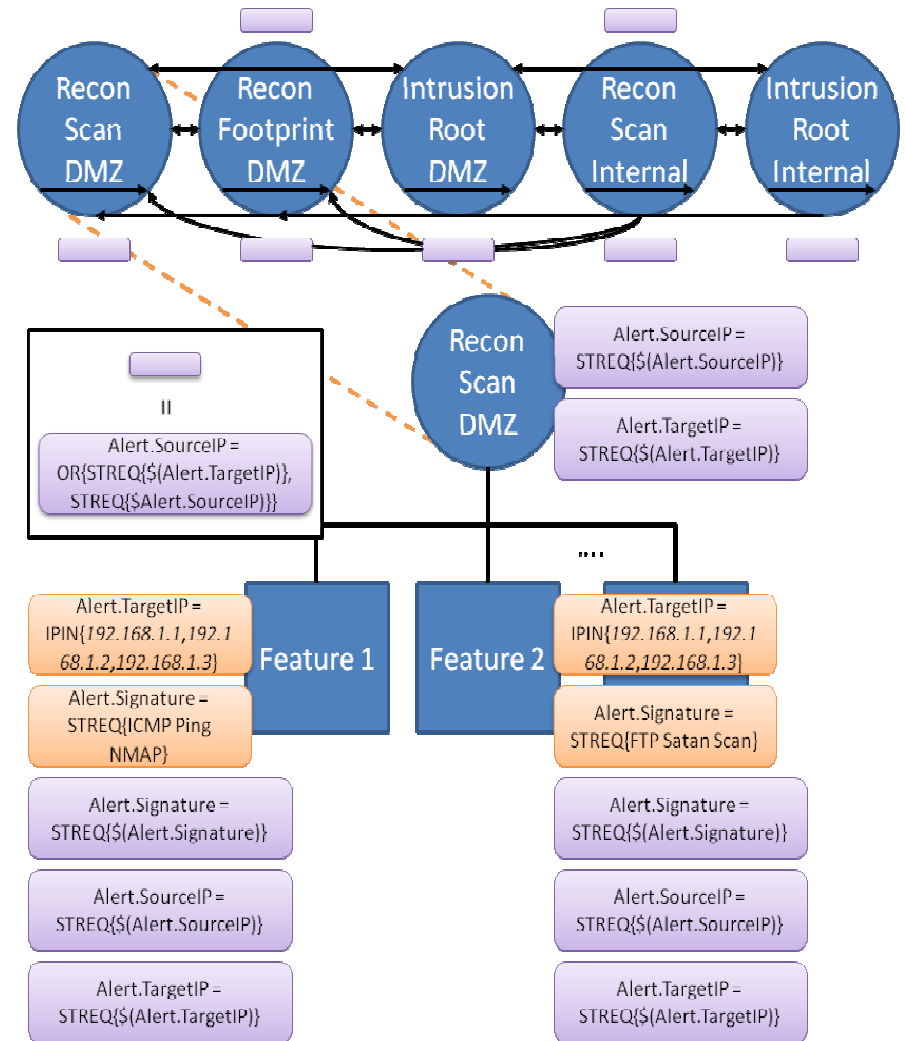
- Events INFERD will elicit from input data stream
- Each Eoi is composed by a set of *Features*
- E.g. Eoi's:
 - Recon Scan DMZ
 - Recon Footprint DMZ
 - ...

- **Features**

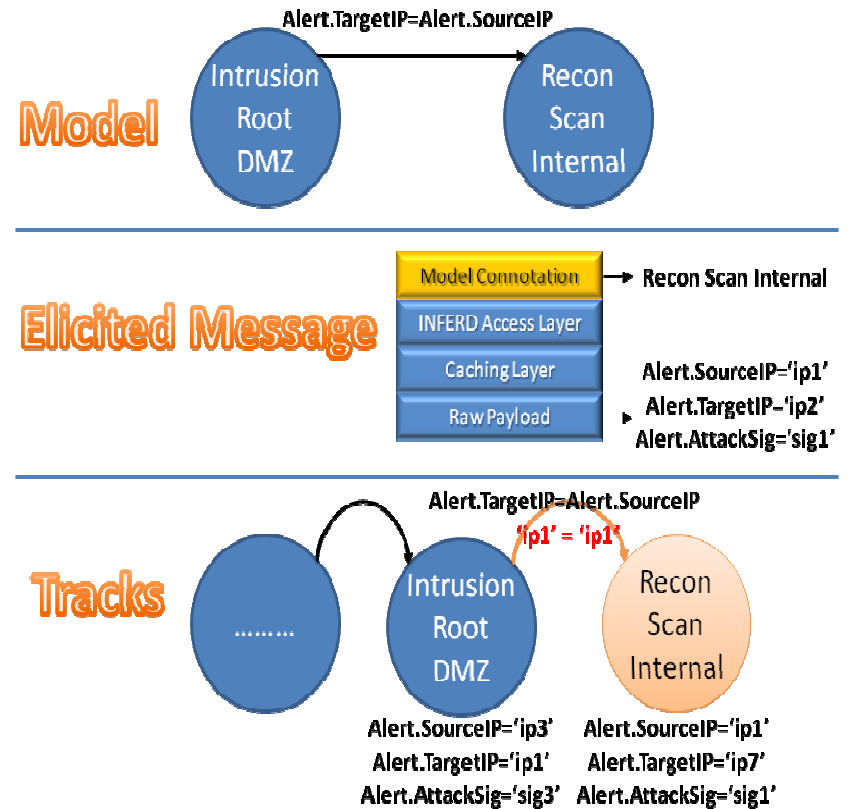
- Define *constraints* which when satisfied by the input data stream, assert the hypothesis that an Eoi has occurred
- E.g. Features:
 - Feature 1
 - Feature 2
 - ...

- **Constraints**

- Static or dynamic
- Can reference values within or between Sensor Messages and Information Tracks

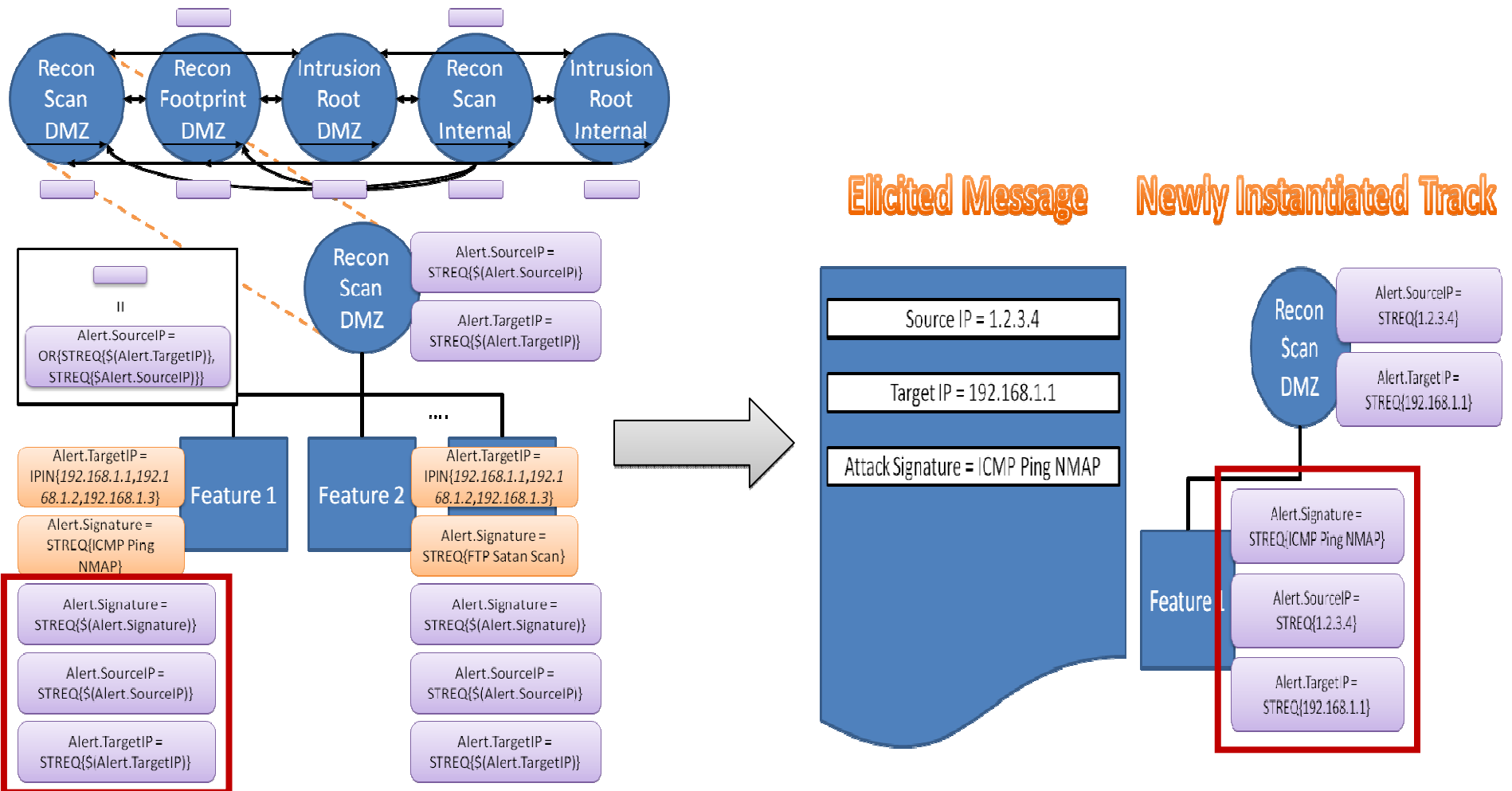


- Model defines relation between *Intrusion Root DMZ* and *Recon Scan Internal*
 - “If target IP of hypothesized attack in DMZ = source IP of hypothesized attack in internal network than the 2 events are related”
- Model also defines Feature constraints which instruct Connotation Elicitation module to see the alert as a *Recon Scan Internal* (Feature and constraints not shown)
 - “If Attack Signature = sig1 and Target IP = ip2 Then event is a Recon Scan Internal”
- Data Association module sees that the newly hypothesized *Recon Scan Internal* attack satisfies the relation constraint defined above so reports the track as relevant
 - “Since source IP of Recon Scan Internal attack = target IP of Intrusion Root DMZ attack, the attacks are related.”



Track Update Example

- Dynamic variables take on values during track update



Benefits of INFERD to the Analyst

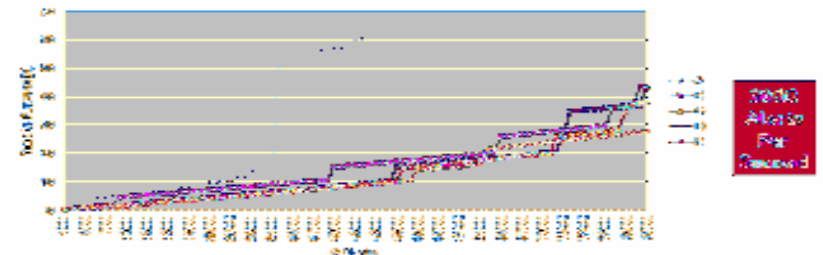
- Near “real-time” detection of cyber attacks
 - System runs at real-time for the AFRL DIW network
 - Scalable to larger networks
- Perception and Comprehension of complex coordinated attacks
 - INFERD fuses alerts into dynamic attack tracks
 - Attack tracks provides Situational Awareness (SA) to analyst
 - Ranking measurements filters hypotheses of interest (Depth, Abnormality, Others)
 - Abnormality and Defragmentation Handlers aid in Comprehension of SA
- Minimize requirement of a-priori knowledge
 - Guidance Templates (models) guide dynamic attack track creation
 - Model flexibility enables new hacker behavior and sensor accommodation
- Interoperability with third-party providers
 - DAO allows for interoperability without sacrificing real-time performance
 - Easy to interface with visualization (Flexviewer) or forensics (TMODS)
- Designed to be extendable for growth of capabilities and applications
 - Automatic Knowledge Reasoning: Pedigree, Discovery and/or Conflict Resolution
 - System Need NOT BE IDS-Centric
 - Impact Assessment or Prediction of Adversary Behavior
 - Process Refinement or Sensor Management
 - Other domains: Asymmetric warfare, Disease Surveillance, IED Detection, etc.

Performance Evaluation and Metrics

- **Confidence:** correctly identify the situation(s)
- **Recall:** Activities detected in relation to the “total known”
- **Precision:** Activities detected in relation to number of detections
- **Fragmentation:** Activities reported as multiple s that should have been singleton
- **Mis-Association:** Activities reported as a singleton that should have been multiple
- **Purity** – characterizes the quality of the detections
- **Mis-Assignment Rate:** Evidence incorrectly assigned to a given activity
- **Evidence Recall:** Evidence detected in relation to the “total known”
- **Cost Utility** – measure of the system in identifying “important” situations
- **Weighted Cost:** Total available cost achieved savings by the system
- **Attack Score:** Attacks identified and where they appear in the proposed list
- **Timeliness** – measures the ability of the system to respond within time requirements of a particular domain

	Threshold	BT#2-4s5	BT#2-4s6	BT#2-4s8	BT#2-4s16	BT#2-4s17
Recall	0.00	97.70%	92.50%	95.80%	88.20%	87.30%
	0.25	92.80%	83.60%	89.40%	78.60%	72.90%
	0.50	92.40%	83.00%	86.30%	76.90%	72.40%
	0.75	92.00%	83.00%	84.20%	76.90%	72.40%
	0.95	91.30%	82.40%	82.70%	76.40%	72.40%
Precision	0.00	100.00%	94.20%	89.50%	96.20%	92.90%
	0.25	94.90%	85.30%	83.60%	85.70%	77.60%
	0.50	94.60%	84.60%	80.60%	83.80%	77.10%
	0.75	94.20%	84.60%	78.60%	83.80%	77.10%
	0.95	93.40%	84.00%	77.30%	83.30%	77.10%
Fragmentation	0.00	0.00%	5.10%	10.50%	3.30%	7.10%
	0.25	0.00%	1.30%	5.90%	4.30%	0.60%
	0.50	0.00%	1.30%	1.30%	0.50%	0.00%
	0.75	0.00%	0.00%	0.30%	0.00%	0.00%
	0.95	0.00%	0.00%	0.00%	0.00%	0.00%
Mis-Association	0.00	0.00%	0.00%	0.00%	0.00%	0.00%
	0.25	5.10%	12.80%	10.50%	9.50%	21.80%
	0.50	5.40%	13.50%	18.10%	15.20%	22.90%
	0.75	5.80%	14.70%	21.10%	15.70%	22.90%
	0.95	34.20%	57.90%	59.60%	86.80%	50.60%

	Threshold	BS#2-4s5	BS#2-4s6	BS#2-4s8	BS#2-4s16	BS#2-4s17
Miss Assignment	0.00	2.80%	26.80%	12.20%	82.80%	28.70%
	0.25	3.20%	25.30%	9.70%	84.60%	35.00%
	0.50	3.10%	23.40%	15.30%	87.20%	35.10%
	0.75	3.10%	32.10%	21.10%	87.30%	5.00%
	0.95	3.30%	32.50%	22.30%	87.50%	5.00%
Evidence Recall	0.00	35.90%	13.10%	28.30%	20.50%	13.50%
	0.25	98.60%	89.30%	54.00%	72.60%	99.40%
	0.50	99.20%	90.60%	80.30%	98.60%	99.80%
	0.75	99.70%	99.60%	98.80%	99.50%	100.00%
	0.95	100.00%	100.00%	100.00%	99.80%	100.00%



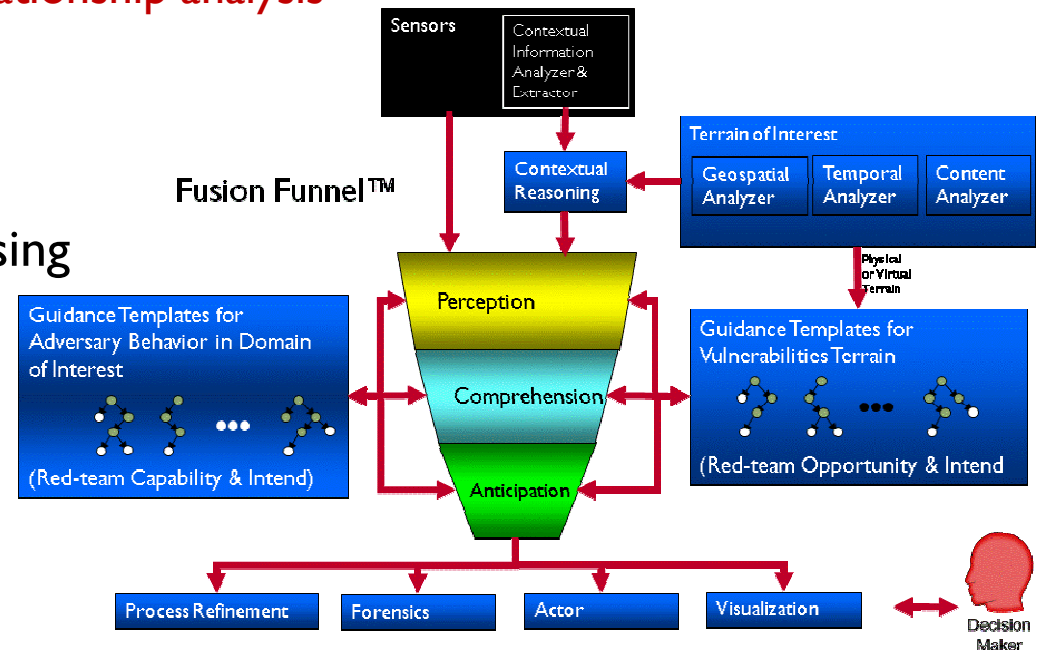
Scenario	Classification	Detection	Elimination	Algorithm	Time	Miss	Timeliness
A	AD1	AD1	AD1	AD1	AD1	AD1	AD1
B	AD2	AD2	AD2	AD2	AD2	AD2	AD2
C	AD3	AD3	AD3	AD3	AD3	AD3	AD3
D	AD4	AD4	AD4	AD4	AD4	AD4	AD4
E	AD5	AD5	AD5	AD5	AD5	AD5	AD5

Conclusions

- Does not require network information
 - Robust to changing network configurations
 - Prone to false positives from sensors
 - Easy to configure and install on networks of any size/shape
- Can provide network assessment in real-time
 - Gives security analyst a chance to react to critical multi-stage attacks
 - Does not perform complex relationship analysis

Future Work

- Add subsequent layered processing to include detailed network information when available
(Comprehension)
- Predict future attack vectors
(Anticipation)



Virtual Terrain (Network Representation)

Slide 21

- Infrastructure Topology

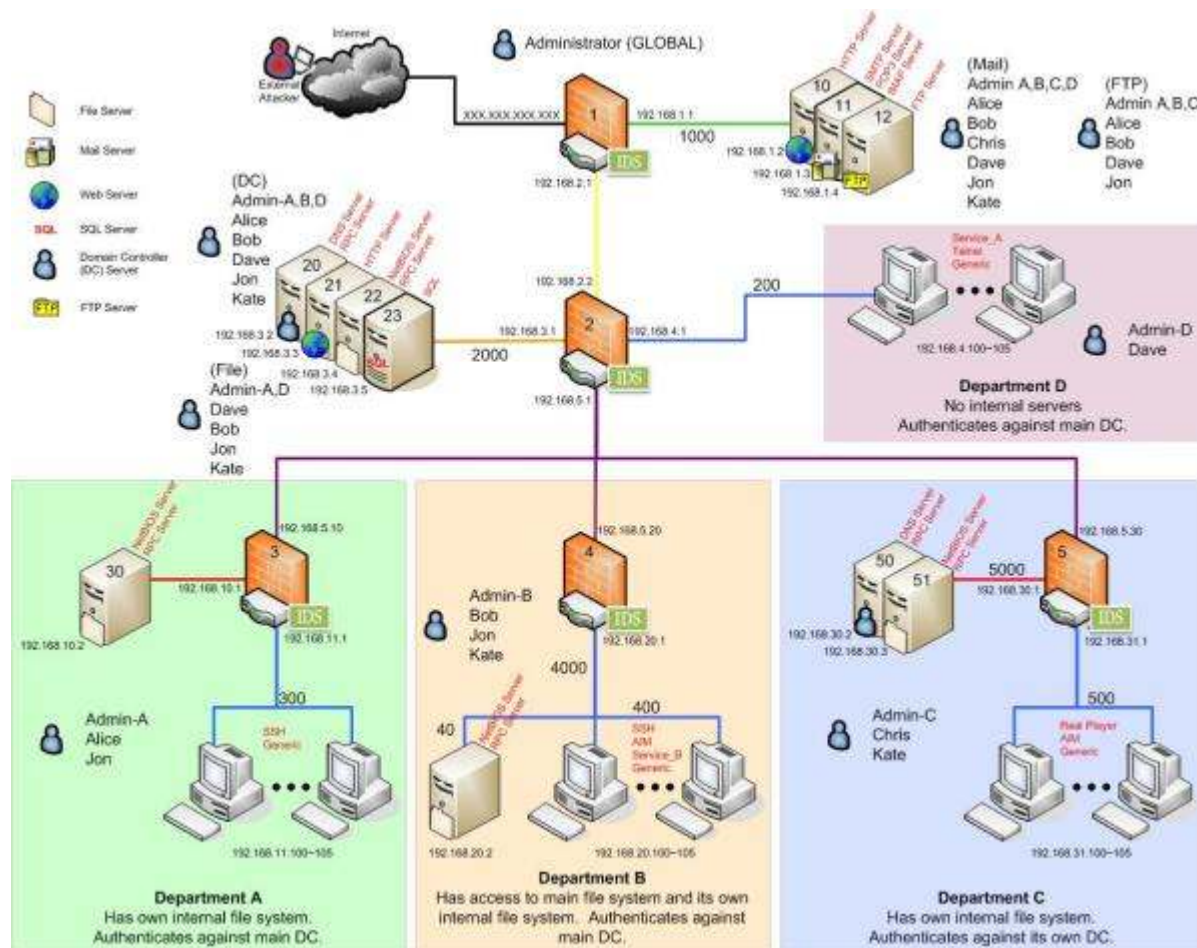
- Hardware
- Software
- Connectivity

- Information

- Privileges
- Location
- Criticality
- User, etc.

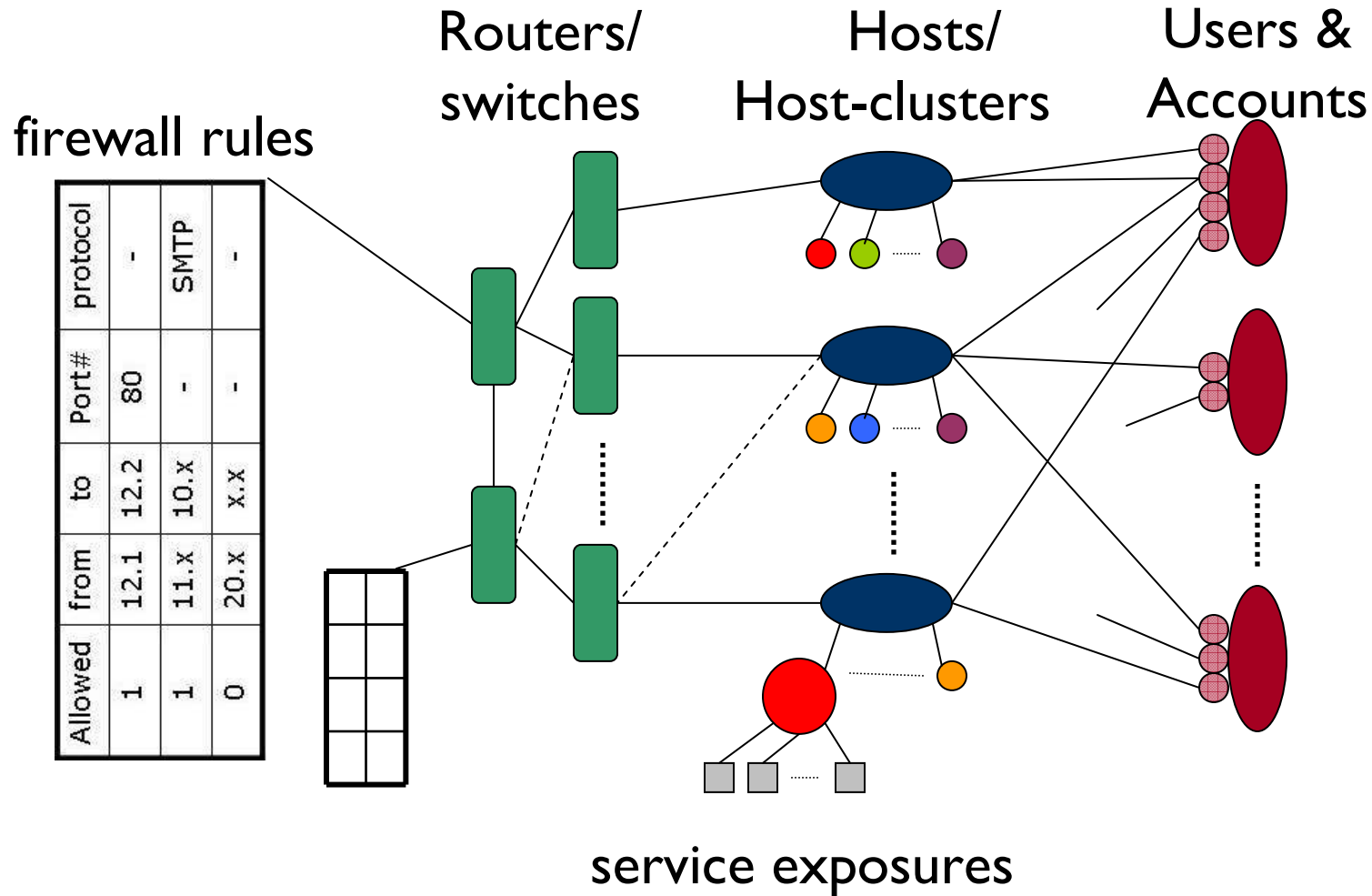
- Cyber Sensors

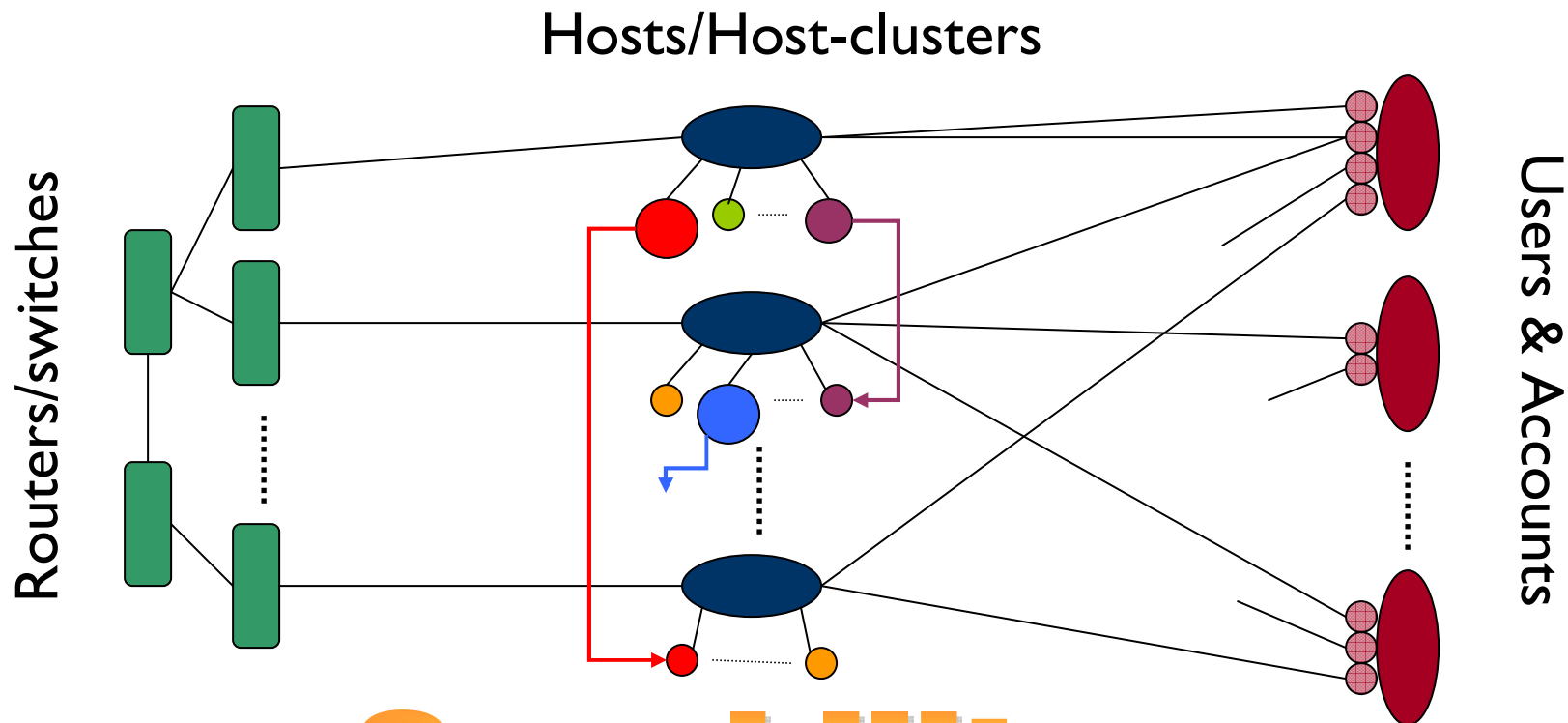
- Type,
- Location,
- Pedigree, etc.



UNCLASSIFIED

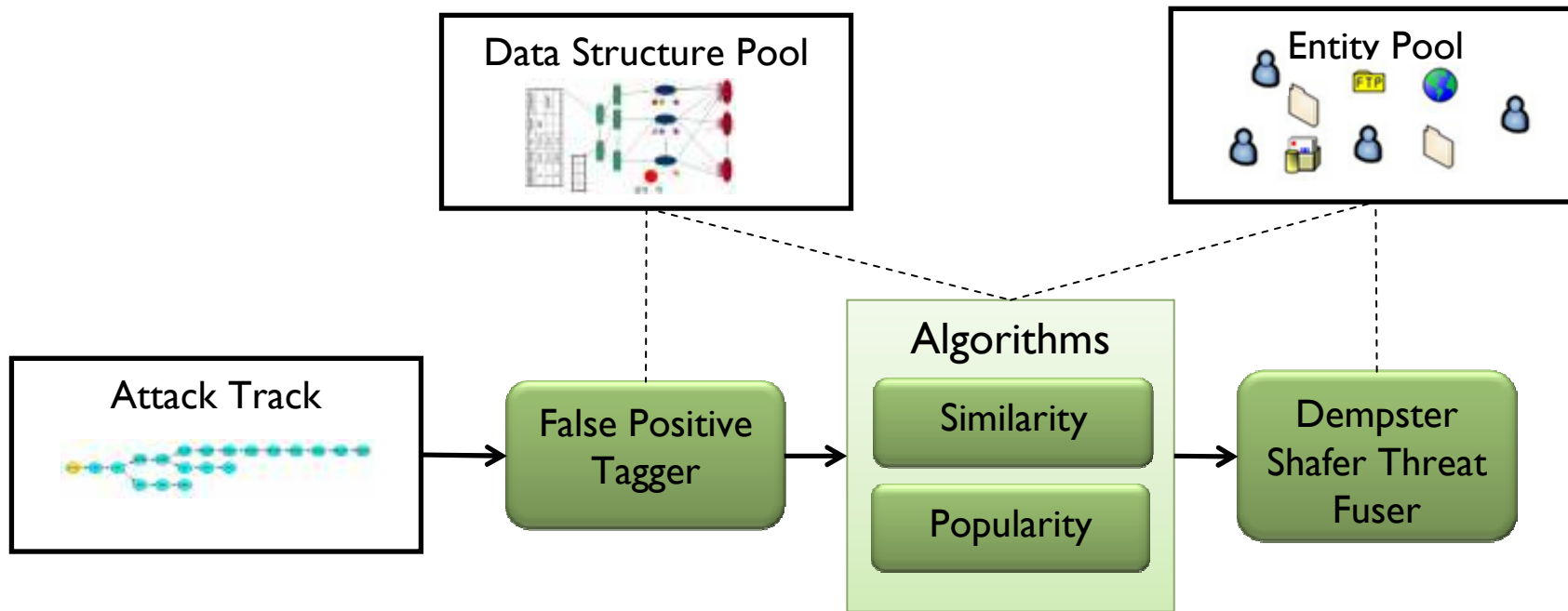
Virtual Terrain (VT) Definition





Hosts connected to the network via their capability are

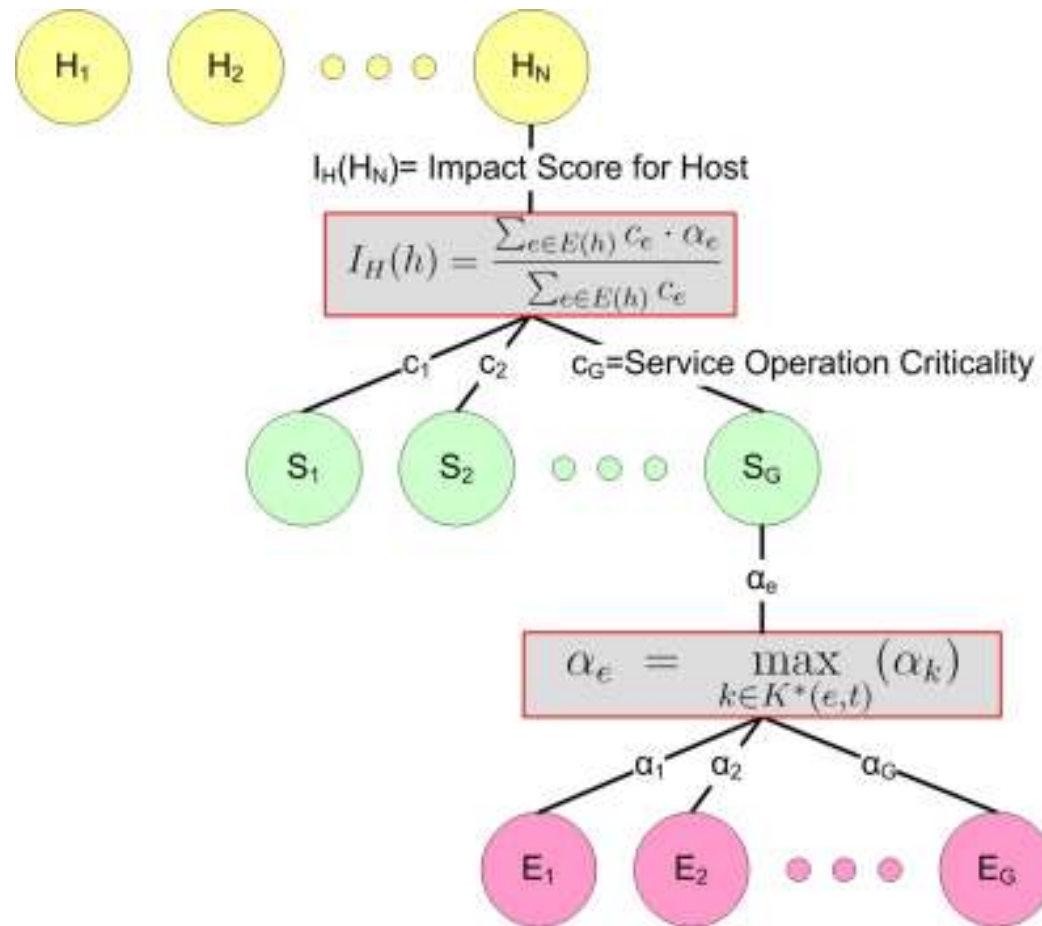
- Firewall and permission rules exposed; threat accounts and privilege rules define potentially threatened hosts
- define a dynamic neighbor list for each attacked host



- Domain independent implementation
- Data structures provide contextual information
- Algorithms provide different perspectives of analysis
- Multiple threat scores on an entity are fused using Dempster-Shafer

VTAC: Virtual Terrain Assisted Impact Assessment for Cyber Attacks

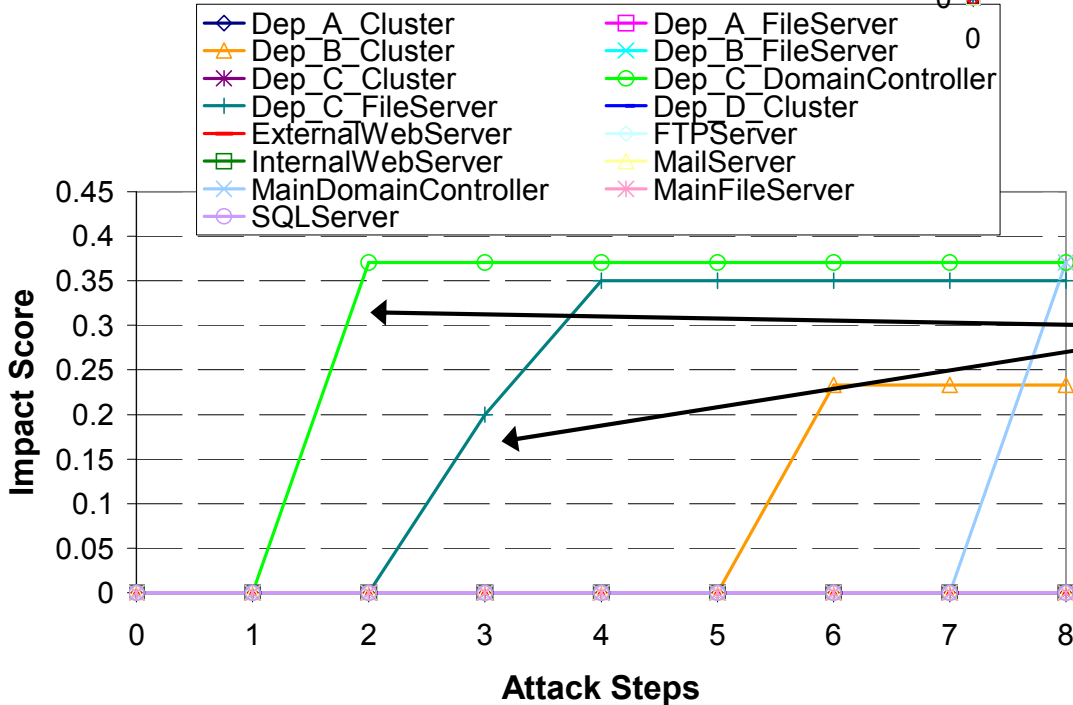
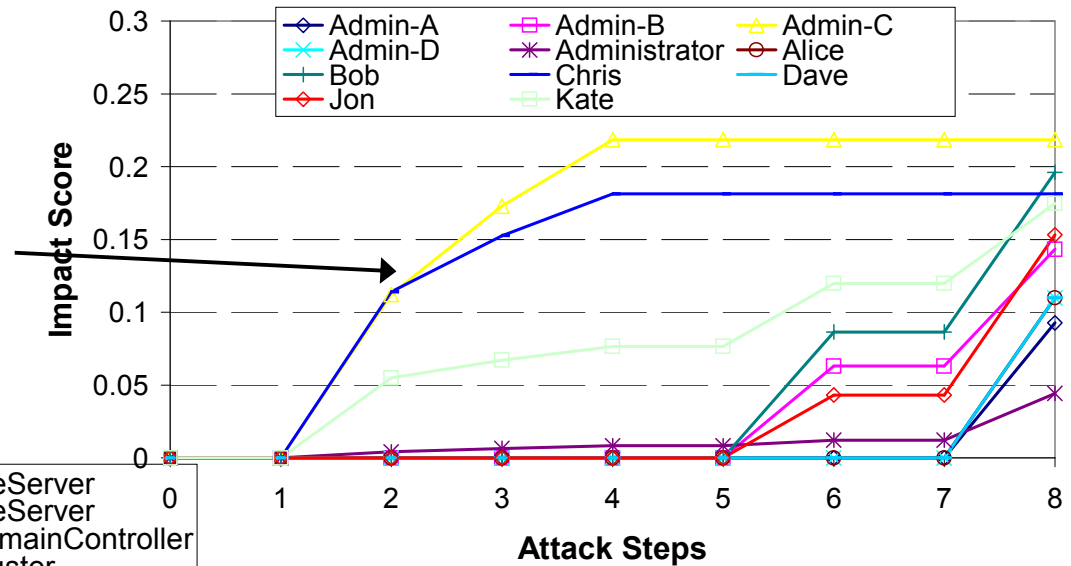
- Can calculate impact for hosts, services, users, network



UNCLASSIFIED

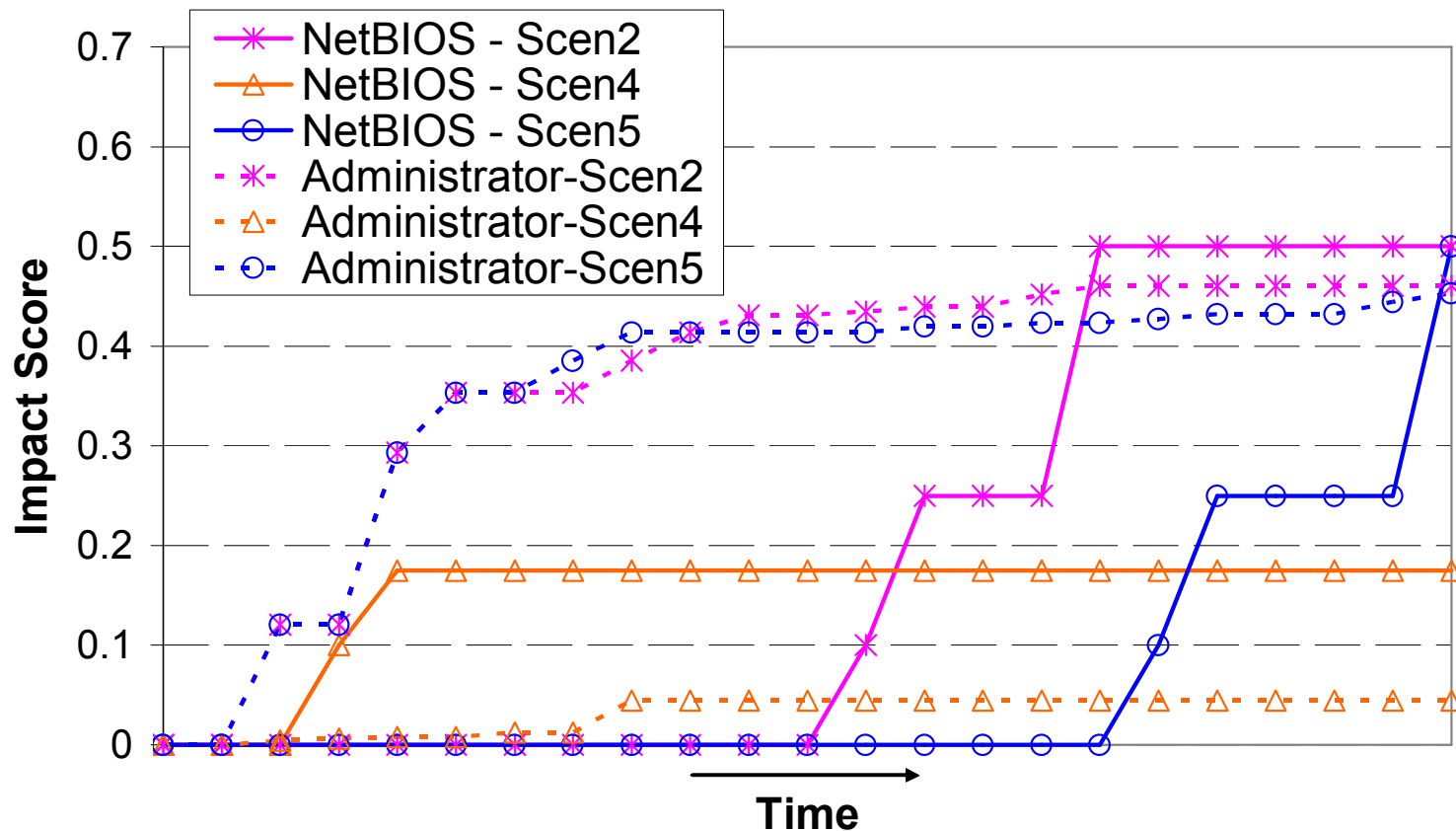
Insider Attack

Initial IU to peak is not administrator



Inside machines affected before external server subnets being impacted

Attack Track Ranking



- Future Work
 - Refine INFERD
 - Refine TANDI algorithms
 - Integrate TANDI/VTAC for current and future impact
- Automated impact assessment
 - Is necessary to improve an analyst's view of the situations
 - Should allow the analyst to be the final decision-maker
 - Requires better network service technology to be truly effective