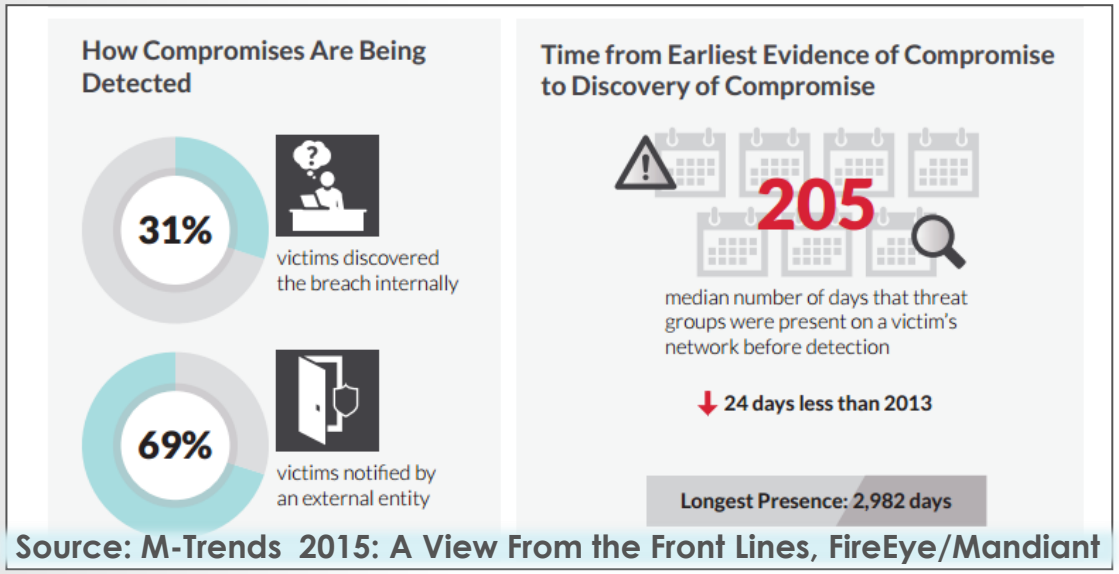
Integrated Adaptive Cyber Defense: Integration Spiral Results

Wende Peters, JH-APL
wende.peters@jhuapl.edu
iacd@jhuapl.edu
September 2015

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

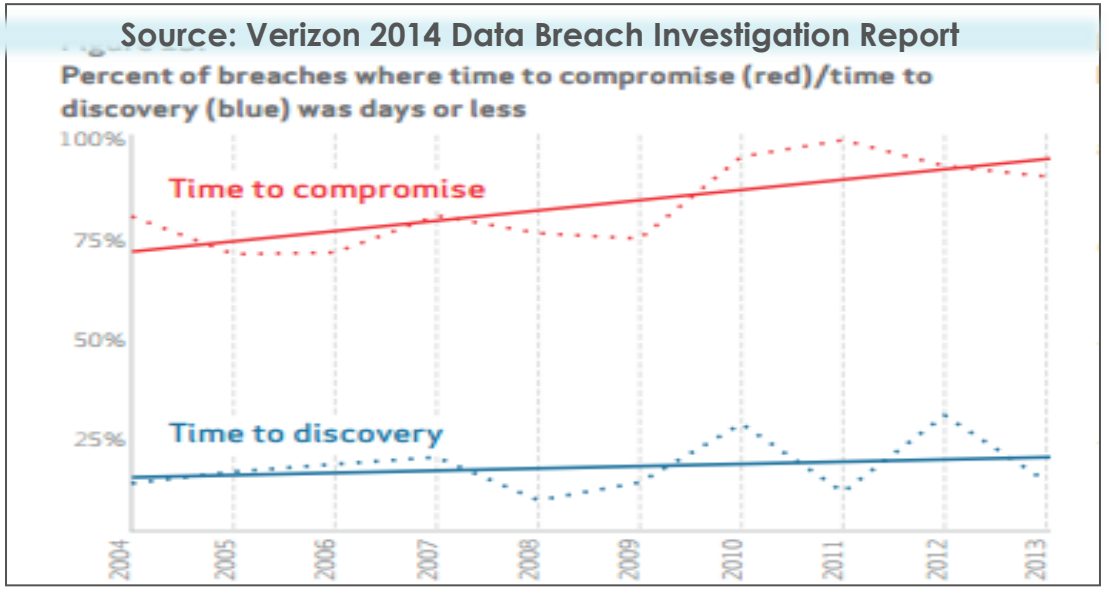
Cybersecurity Reality in the Greater Cyber Ecosystem



Source: M-Trends 2015: A View From the Front Lines, FireEye/Mandiant

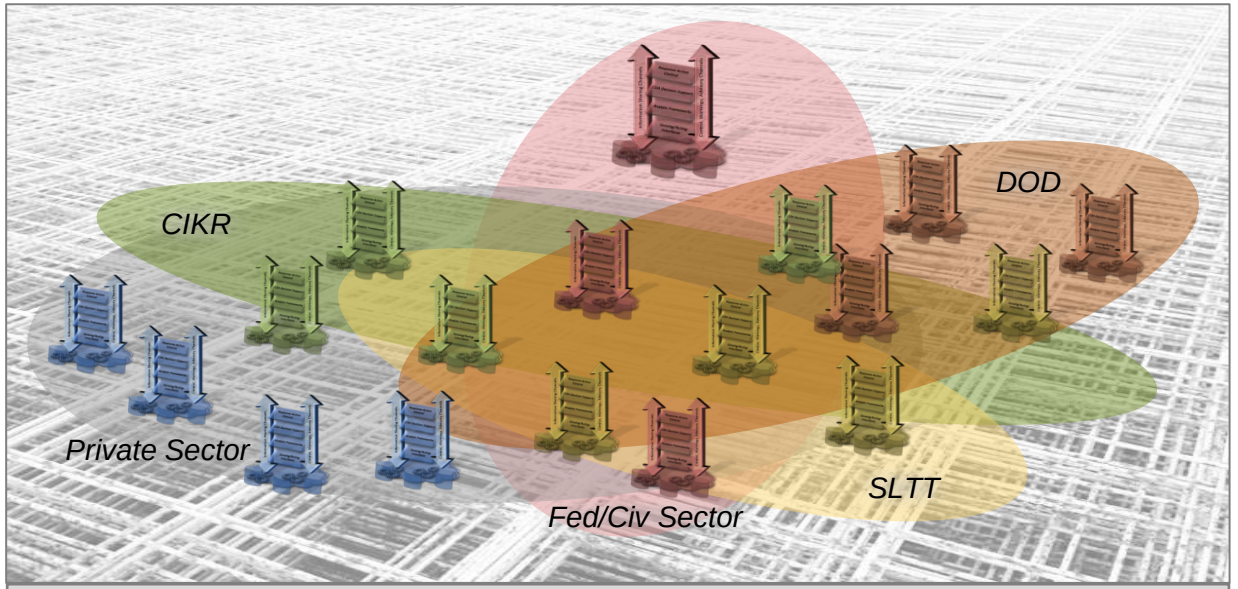
We aren't controlling the space or the outcomes

We're getting worse at this



What Does Success Look Like?

Secure integration and automation across a diverse, changeable array of cyber defense capabilities



National	Coordinate National-level operations and support cross-enterprise cyber response
Regional	Enable collaborative, 'beyond-line-of-sight' defense
Local	Enable participants to defend themselves

What Does Success Look Like?

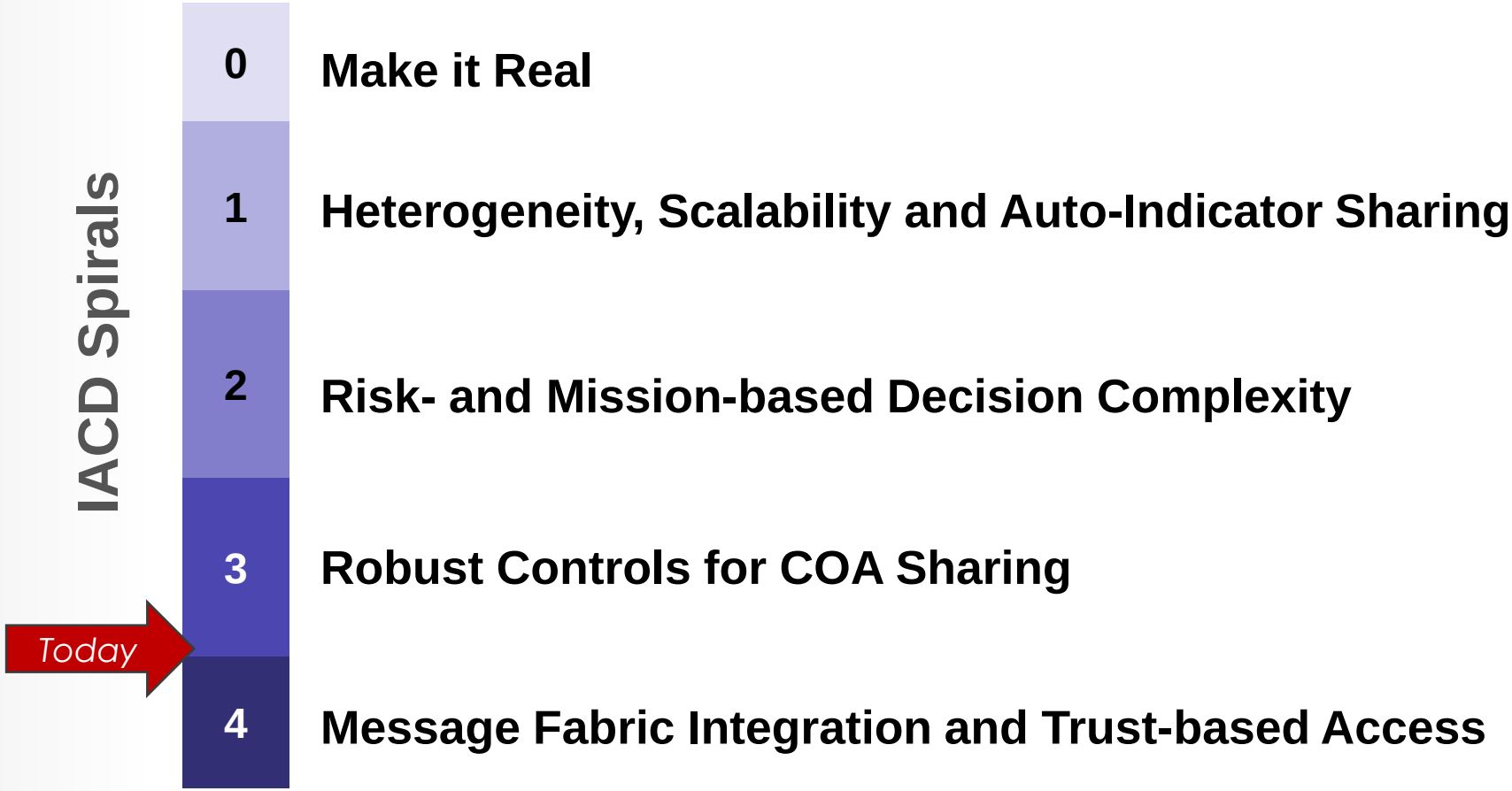
Secure integration and automation across a diverse, changeable array of cyber defense capabilities

- Dramatically change timeline and effectiveness
- Enable consistent effects in cyber-relevant time
- Provide operational and acquisition freedom to take advantage of advances
- Support use of existing and emerging standards to enable commercial-based solutions
- Ensure control and action that can be achieved under network owners' authorities and capabilities

Integrated Adaptive Cyber Defense (IACD) is our initiative to address these challenges

IACD Spiral Approach

Using an Agile Approach – Requirements and Capability ***Elicitation*** and Efficiency and Security Improvement ***Demonstration***

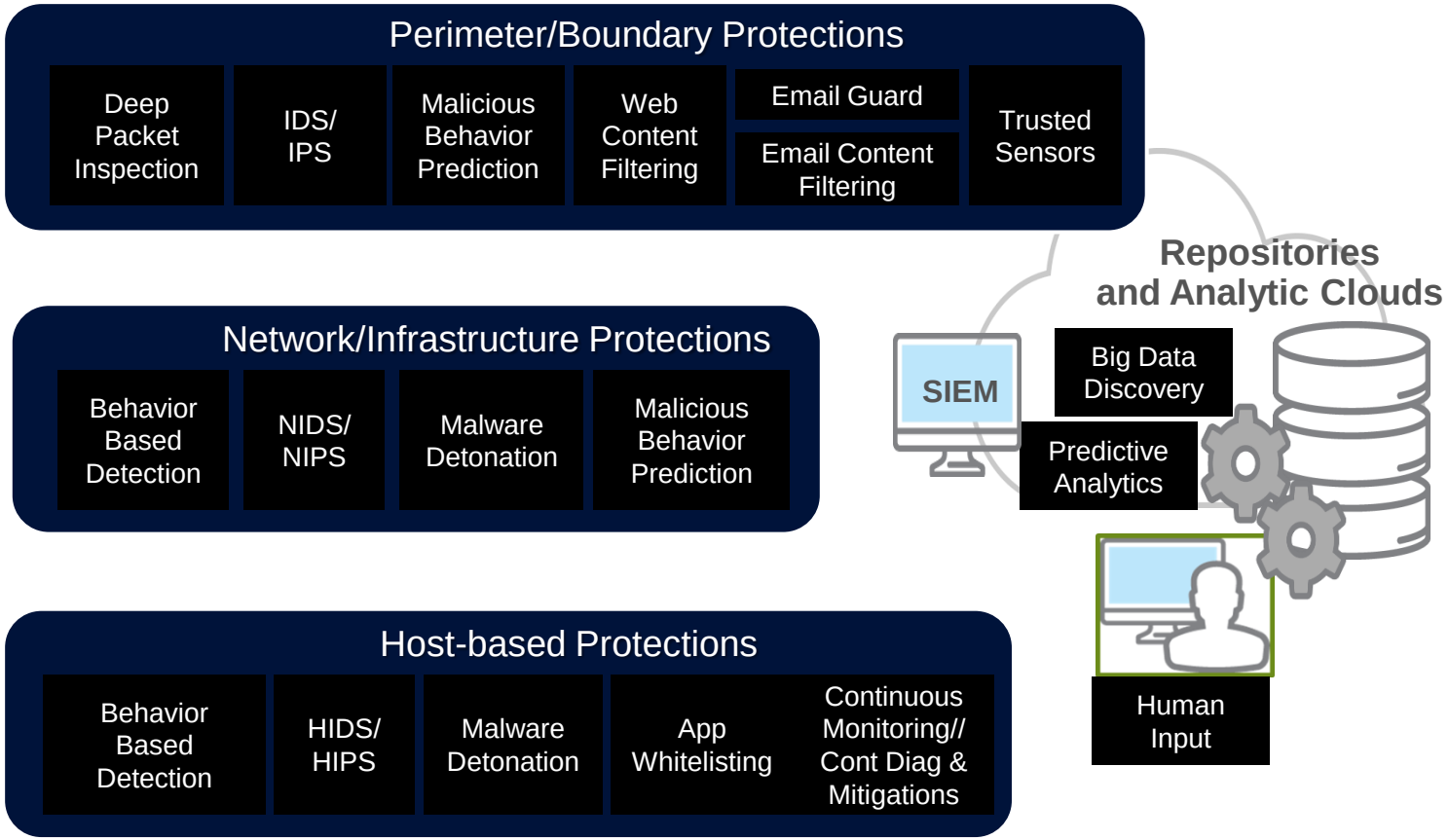


First: Every Defender Brings Their Own Enterprise

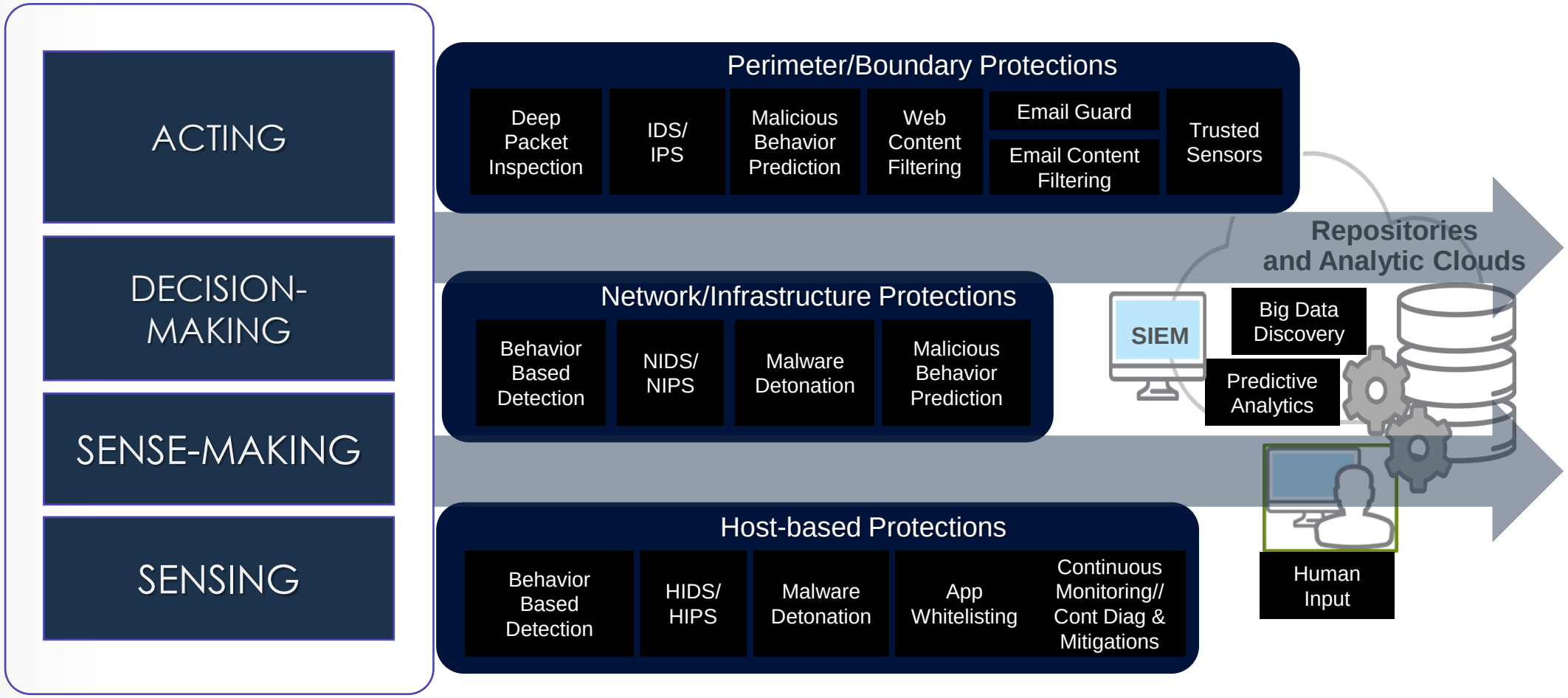
Their own profile, priorities, capabilities, and risk tolerance

How do we maximize the effectiveness of our current and future cyber defense capabilities?

How do we interconnect our capabilities to 'move left of boom'?

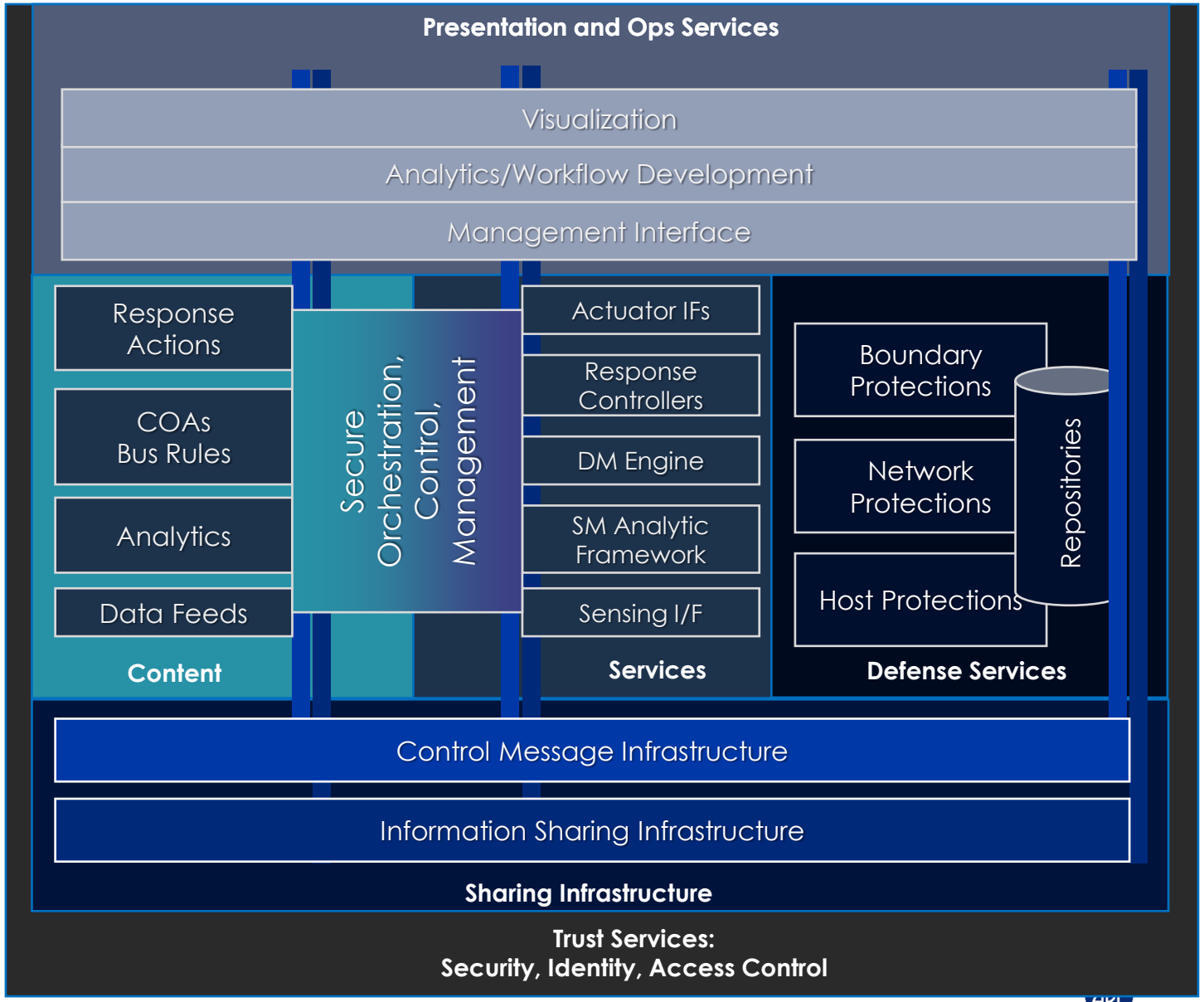


Challenge: Integrate and Automate Across What They Bring



IACD Functionality Inside the Enterprise

- What core *interoperable, flexible* services need to exist to integrate and automate across our defenses?
- What will it take to create, manage, and control this integration
- What content needs to be available and exchangeable?
- How will we interconnect the capabilities inside the enterprises?
- Will performance or security drive separate control needs?
- What tools must be provided to the analysts and operators?
- What trust, identity, and security needs to be in place to assure mission?

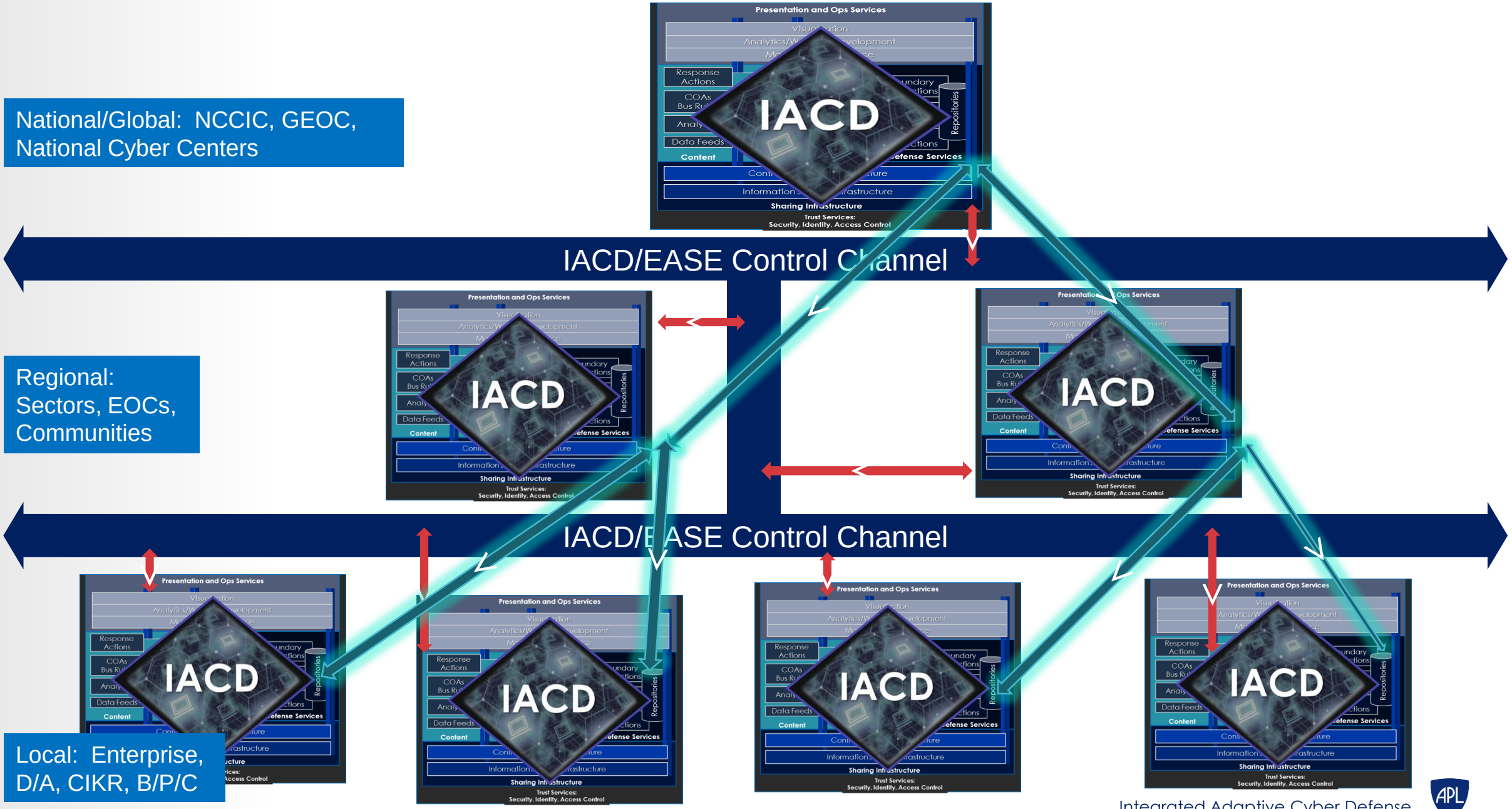


IACD Functionality Across/Among Diverse Enterprises

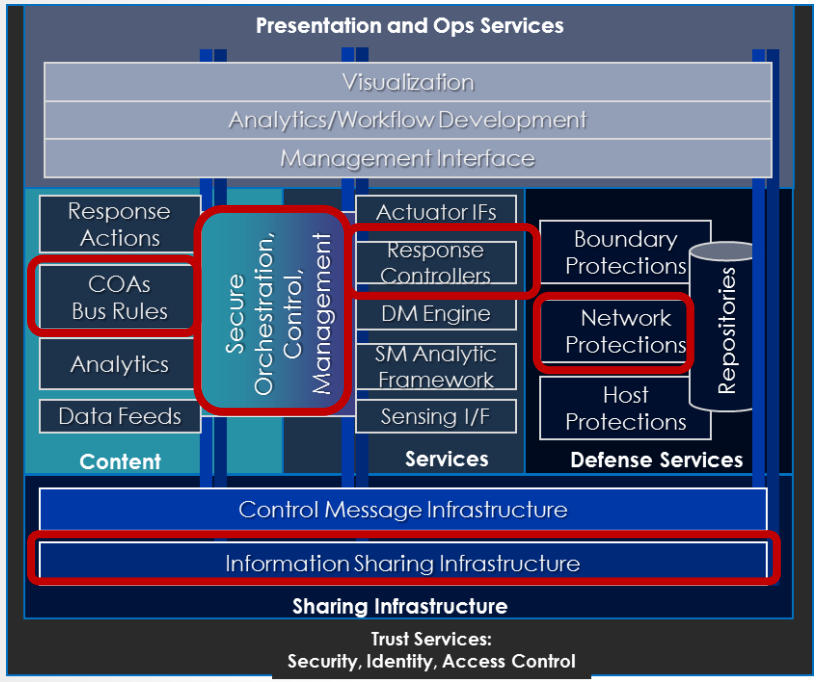
National/Global: NCCIC, GEOC, National Cyber Centers

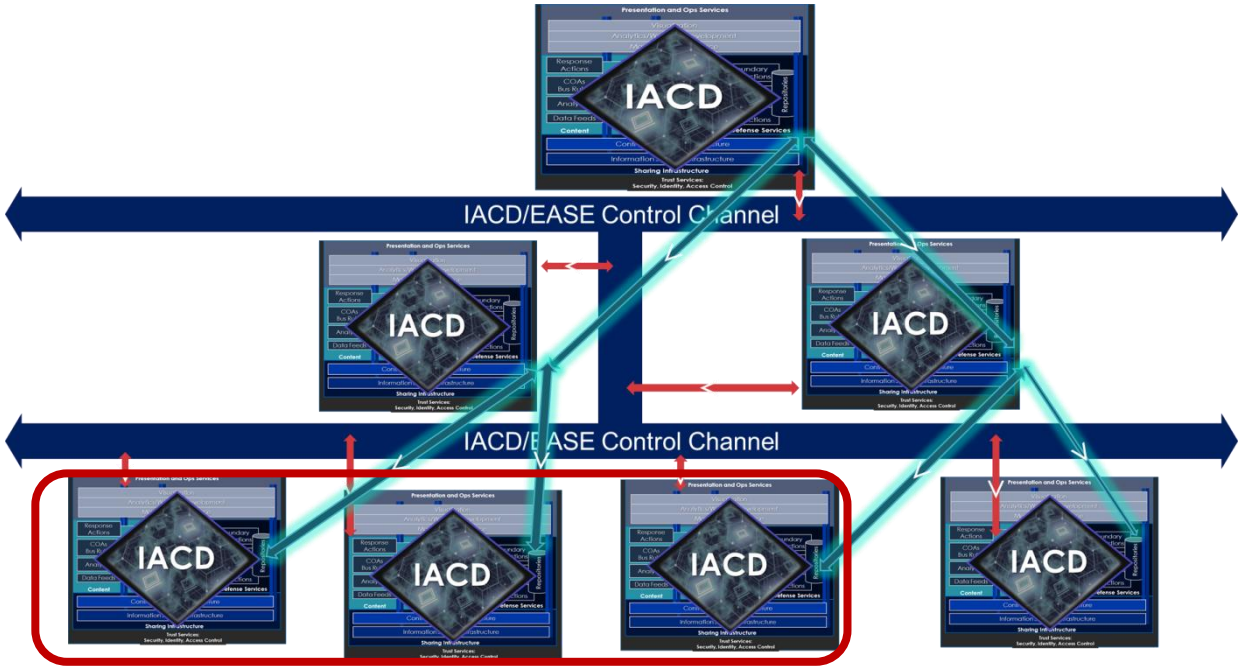
Regional: Sectors, EOCs, Communities

Local: Enterprise, D/A, CIKR, B/P/C



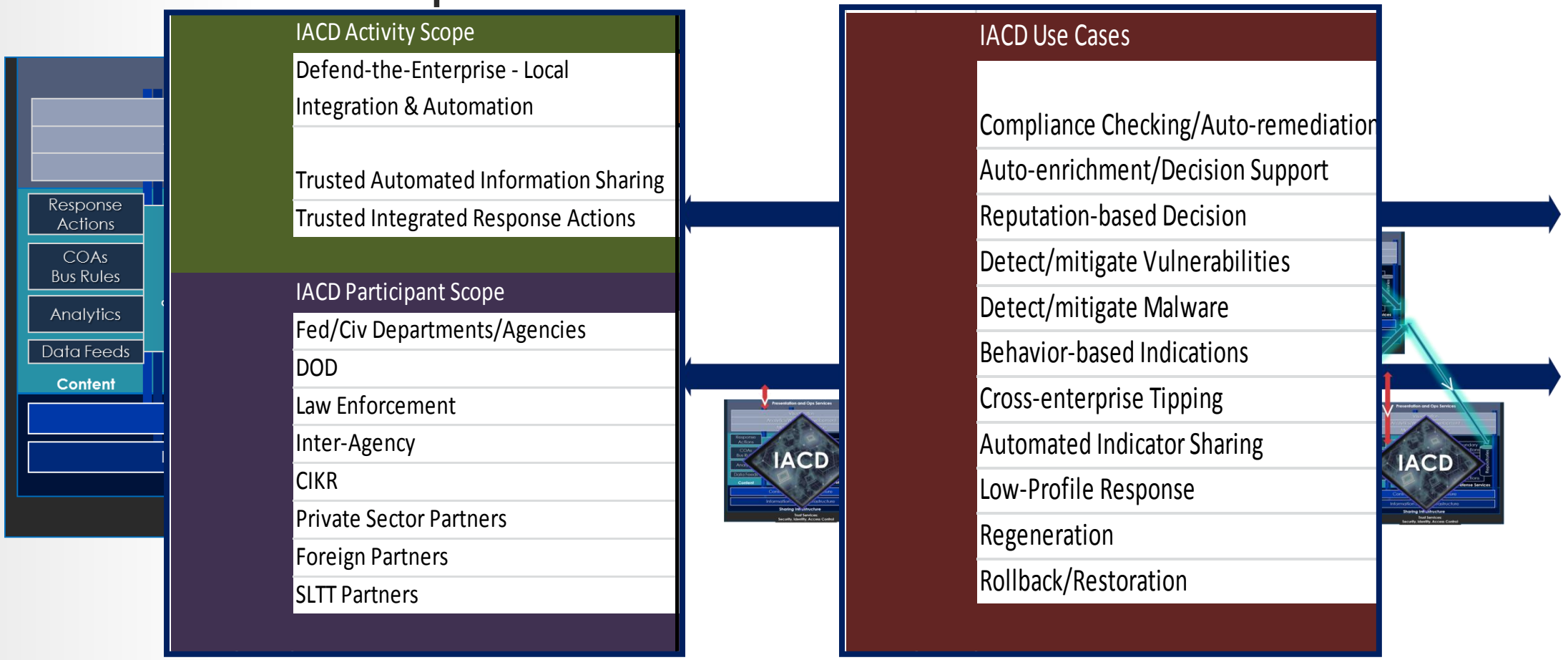
Agile Approach to Capability Demonstration and Requirements/Standards Elicitation





For each 90 day spiral, focus on some subset of target IACD capabilities – Within a single enterprise or across multiple enterprises with multiple roles

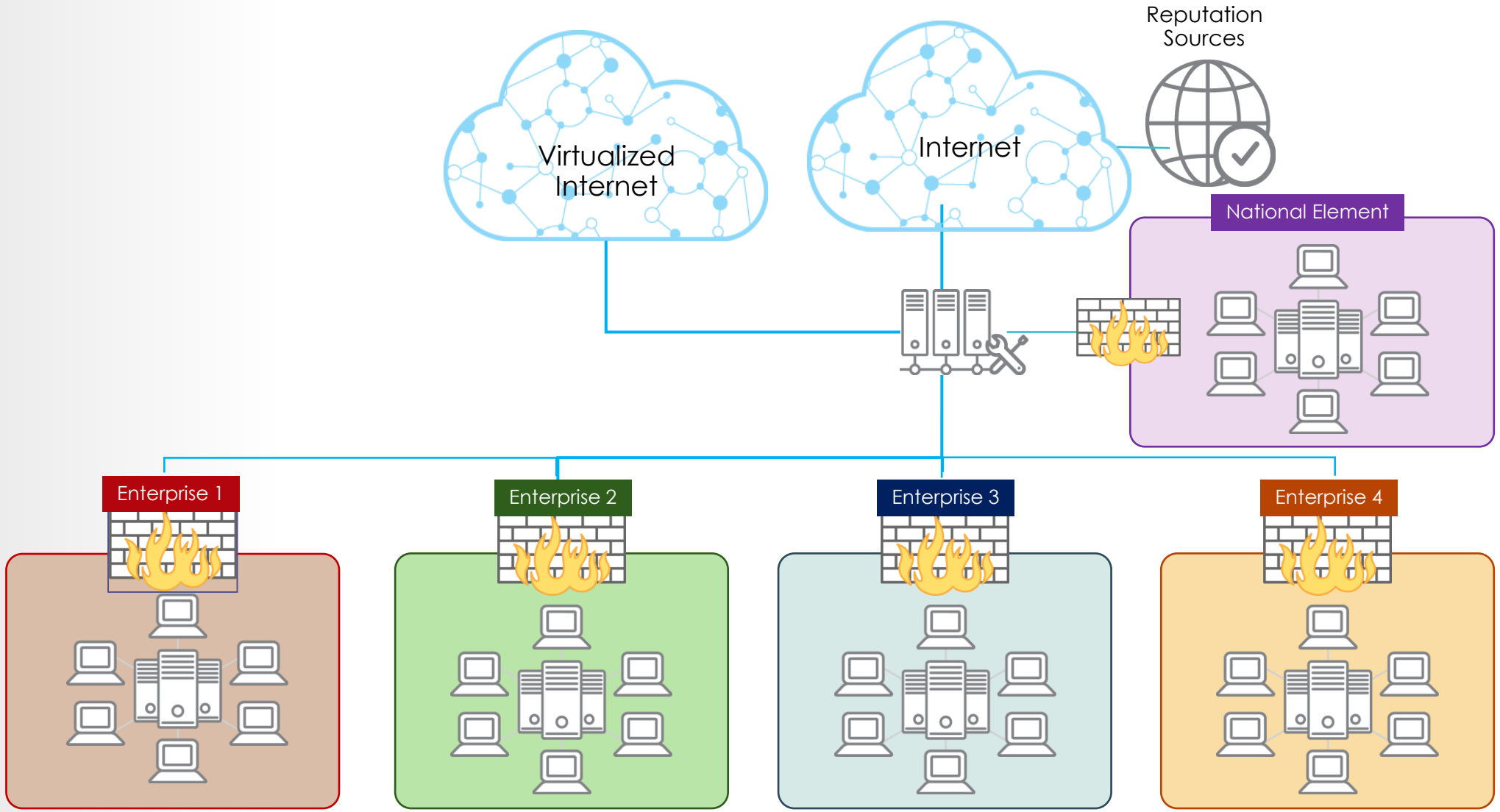
Agile Approach to Capability Demonstration and Requirements/Standards Elicitation



Ensure coverage of the operational space, including types of missions, user roles and authorities, and desired use cases

Federated Innovation, Integration & Research Environment for IACD Spirals

FIIRE
FEDERATED INNOVATION, INTEGRATION, & RESEARCH ENVIRONMENT



0 Make it Real

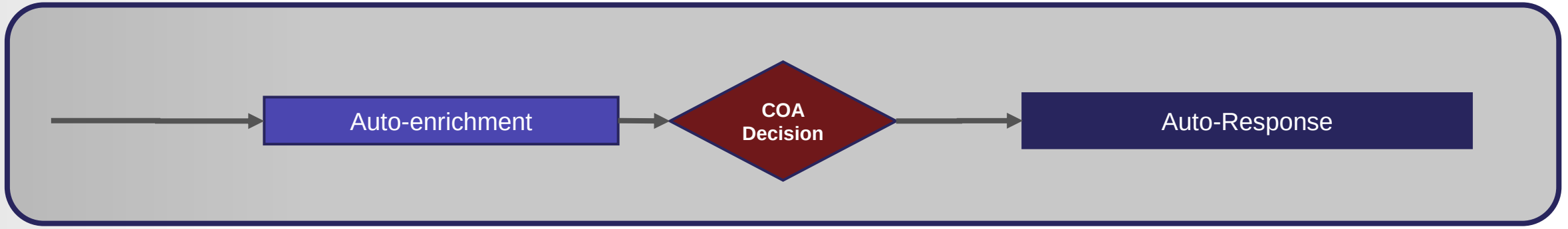
1 Scalability and Auto-Indicator Sharing

2 Risk- and Mission-based Decision Complexity

3 Robust Controls and Analytic-informed Decisions

4 Identity-driven Trust Communities

Spiral 0 Emphasis: Orchestration and Automation Intra-Enterprise



Increasing speed of assessment, efficient use of limited analyst resources

0 Make it Real

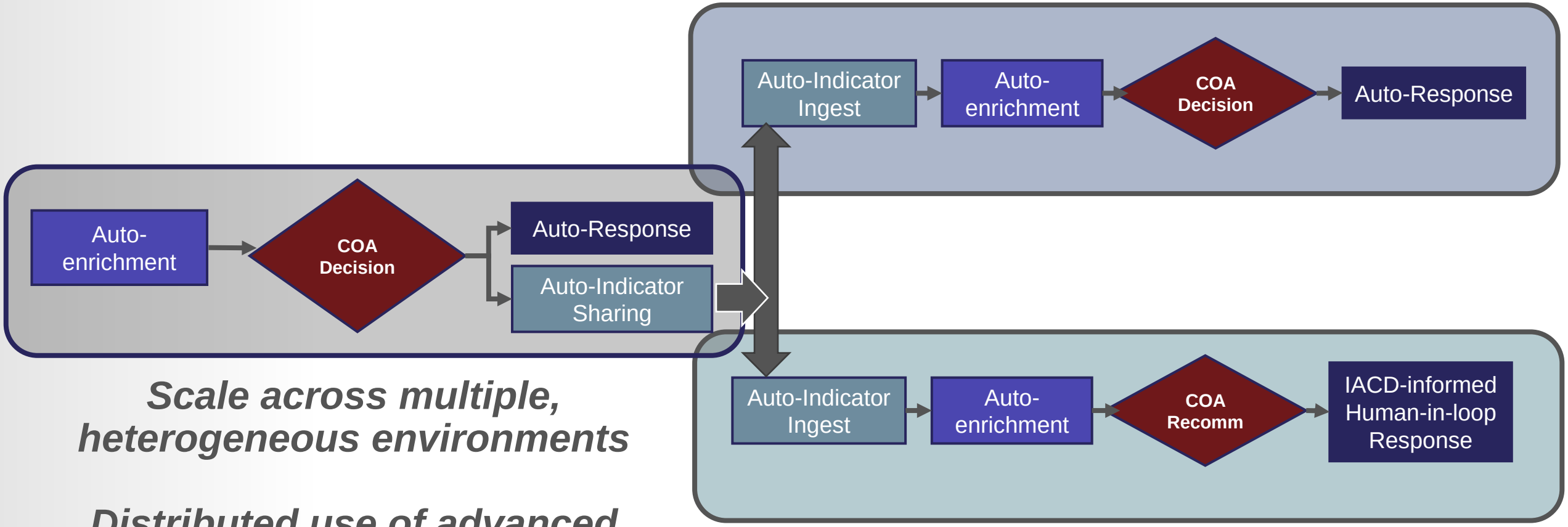
1 Scalability and Auto-Indicator Sharing

2 Risk- and Mission-based Decision Complexity

3 Robust Controls and Analytic-informed Decisions

4 Identity-driven Trust Communities

Spiral 1 Emphasis: Indicator Sharing and Auto-Response Across Communities of Trust



Scale across multiple, heterogeneous environments

Distributed use of advanced solutions

Spiral 2 Emphasis: Risk- and Mission-based Decision Complexity

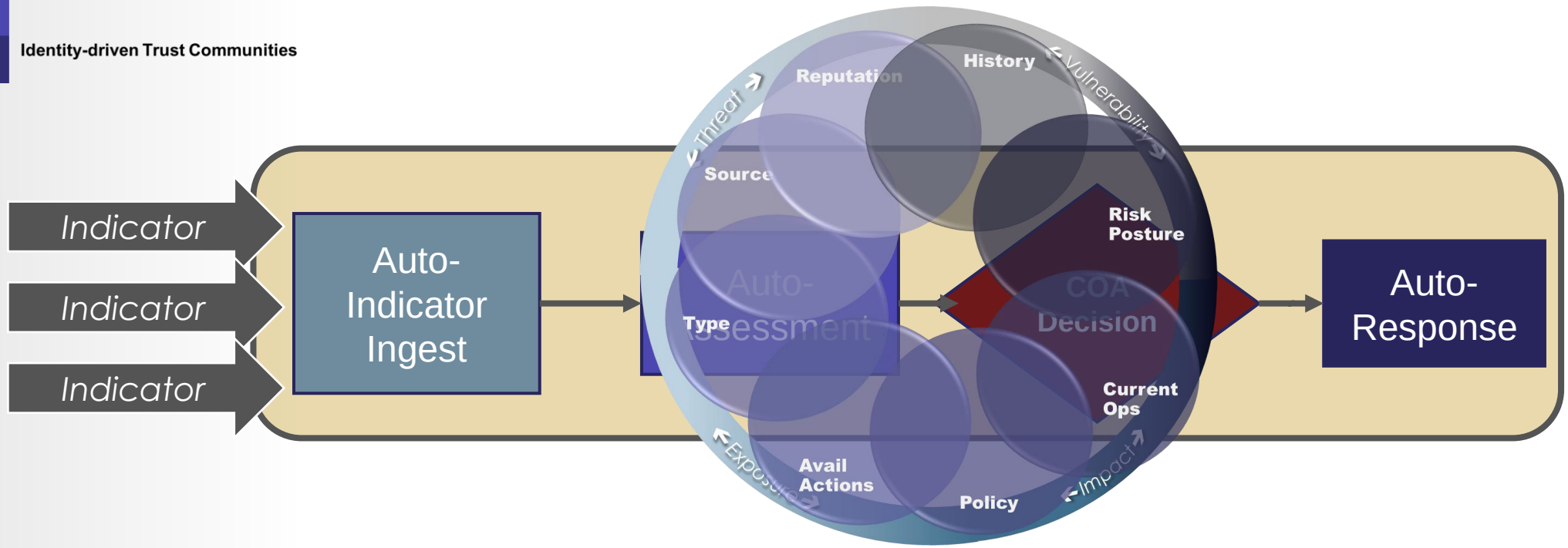
0 Make it Real

1 Scalability and Auto-Indicator Sharing

2 **Risk- and Mission-based Decision Complexity**

3 Robust Controls and Analytic-informed Decisions

4 Identity-driven Trust Communities



Spiral 2 Emphasis:
Risk- and Mission-based Decision Complexity

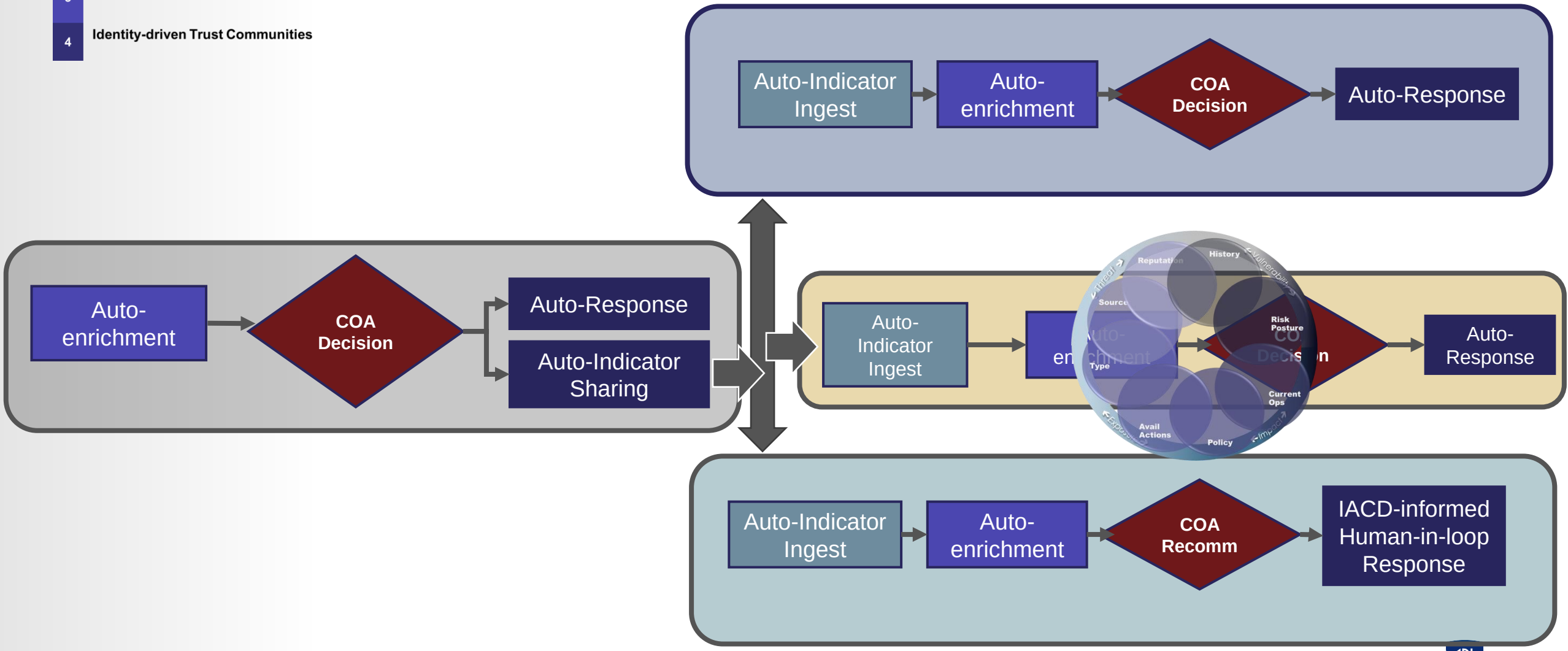
0 Make it Real

1 Scalability and Auto-Indicator Sharing

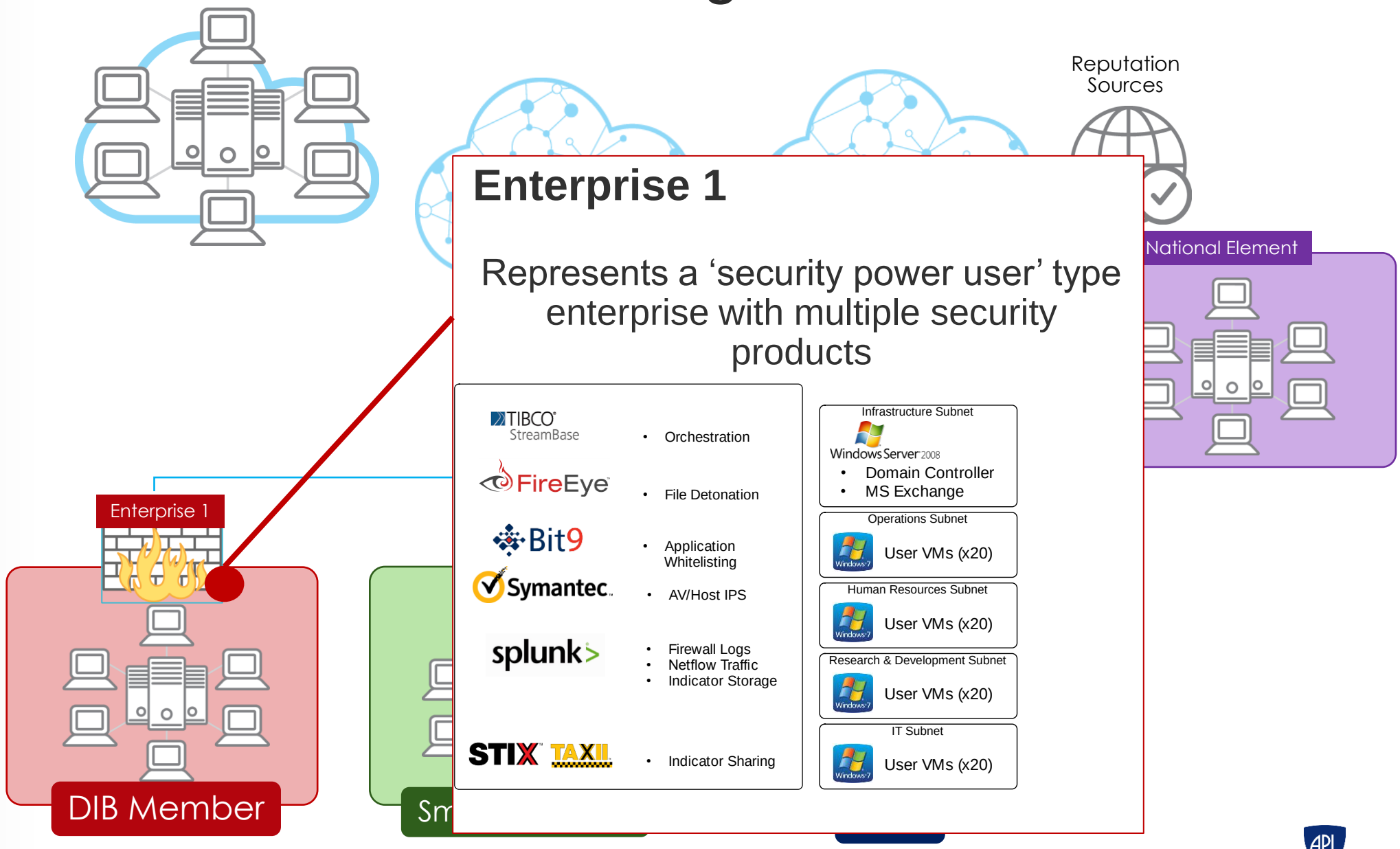
2 Risk- and Mission-based Decision Complexity

3 Robust Controls and Analytic-informed Decisions

4 Identity-driven Trust Communities



IACD FIIRE Configuration



IACD FIIRE Configuration

Enterprise 2

Represents a smaller, cost-sensitive enterprise utilizing open source solutions

- Microsoft System Center Orchestrator — Orchestration
- Suricata — IDS
- Web Traffic Analysis
- Netflow
- Windows Server 2008 — File Retrieval
- splunk> — Firewall Logs, Netflow Traffic, Indicator Storage
- RTIR secure response — Ticketing
- STIX TAXII — Indicator Sharing

Infrastructure Subnet
Windows Server 2008
- Domain Controller
- MS Exchange

Operations Subnet
User VMs (x20)

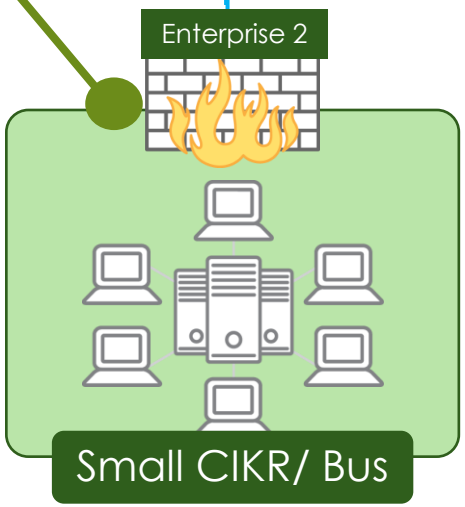
Human Resources Subnet
User VMs (x20)

Research & Development Subnet
User VMs (x20)

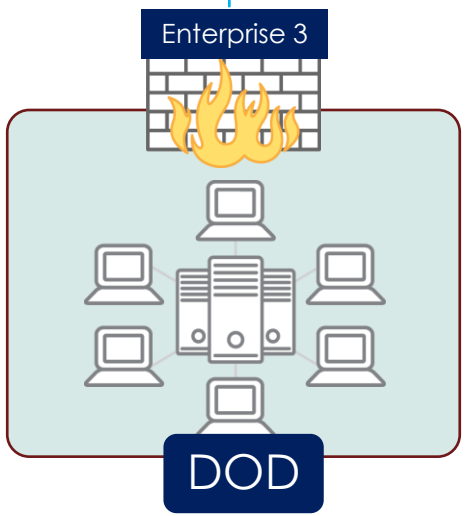
IT Subnet
User VMs (x20)

National Element

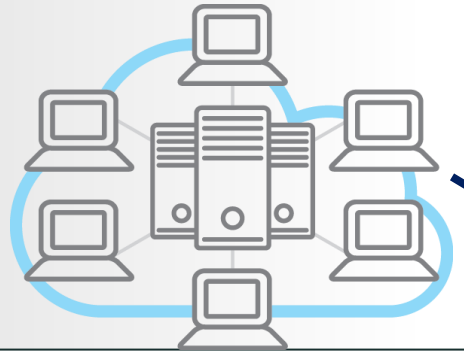
Enterprise 2



Enterprise 3



IACD FIIRE Configuration



Enterprise 3

Enterprise partner with a vertically integrated security stack – DOD representative environment

- HBSS
- Firewall Logs
- Netflow Traffic
- Indicator Storage
- Indicator Sharing

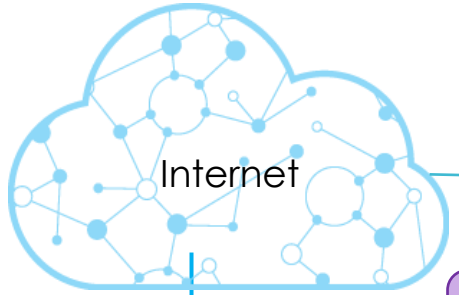
Infrastructure Subnet
Windows Server 2008
- Domain Controller
- MS Exchange

Operations Subnet
User VMs (x20)

Human Resources Subnet
User VMs (x20)

Research & Development Subnet
User VMs (x20)

IT Subnet
User VMs (x20)



Reputation Sources

National Element

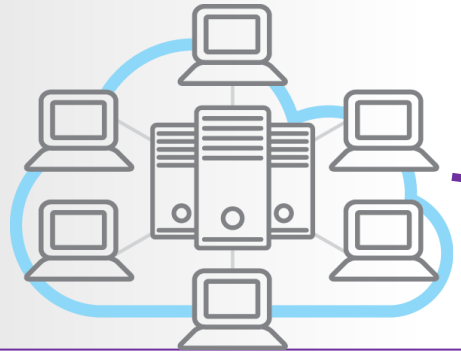
Enterprise 2

Enterprise 3

Small CIKR/ Bus

DOD

IACD FIIRE Configuration



Virtualized Internet

Internet

Reputation Sources

National Element

National Element (or Regional)

Aggregation/Coordination; Multi-enterprise SA; security service provider; COA/ mitigation development

- Web Traffic Analysis
- Netflow

ESSA CREATE SHARE ENHANCE

- Government Reputation Sources

cuckoo

- Malware Detonation

splunk>

- Firewall Logs
- Netflow Traffic
- Indicator Storage

STIX TAXII

- Indicator Sharing

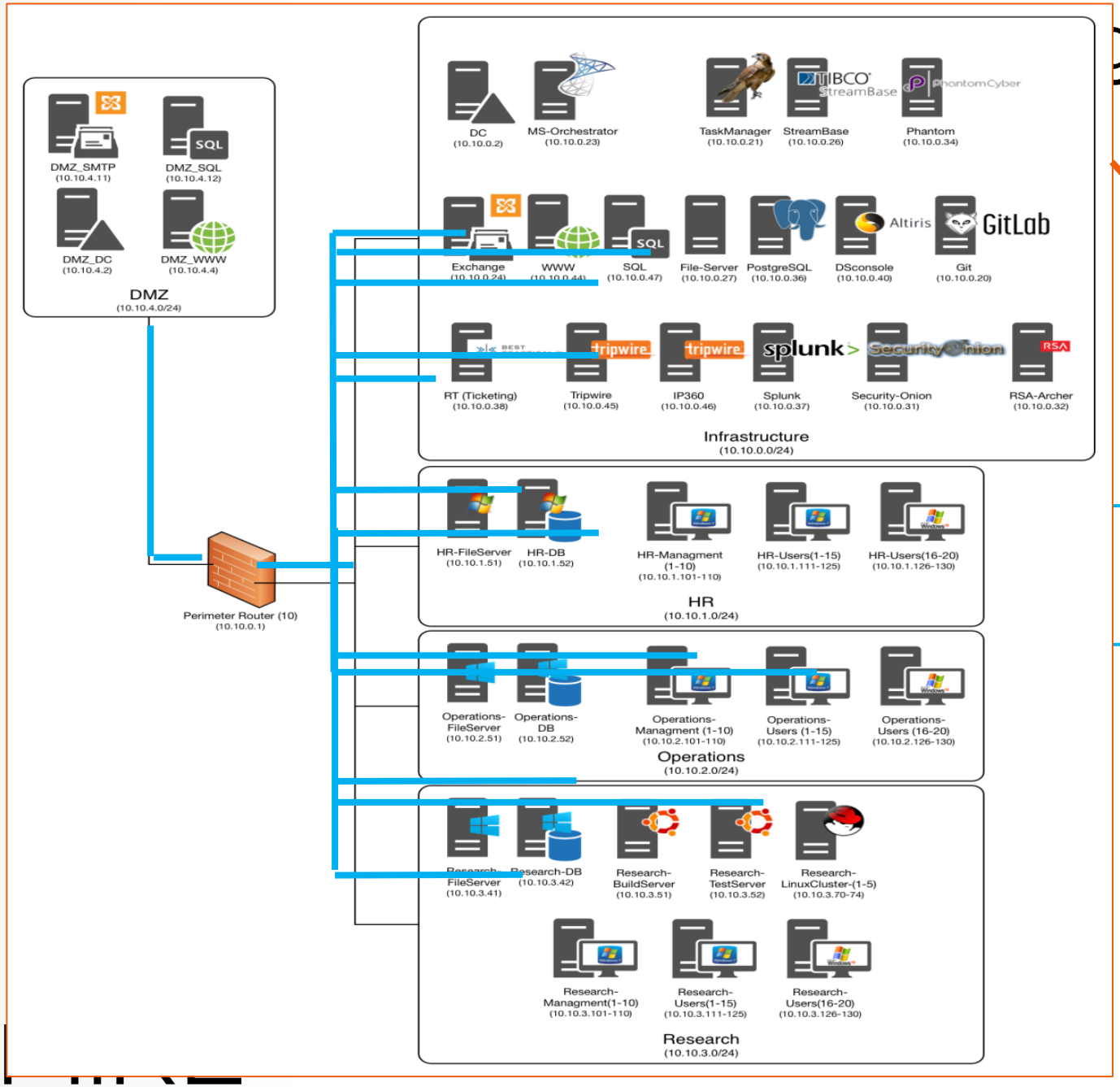
Enterprise 2

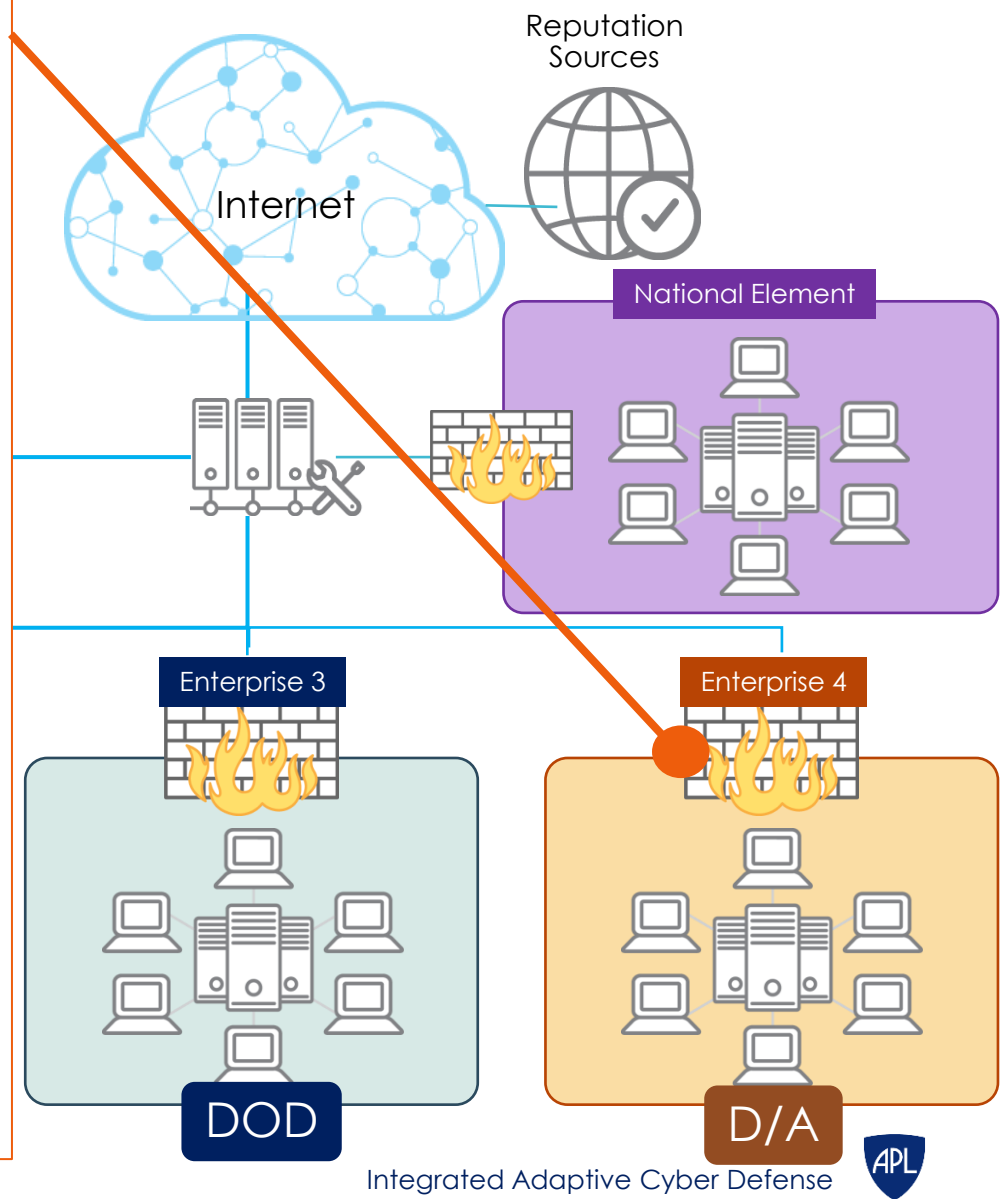
Small CIKR/ Bus

Enterprise 3

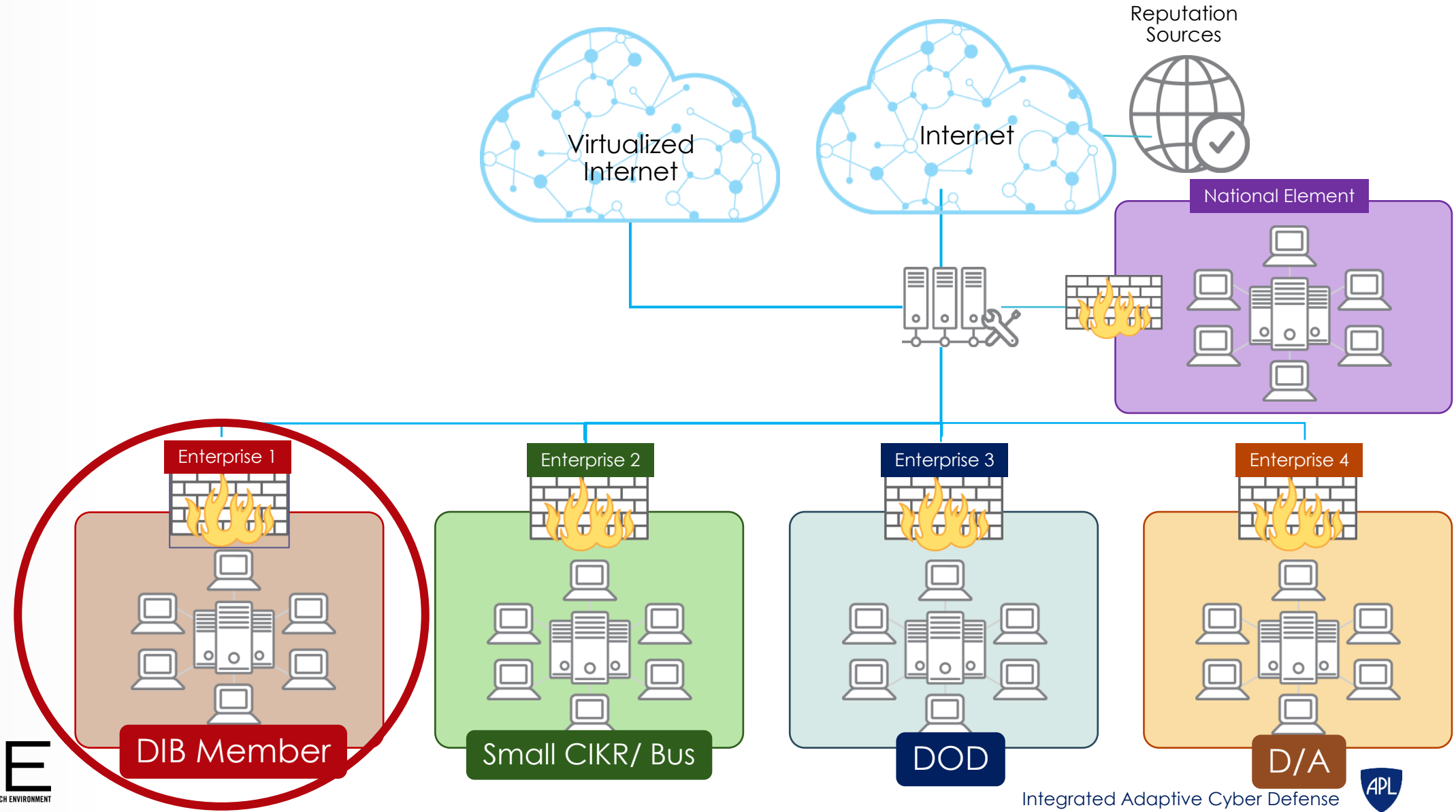
DOD

guration


DMZ_SMTP
(10.10.4.11)
DMZ_SQL
(10.10.4.12)
DMZ_DC
(10.10.4.2)
DMZ_WWW
(10.10.4.4)
DMZ
(10.10.4.0/24)
Perimeter Router (10)
(10.10.0.1)
DC
(10.10.0.2)
MS-Orchestrator
(10.10.0.23)
TaskManager
(10.10.0.21)
StreamBase
(10.10.0.26)
Phantom
(10.10.0.34)
Exchange
(10.10.0.24)
WWW
(10.10.0.44)
SQL
(10.10.0.47)
File-Server
(10.10.0.27)
PostgreSQL
(10.10.0.36)
DSconsole
(10.10.0.40)
Git
(10.10.0.20)
RT (Ticketing)
(10.10.0.38)
Tripwire
(10.10.0.45)
IP360
(10.10.0.46)
Splunk
(10.10.0.37)
Security-Onion
(10.10.0.31)
RSA-Archer
(10.10.0.32)
Infrastructure
(10.10.0.0/24)
HR-FileServer
(10.10.1.51)
HR-DB
(10.10.1.52)
HR-Managment
(1-10)
(10.10.1.101-110)
HR-Users(1-15)
(10.10.1.111-125)
HR-Users(16-20)
(10.10.1.126-130)
HR
(10.10.1.0/24)
Operations-
FileServer
(10.10.2.51)
Operations-
DB
(10.10.2.52)
Operations-
Managment (1-10)
(10.10.2.101-110)
Operations-
Users (1-15)
(10.10.2.111-125)
Operations-
Users (16-20)
(10.10.2.126-130)
Operations
(10.10.2.0/24)
Research-
FileServer
(10.10.3.41)
Research-DB
(10.10.3.42)
Research-
BuildServer
(10.10.3.51)
Research-
TestServer
(10.10.3.52)
Research-
LinuxCluster-(1-5)
(10.10.3.70-74)
Research-
Managment(1-10)
(10.10.3.101-110)
Research-
Users(1-15)
(10.10.3.111-125)
Research-
Users(16-20)
(10.10.3.126-130)
Research
(10.10.3.0/24)

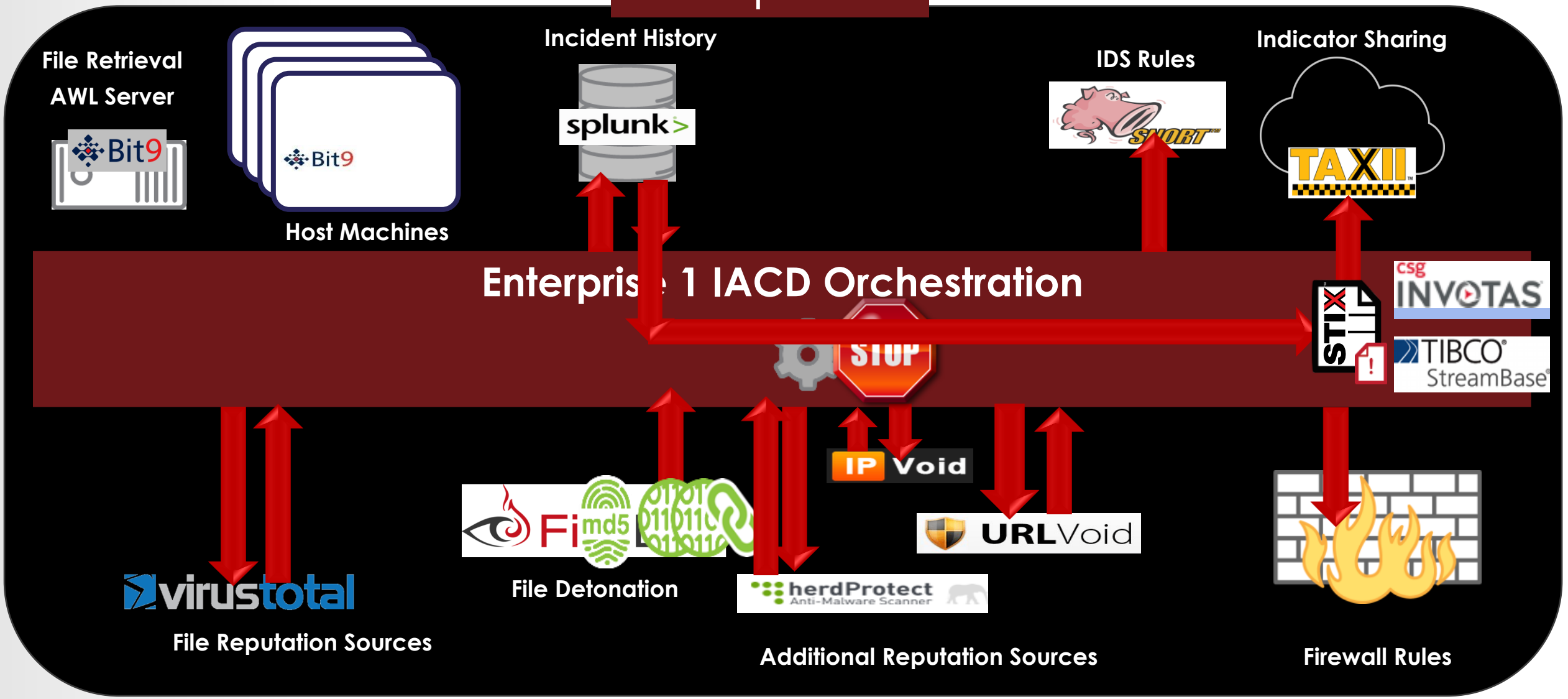

Reputation
Sources
Internet
National Element
Enterprise 3
Enterprise 4
DOD
D/A

IACD FIIRE Configuration



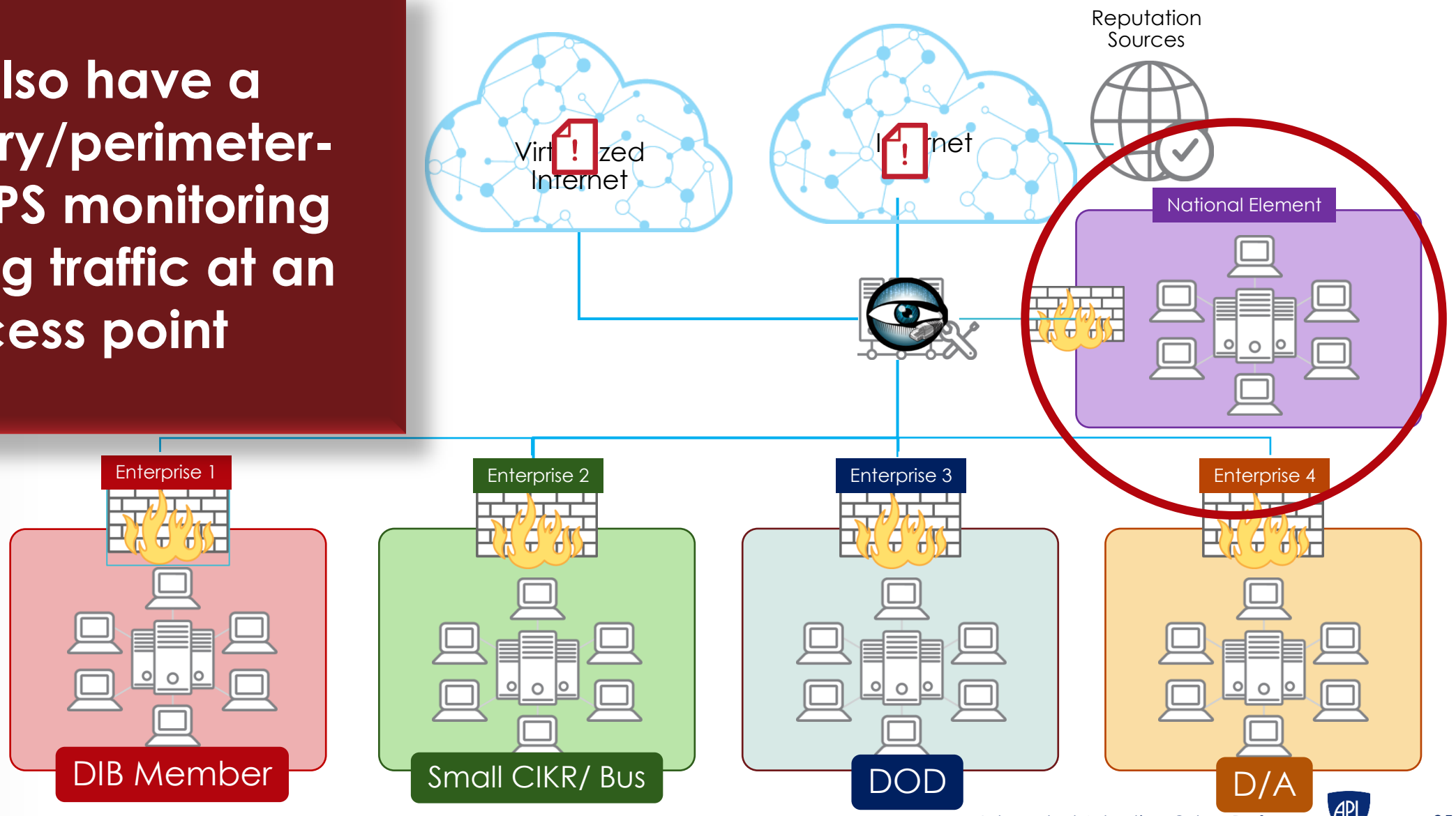
Enterprise 1

Enterprise 1

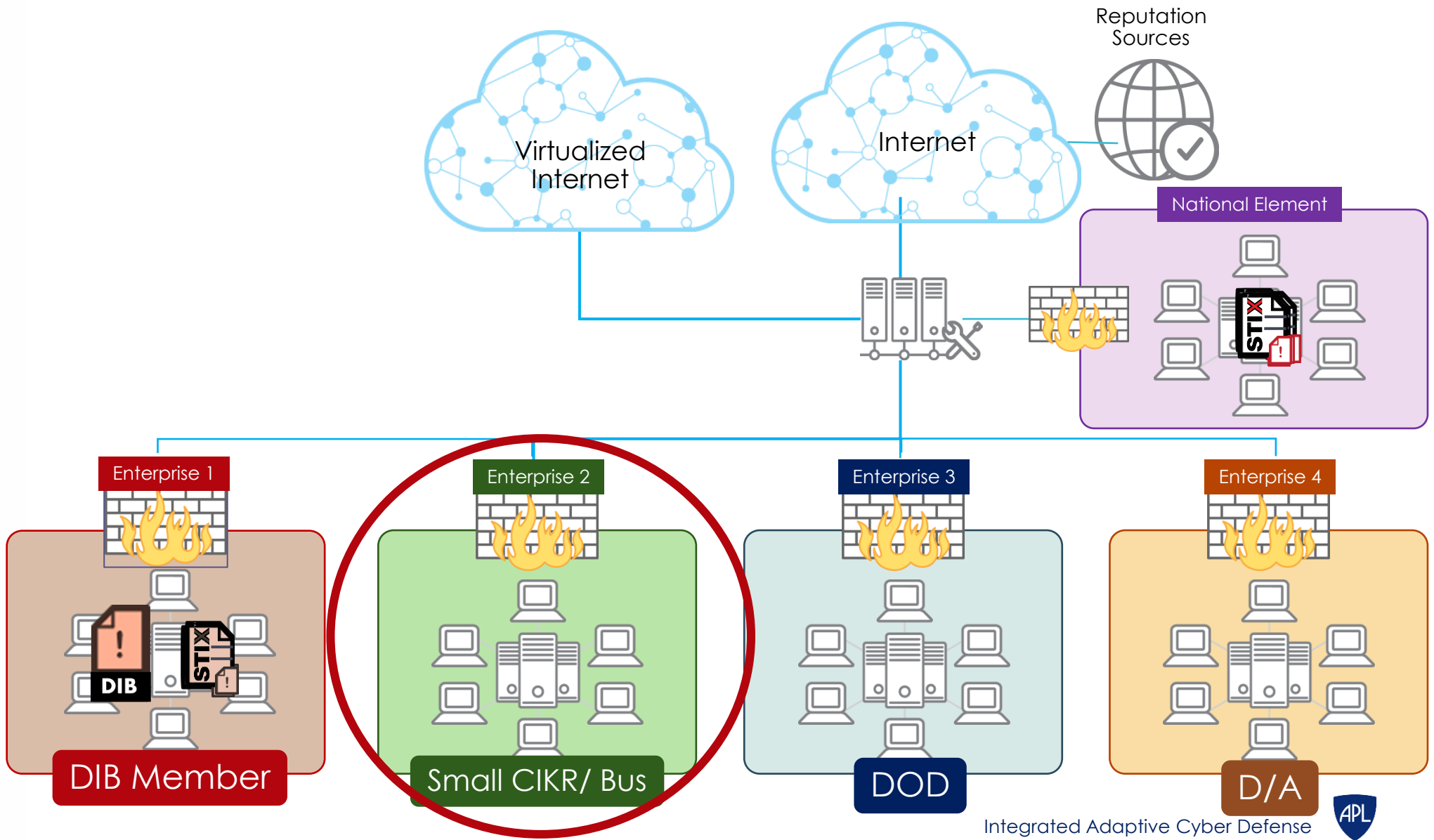


IACD FIIRE Configuration – Multiple Sources of Indicators

We also have a boundary/perimeter-based IPS monitoring incoming traffic at an access point



IACD FIIRE Configuration – Multiple Sources of Indicators



Enterprise 2

Host Machines

IDS

File Reputation Sources

virustotal

Incident History

Enterprise 2 IACD Orchestration

Microsoft® System Center Orchestrator

Indicator Sharing

Ticketing

Human-in-the-Loop

Firewall Rules

Enterprise 2

Host Machines

IDS

File Reputation Sources

virustotal

Incident History

splunk>

Enterprise 2 Orchestration

Microsoft® System Center Orchestrator

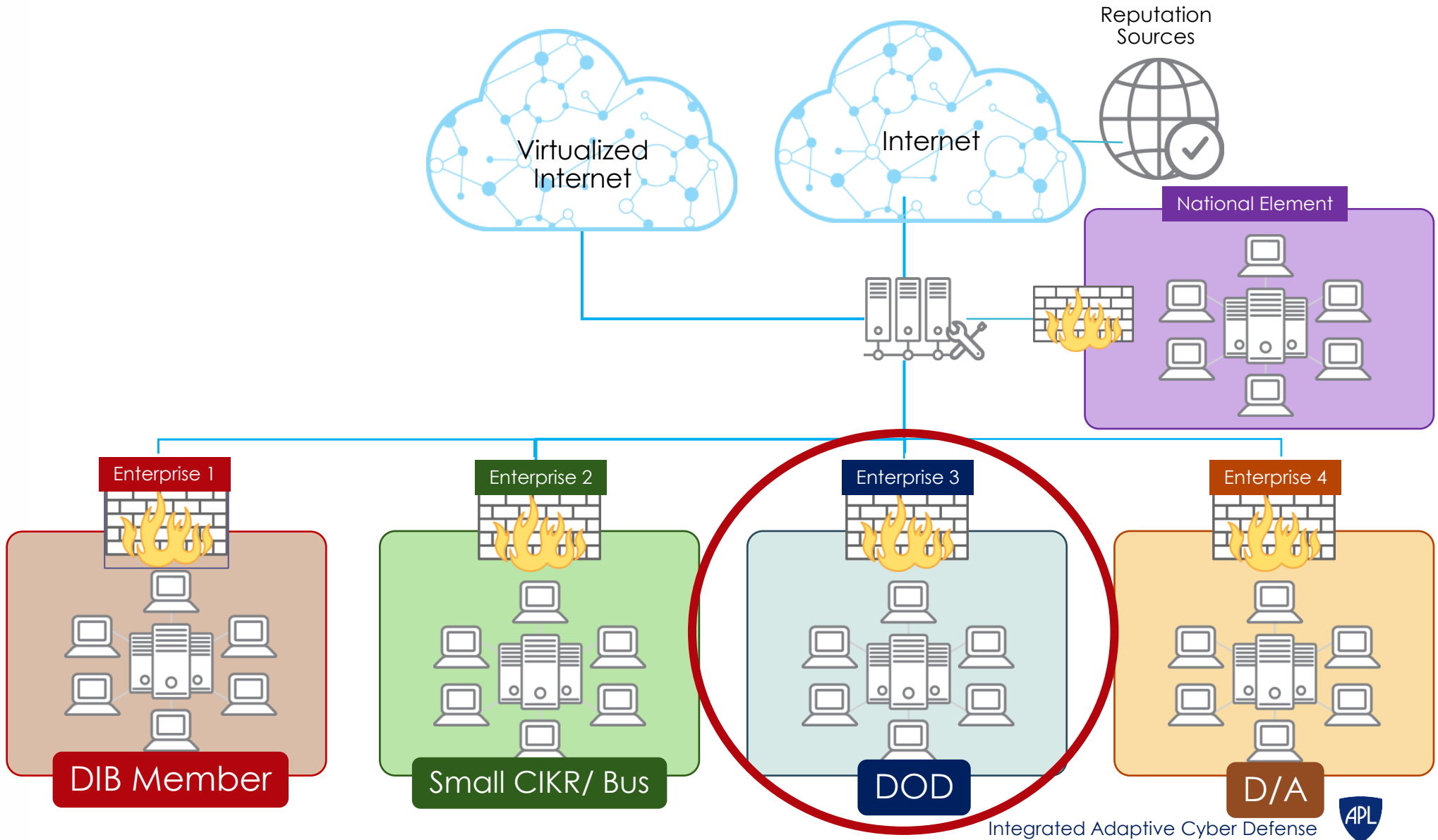
Indicator Sharing

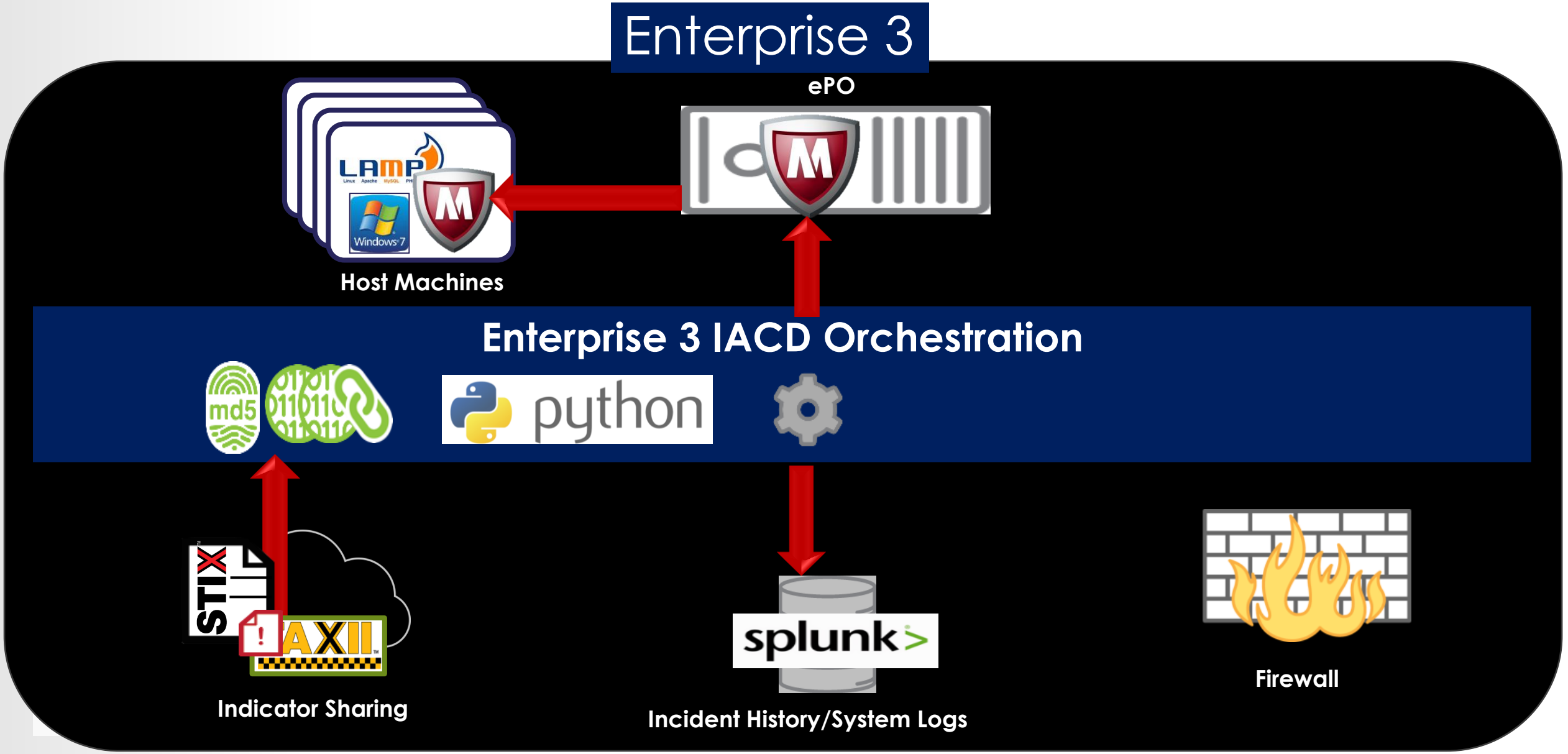
Ticketing

Human-in-the-Loop

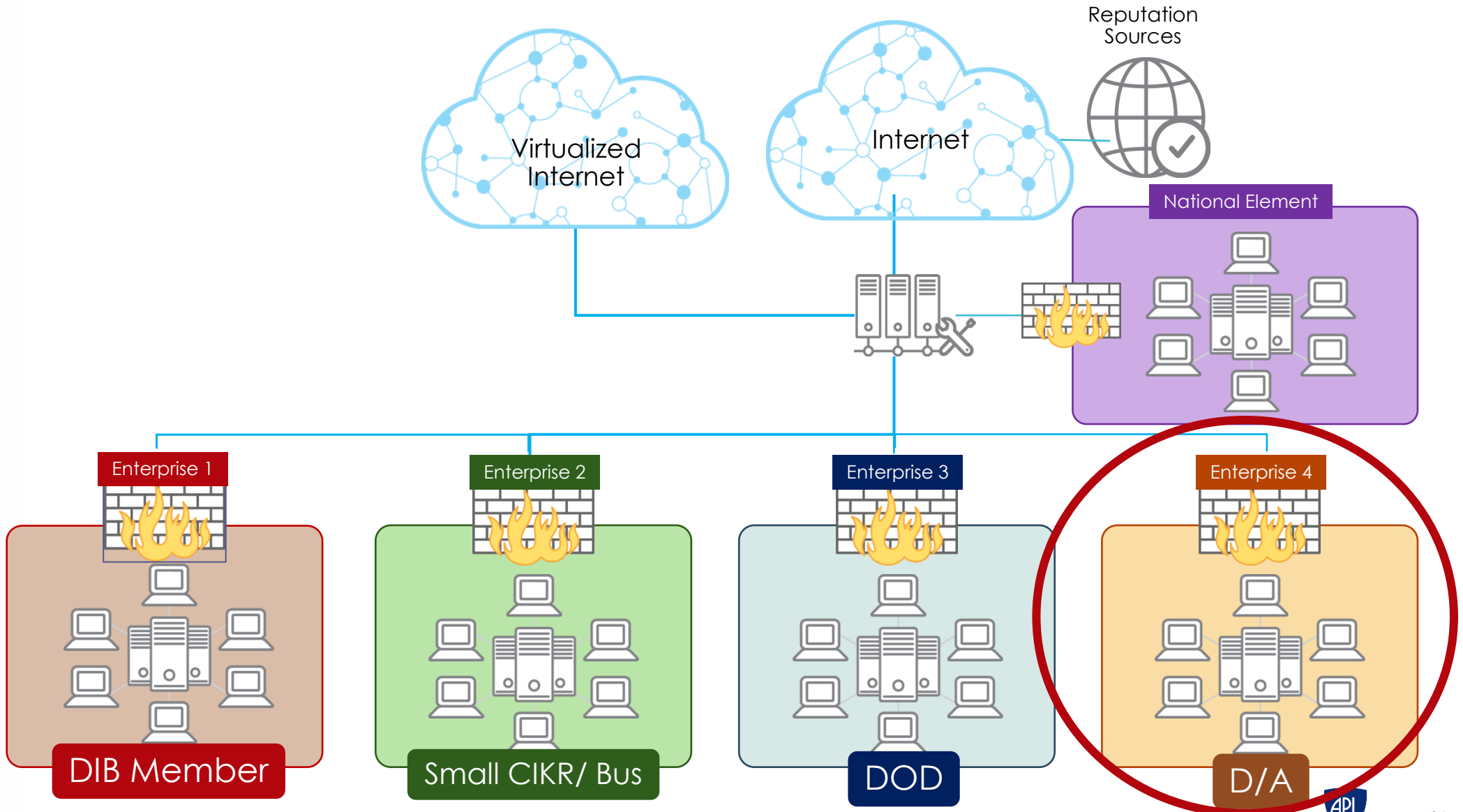
Firewall Rules

IACD FIIRE Configuration



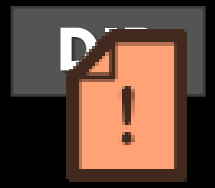

Enterprise 3
ePO
LAMP
Windows 7
Host Machines
Enterprise 3 IACD Orchestration
md5
python
STIX
TAXII
Indicator Sharing
splunk>
Incident History/System Logs
Firewall

IACD FIIRE Configuration



Parsing

Indicator Receipt



IACD/EASE Services

TIBCO StreamBase

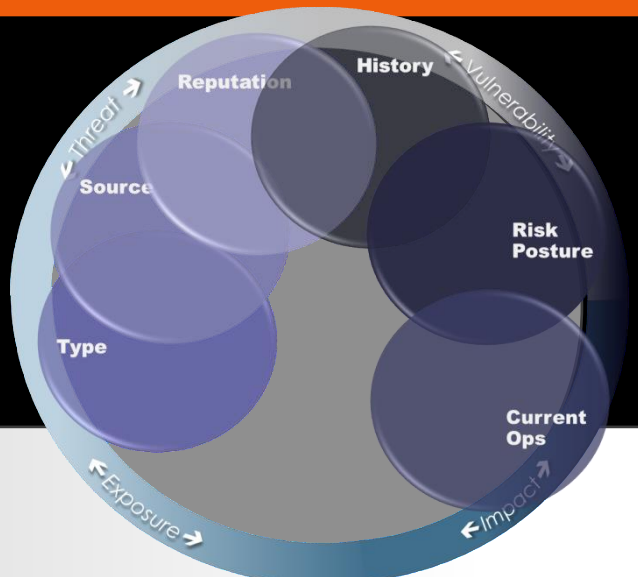
Steps Towards Decision-Making tracked here

Incident History

Enrichment

Indicator Enrichment Sources

WHOis.net
IP Void
WOT WEB OF TRUST
virustotal
Alexa
URLVoid
TIBCO StreamBase
md5
Indicator Reputation Scores
Indicator History
Hosts Connections
Host Risk Posture



splunk>

Incident History

Host Enrichment Sources

tripwire

Scoring

Indicator Histo… …onnections

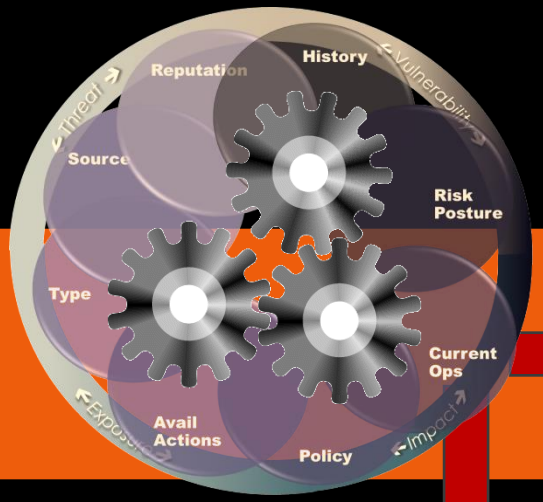
Indicator Reputatio… …Scores …Risk Posture

TIBCO StreamBase

IACD/EASE Services

Scoring

COA Selection



TIBCO StreamBase

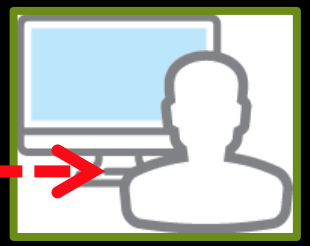
IACD/EASE Services

COA Automation

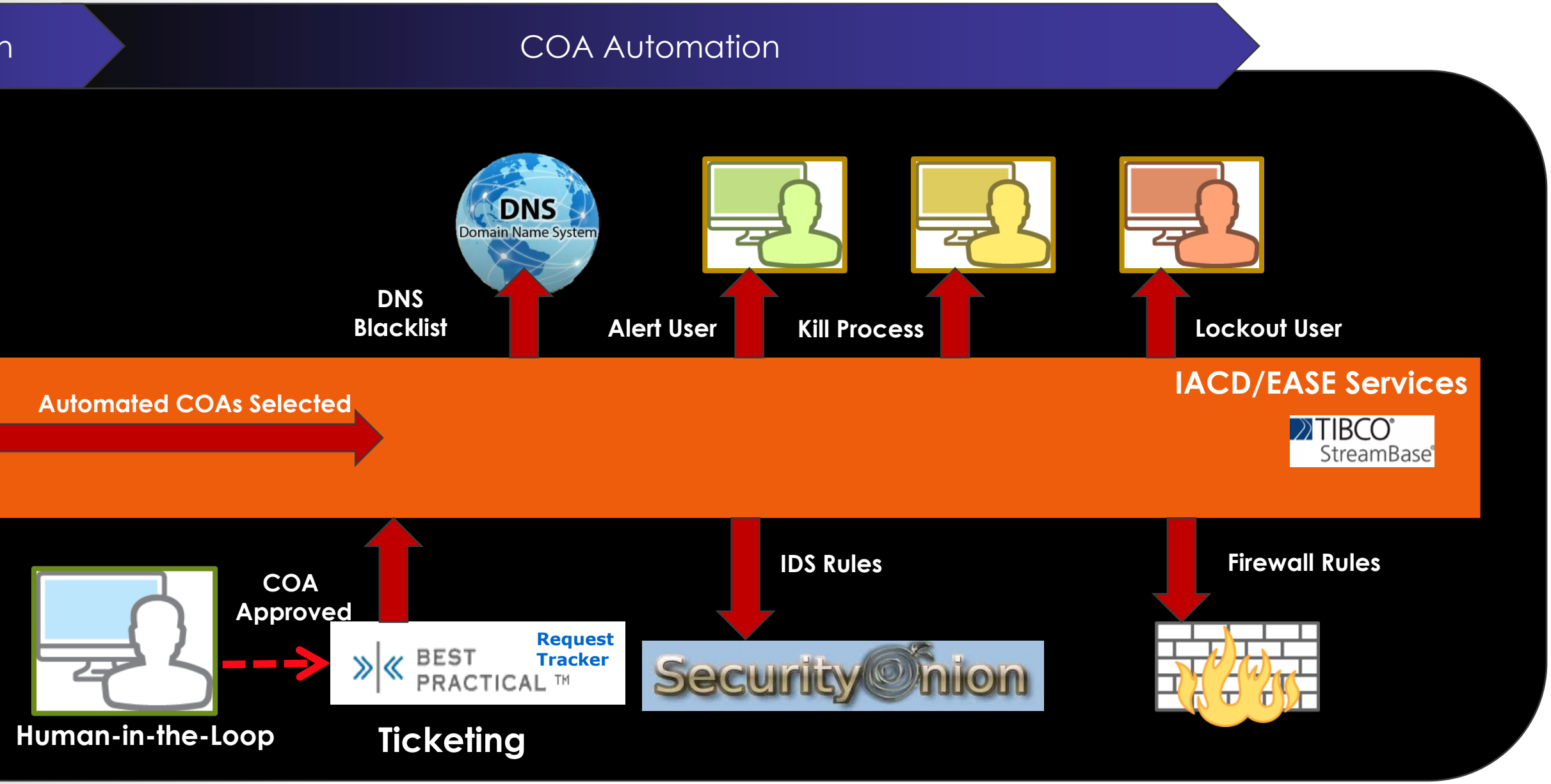
Enriched Tickets
COA Recomm

BEST PRACTICAL™ Request Tracker

Ticketing



Human-in-the-Loop


n
COA Automation
DNS
Domain Name System
DNS
Blacklist
Alert User
Kill Process
Lockout User
IACD/EASE Services
TIBCO
StreamBase
Automated COAs Selected
COA
Approved
IDS Rules
Firewall Rules
BEST
PRACTICAL ™
Request
Tracker
Security Onion
Human-in-the-Loop
Ticketing

Spiral Results & Outcomes

Spiral 0 Results: Operations Timeline Comparison

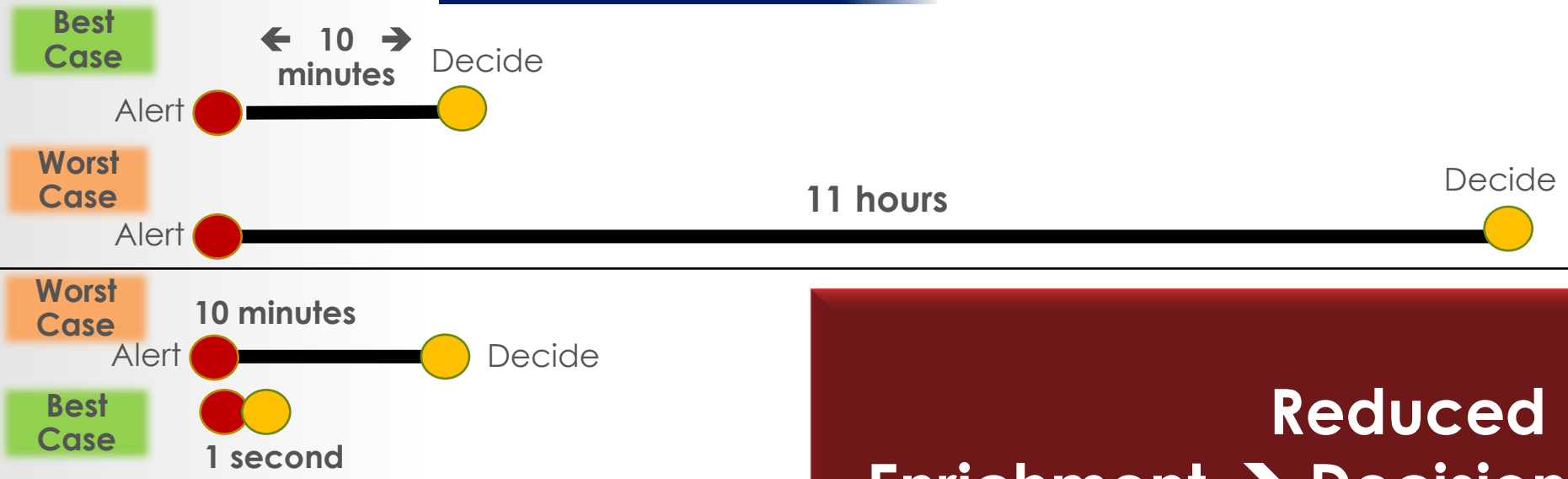
1 Billion
Events per Day

65

Tier 1 Analyst Assigned

30-50 Tier 1 Analyst Hours / Day

50,000
Unknown File on Host



Reduced Enrichment → Decision Timeline by 97-99% per Event

Spiral 0 Results: Operations Timeline Comparison

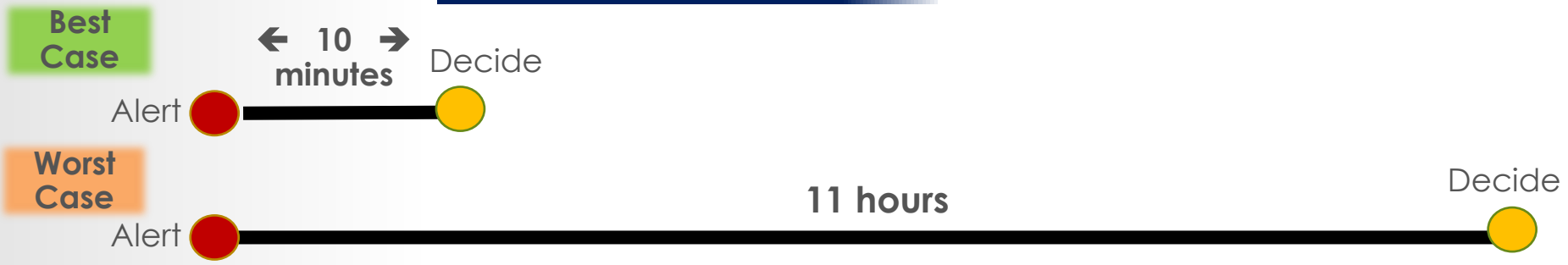
1 Billion
Events per Day

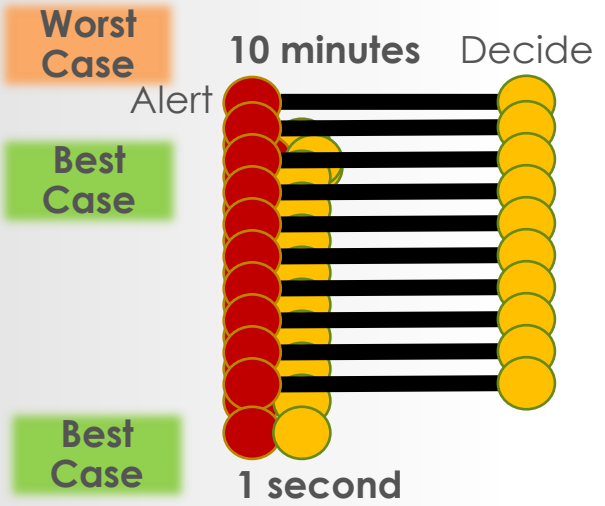
65

Tier 1 Analyst Assigned

30-50 Tier 1 Analyst Hours / Day

50,000
Unknown File on Host





24 – 96 Simultaneous Events

Increased Triage Capacity Over 10,000 Times

Spiral 0 Results: Operations Timeline Comparison

1 Billion
Events per Day

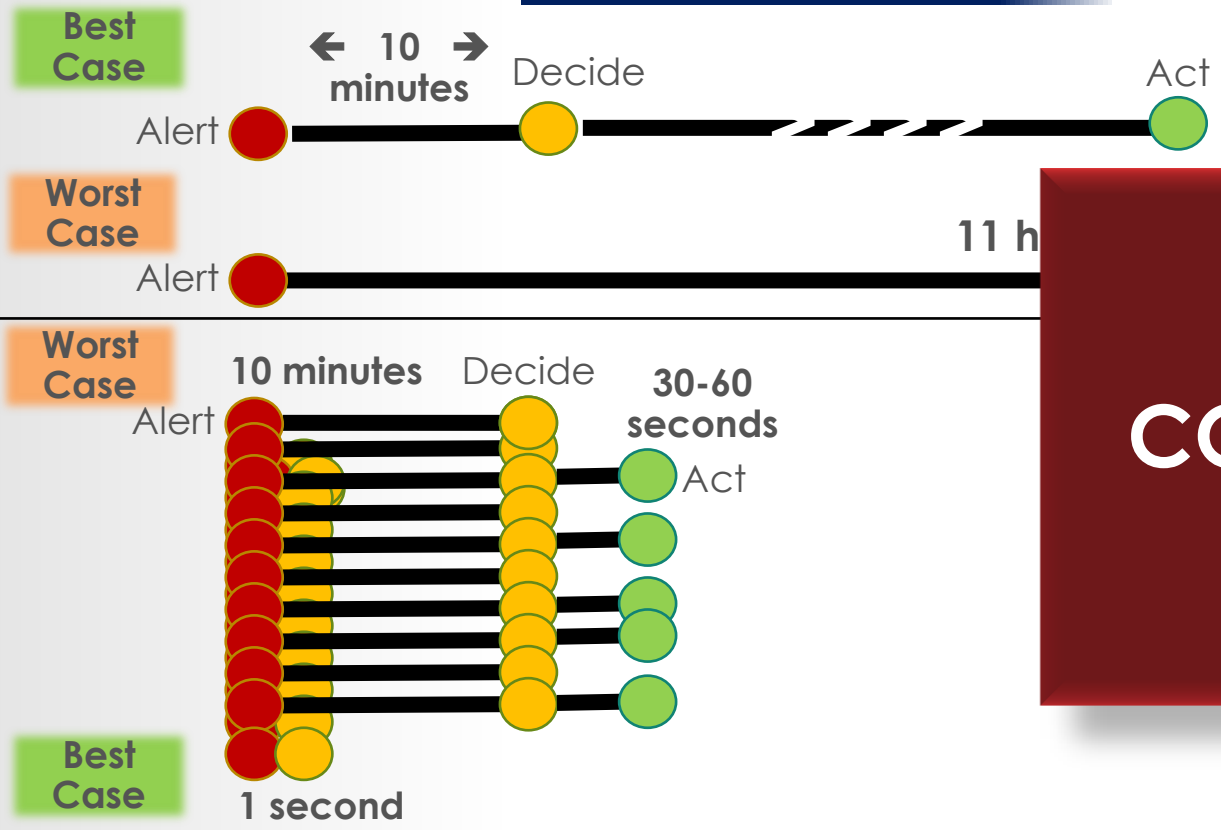
65

Tier 1 Analyst Assigned

30-50 Tier 1 Analyst Hours / Day

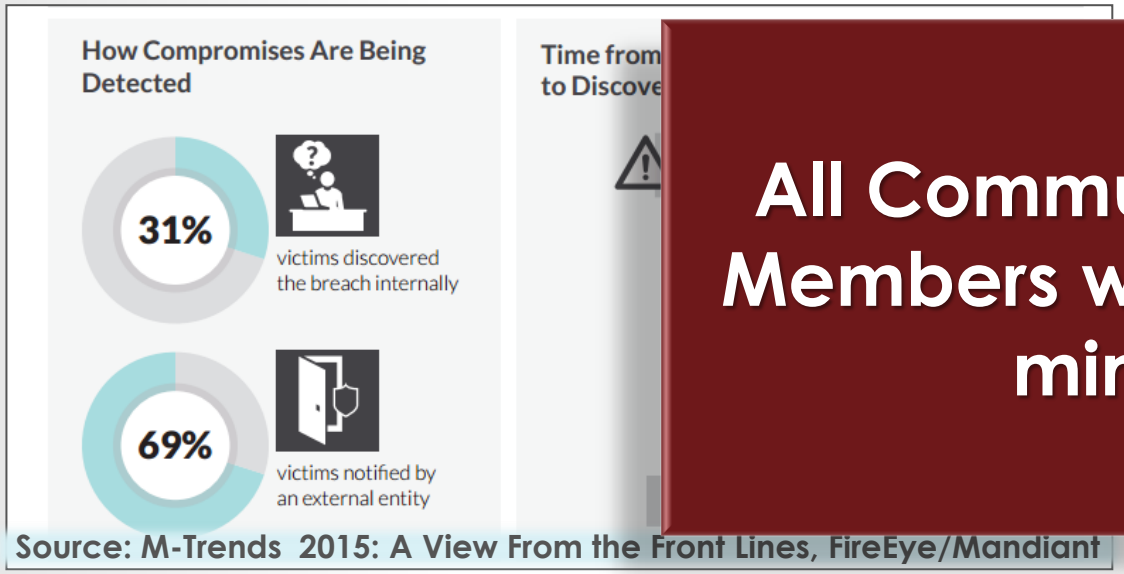
50,000
Unknown File on Host

Average Analyst Ticket Processing
45 Minutes



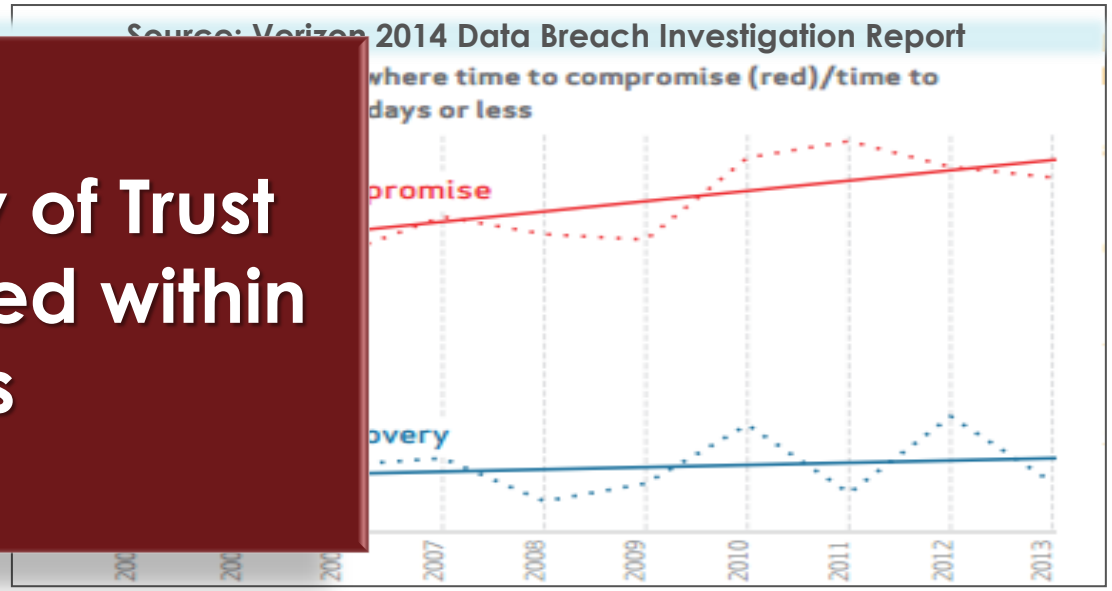
Reduced COA Implementation Timeline by 98%

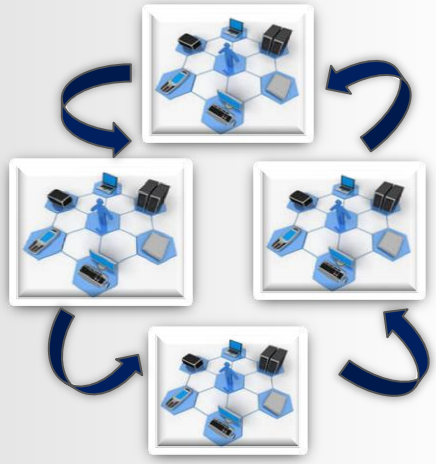
Spiral 1: Real-world Comparisons
Multi-Enterprise Info Sharing



Source: M-Trends 2015: A View From the Front Lines, FireEye/Mandiant

All Community of Trust Members warned within minutes





IACD Community of Trust

Best Case

Indicator → Detect/Decide → Self-Defense → 1 sec – 1 minute

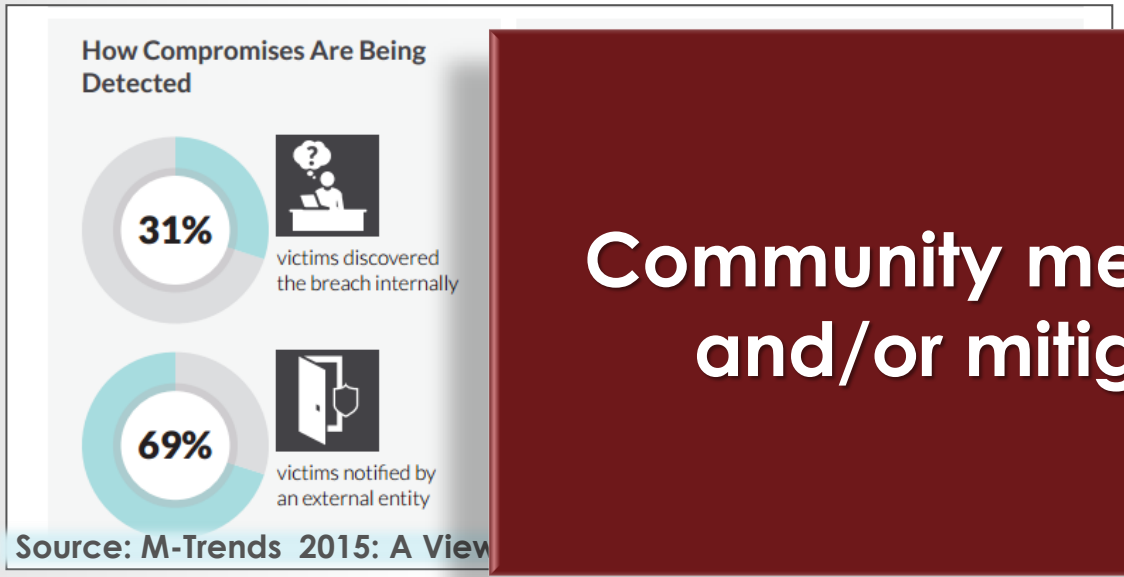
Indicator → Detect/Decide → Auto-Indicator Sharing → < 2 minutes

"Worst" Case

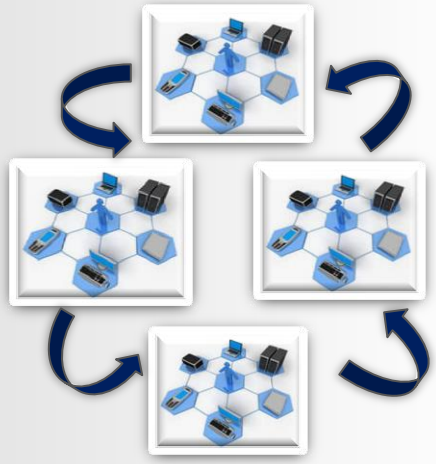
Indicator → Detect/Decide → Self-Defense → 8 minutes

Indicator → Detect/Decide → Auto-Indicator Sharing → 9 minutes

Spiral 1: Real-world Comparisons
Auto-Indicator Sharing and Auto-Response Across Multiple Enterprises



Community members have protected and/or mitigated within minutes



IACD Community of Trust

Best Case

Indicator → Detect/Decide → Self-Defense → Auto-Indicator Sharing → Community Members Protected

< 1 minute

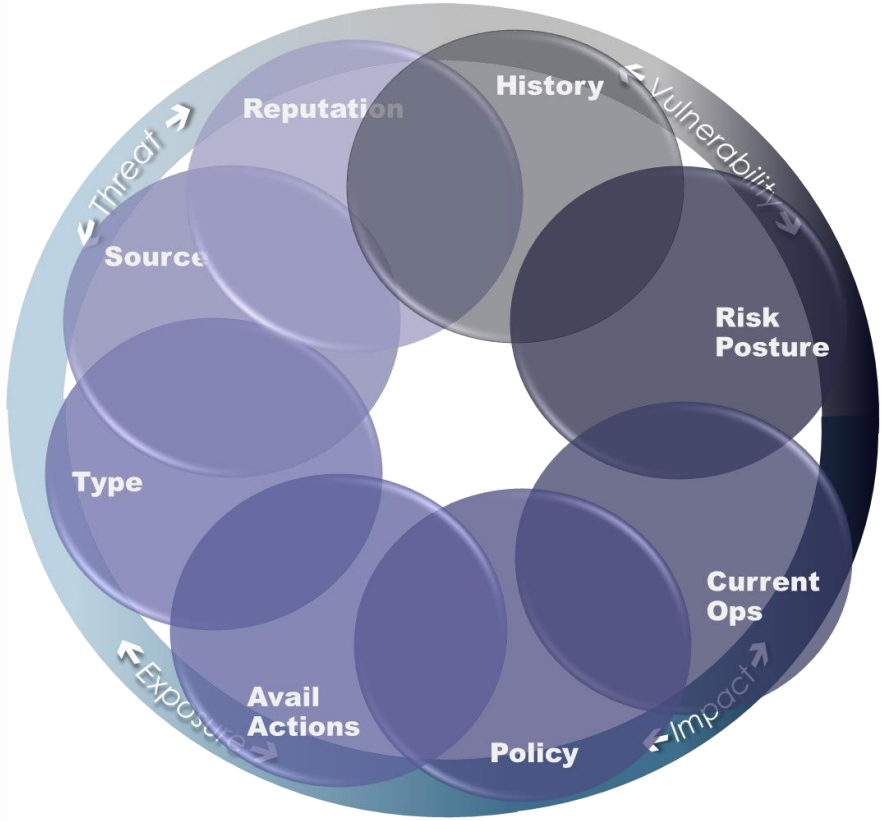
"Worst" Case

Indicator → Detect/Decide → Self-Defense → Auto-Indicator Sharing → Community Members Protected

3 -45 minutes

Spiral 2 Outcomes:
Diversity and Capacity for Automated Indicator Handling

Indicators Processed		
Today	Past Week	Average/Day
295	944	135



- Added Parsing/ Ingest DIB Alerts in addition to STIX
- **10-40x** increase in typical indicator processing volume

Implications:
Scaling to increased volume of indicators via ISAOs achievable

Spiral 2 Outcomes:
Speed/Efficiency of Indicator Processing

Indicators Processed		
Today	Past Week	Average/Day
295	944	135

Indicators Processing Time (seconds)		
Average Time	Minimum	Maximum
50	6	207

- 15-70x faster than analyst-reported times
- No wait time/lag time for analyst handling other priorities

Implications:
Operational resources can be re-directed to high impact/risk areas

Indicator-to-action timeline significantly reduced

Spiral 2 Outcomes:
Degree of 'Selectable' Automation Achievable

Indicators Processed		
Today	Past Week	Average/Day
295	944	135

Indicators Processing Time (seconds)		
Average Time	Minimum	Maximum
50	6	207

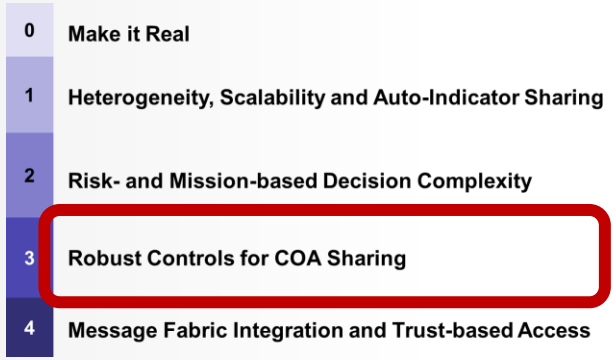
Response Action Recommendations & Automation (Today)		
Total Recommended	Number Automated	% Approved for Automation
561	416	73.98%

- Over 70% of recommended actions could be auto-applied using conservative criteria
- 'Auditable' path/process identified for 'proving' or validating recommendations for future automation

Implications:
Significant time/resource savings achievable even in 'non-automated' uses

Integration/Exploration Through Spiral 3

Looking Ahead



Spiral 3 Themes

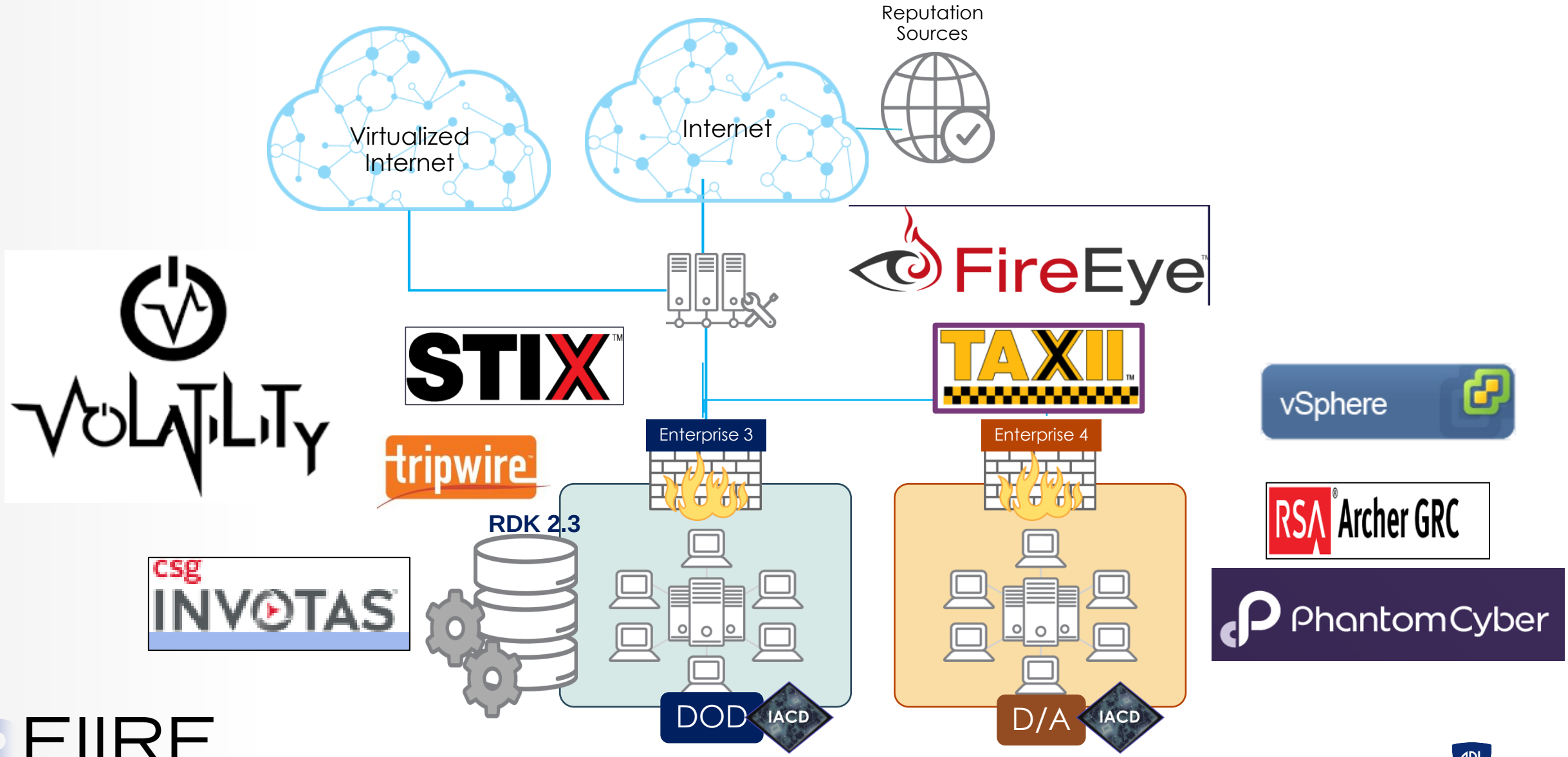
Robust Controls

Expanded Decision Making Complexity

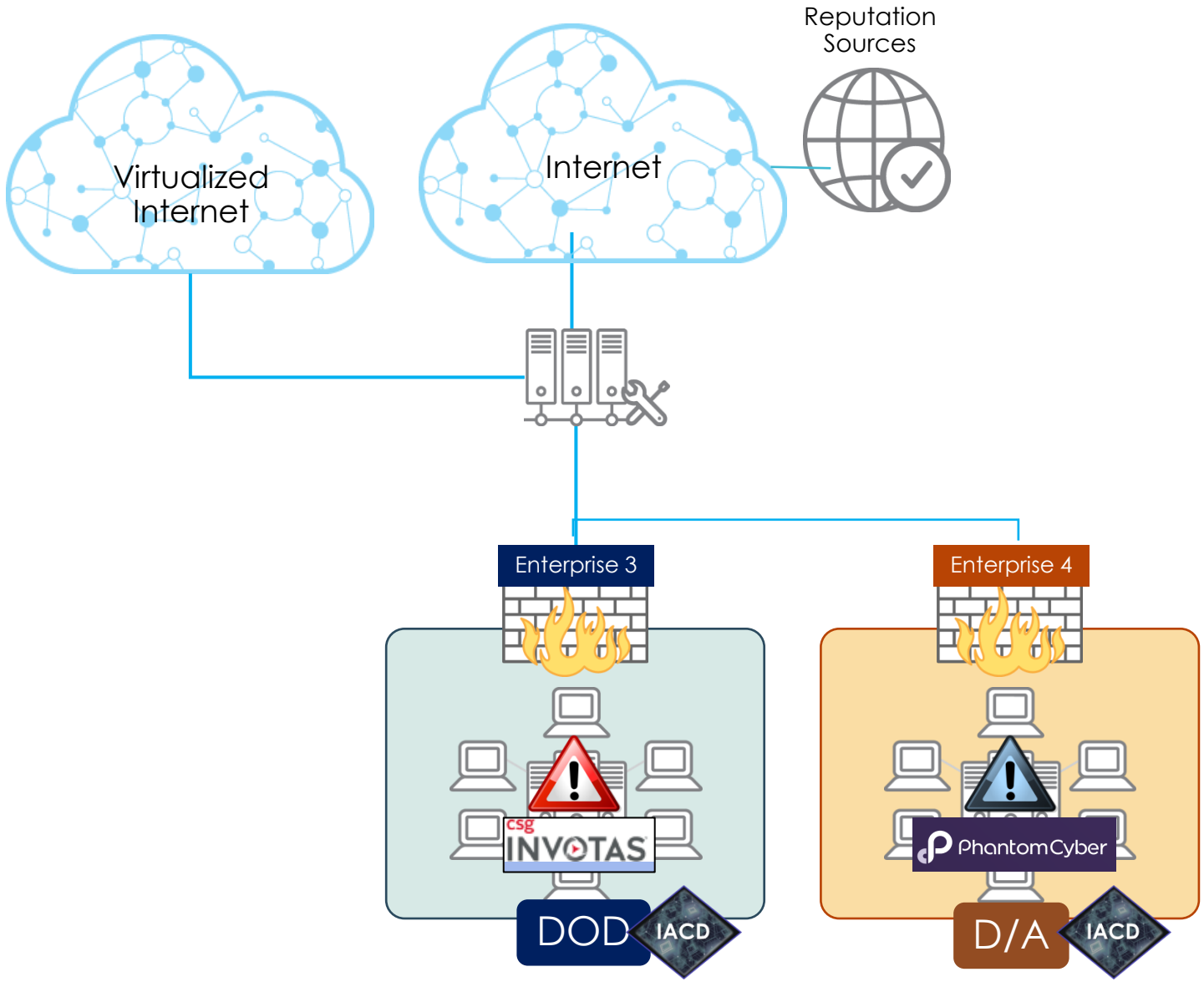
COA/Workflow Sharing/Interoperability

- **Increase number of response actions supported**
- **Diversify defense approaches – expand from data- and network-driven IACD to person/persona and application level for sensing and acting**
- **Begin to explore COAs/create conditional controls that stress the ability to manage responses**
- **Explore use of STIX to exchange COAs across different enterprises, using different orchestration tools**

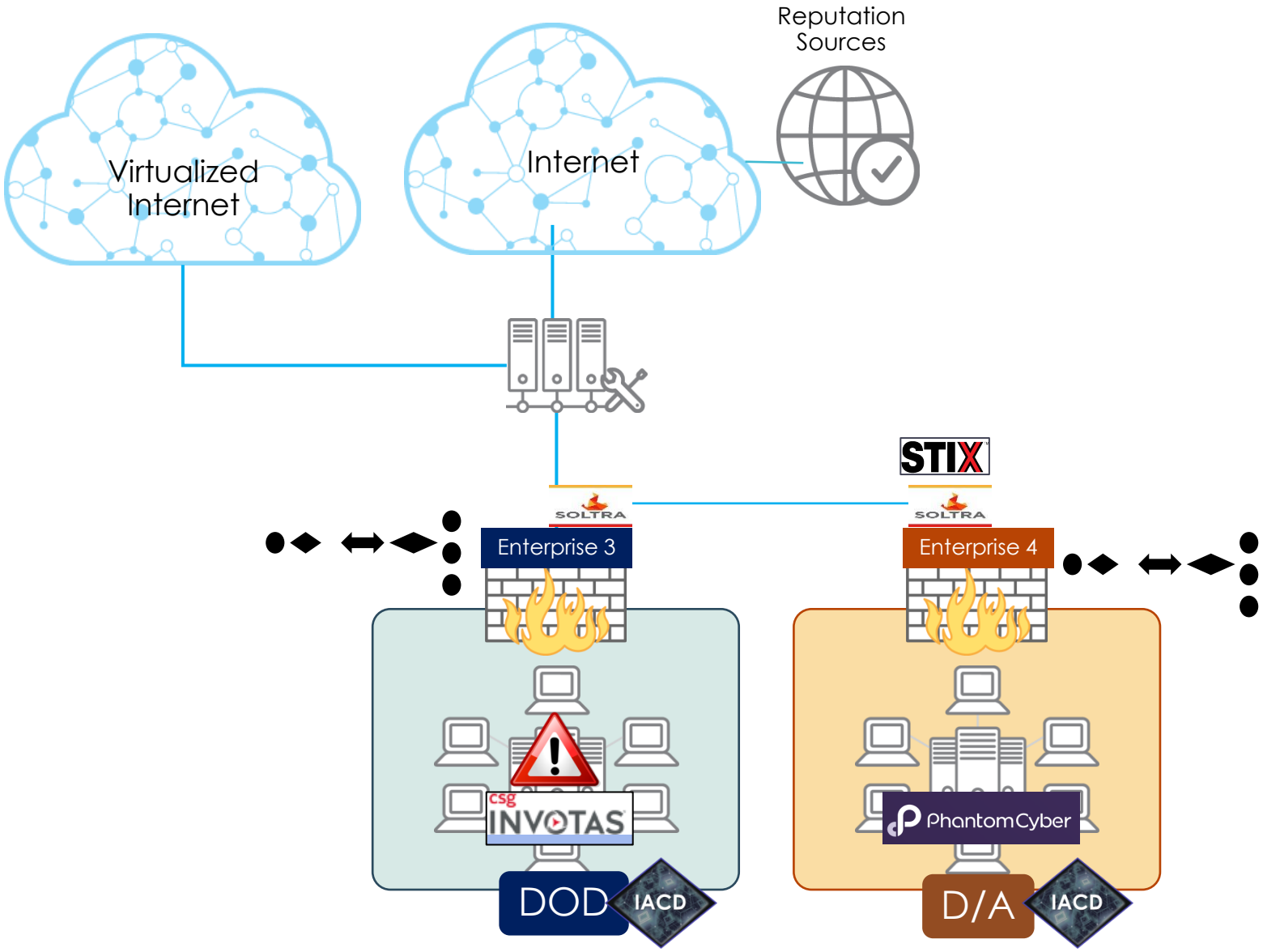
Spiral 3 FIIRE Configuration



Spiral 3 Emphasis: Increased Decision and Control Complexity
Mission Drivers, Behavior-derived Decisions



Spiral 3 Emphasis: Explore Cross-Enterprise Sharing of COAs



Spiral 4 Early Plans

- Continue to evolve COA sharing and COA command/message structure (maintain Spiral 3 FIIRE configuration)
- Add distinct message fabric/control plane mechanism to begin to elicit performance and access control requirements
- Set groundwork for cloud-based service/thin client environments in future spirals;

Discussion