The Methodology of Managed Incident Prevention & Response [MIPR]:

Examining the Evolution of CERT Operations

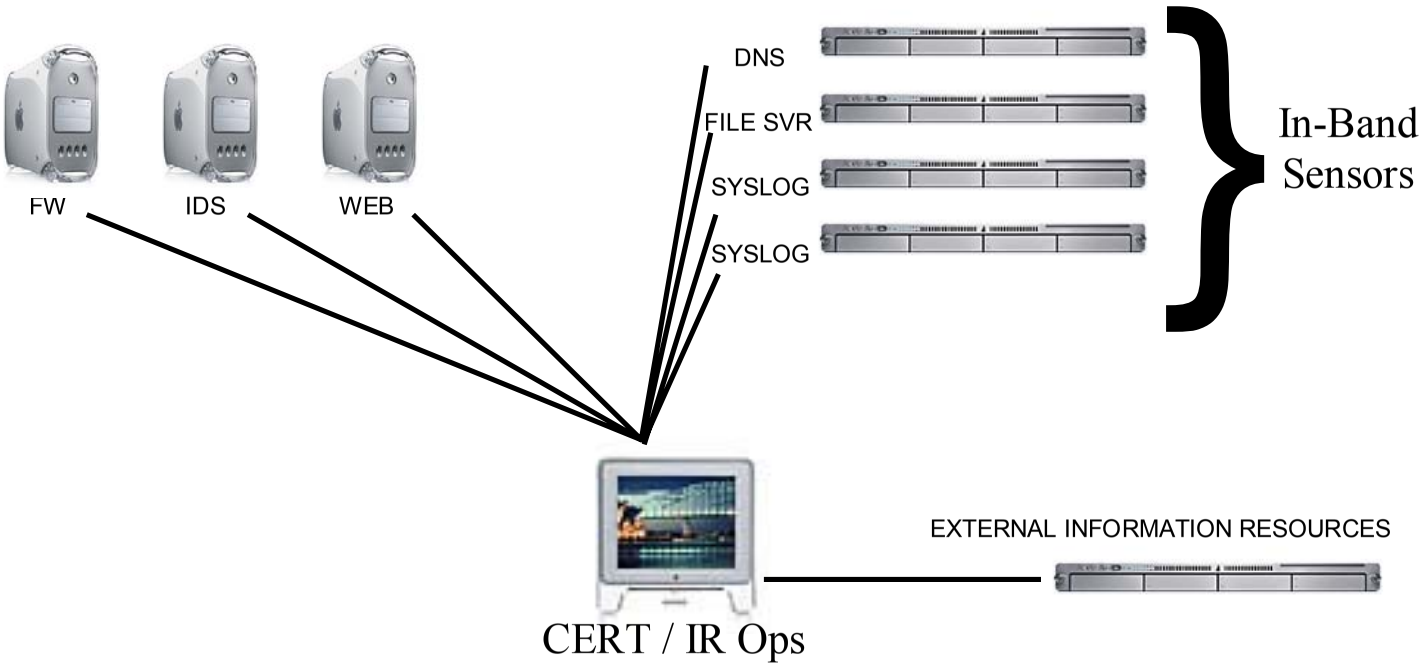
by Robert J. Bagnall
Director of Intelligence Operations
iDEFENSE, Inc.

Contents

- The CERT Today
  - Current CERT Architecture
  - Significant Existing Issues
- The Missing Links:
  - Unplugged Security Leaks [the “SODATA”]
  - End-user Awareness, Policy, & Enforcement
  - [Automated] Correlation & Corroboration
  - Correlation Out-of-Band
  - Intelligence, not simply information
  - Behavioral Modeling
  - Other Factors
- The Complete IR Operations Process

Contents

CERT Operations Architecture Toda



The CERT Today

- Significant Existing Issues:
  1. Extremely Poor Event Visualization
  2. Limited Metrics Compilation
  3. No Behavioral Modeling
  4. No Correlation-Out-of-Band
  5. Lack of Interoperability [COTS]
  6. No Standardized Content Delivery
  7. Personnel Experience Must Make Up Gaps

7 Offensive Data Aggregation Techniques for Attacks: The "SODATA"

Unnecessary Information Leaks [UILs]

Data Disposal Policy & Enforcement [D2]

Bandwidth & Data Flow [B&D]

Organizational Behaviors [OBs]

Terminated Access Controls Enforcement [TACE]

New Systems Identification & Discovery [NSID]

Configuration Management & Maintenance [CMM]

End-user Awareness, Policy, & Enforcement

- STOP IGNORING END-USER AWARENESS!
- End-user awareness = greater security
- End-user awareness = end-user accountability
- Accountability = legal protection for the corporation
- Accountability is not possible without a comprehensive, yet digestible corporate security and acceptable use policy
- Enforcement, like other information gathering, should be 75% automated and 25% human oversight

[Automated] Correlation & Corroboration

- Let the technology do what it does best
- Incorporate behavior
- Match it against history
- Eliminate what you know and what you can predict and that will leave you with what you don't know
- Infuse information & refine it into intelligence

Correlation Out-of-Band

- Merge biometric, access card, and other physical access data with cyber-security infrastructure
- Gather accessibility information on all portable devices and secure each individually
- Compare user & group access information versus real-time access data on critical servers

Intelligence, Not Information

Effective Intelligence requires both human and automated resources to discern actionable intelligence from available data by utilizing network information correlated with open source reporting and corroborated by a fundamental understanding of historic enterprise behavior, organizational presence in the world-at-large, and outsider threats.

Enterprise Operational Data
Behavioral Modeling
All-source Information
Understanding of the "Brand"
Knowledge of Opponents

} =

Efficient, Timely Decision Making

Know Your Enemy, Know Yourself, and Win the Day

Behavioral Modeling

Behavioral Modeling is second only to an established end-user awareness program in both importance and how frequently it is overlooked by organizations.

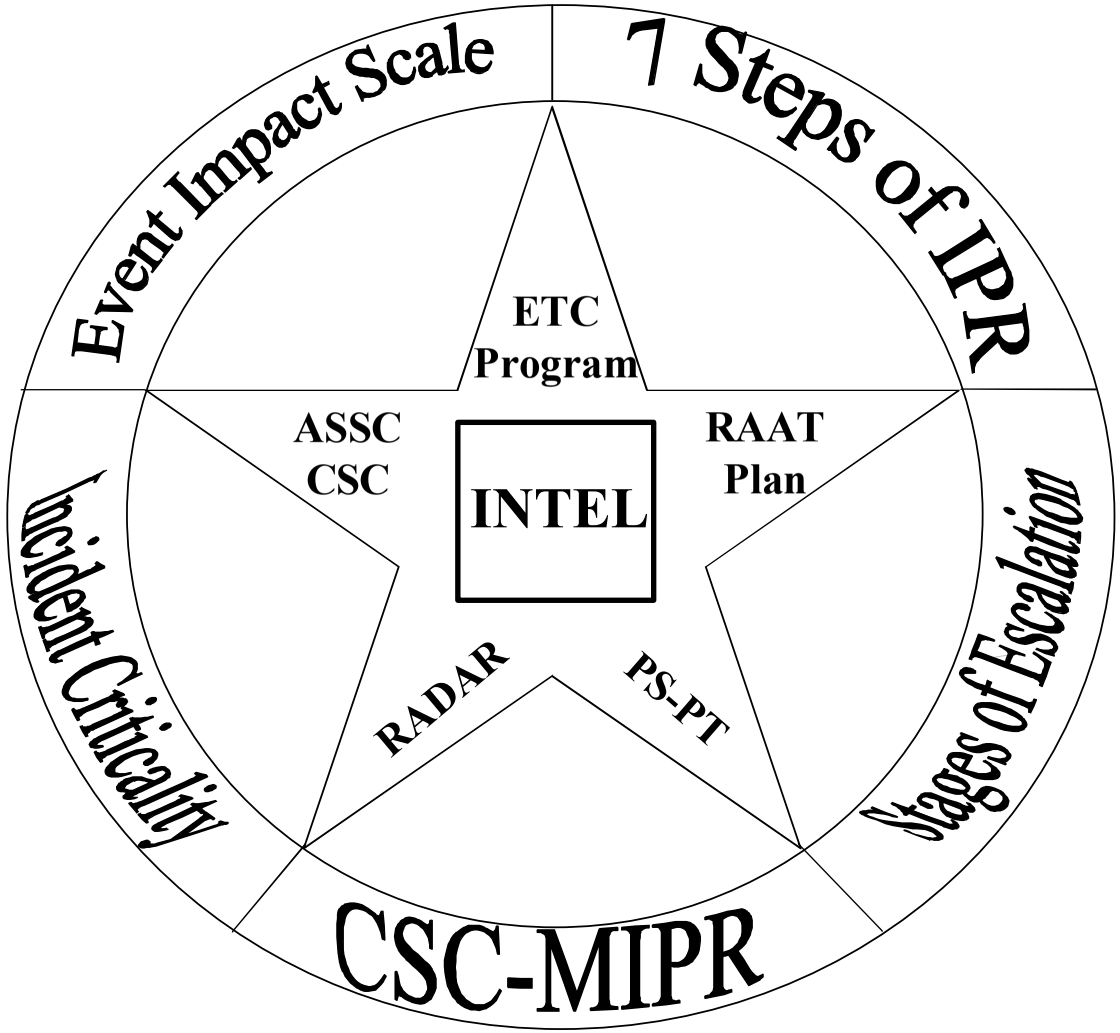
Behavioral Modeling consists of:

1> monitoring daily enterprise use and function
2> establishing strong, easily understood corporate acceptable use policy
3> writing policy enforcement agents to crawl the system
4> shutting off unnecessary ports, services, shells, etc.
5> establishing a database of enterprise architecture functionality
4> linking policy to agents to alert on violations
5> linking sensor alerts to system behaviors & system behaviors to agent alerts
6> educating enterprise end-users on cyber-security awareness
7> linking agents to training & certification tracking as well as violations by users

21 Pieces to A Complete IR Operations Process

MSS Monitoring	Intelligence	Correlation Out-of-Band
Correlation	Behavioral Modeling	Config Management & Maint.
Corroboration	Scans, Risk Assessments, IV+V	Malware Defense
Historical Analysis	Threat Impact Ratings	Atypical/ Asymmetrical Defenses
Profiling	Con Plan & Disaster Recovery	Visualization
Health & Welfare	Metrics	Prevention
Analysis & Assessment	Reporting	Training

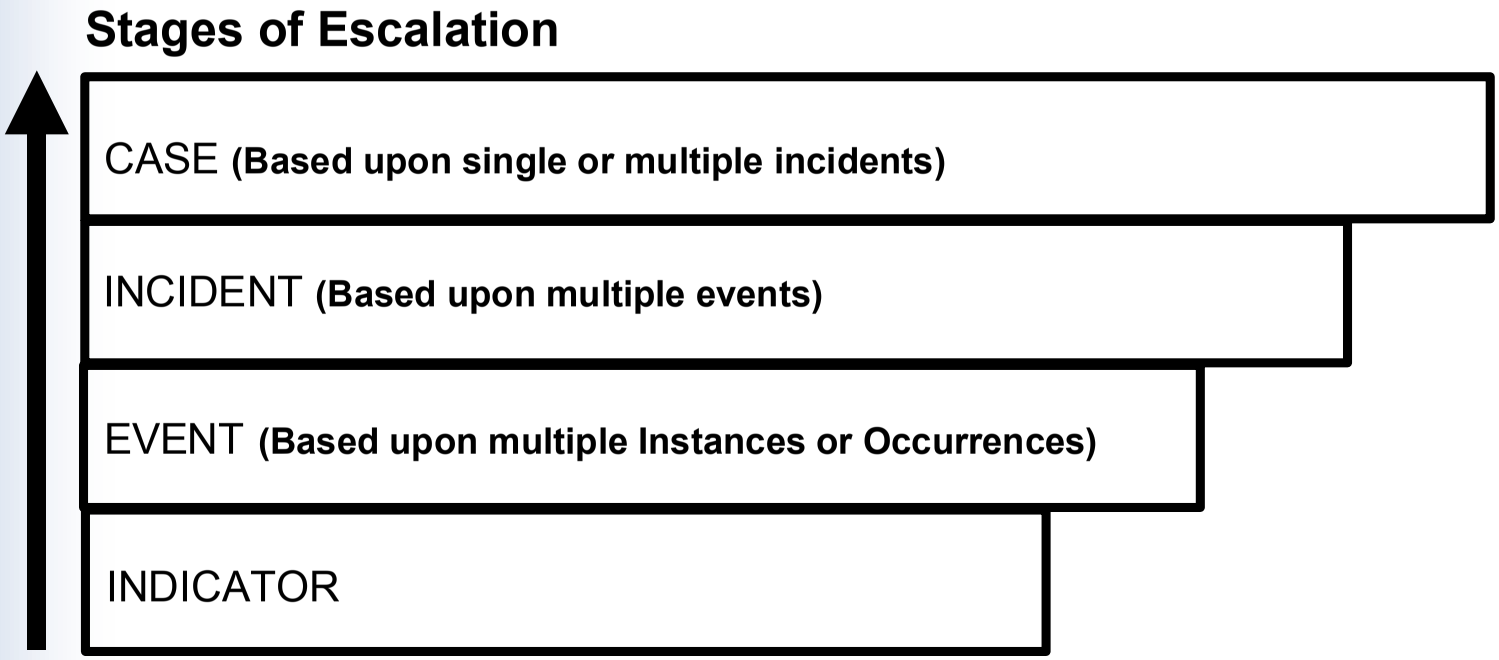
The MIPR Methodology



The 7 Steps of Incident Prevention & Response

1. **Data Collection** [from the user to the enterprise level]
2. **Intelligence Integration** [profiling & all-source reporting from external forces]
3. **Behavioral Infusion** [from system to user to attacker to nation state]
4. **Collation Analysis** [What does all the data tell us? What is the Ņbig pictureÓ?]
5. **Resultant Action** [What do we do about it?]
6. **Conclusive Reporting** [Here is what we did about it Š plays into behavioral infusion in the future]
7. **Operations Review** [What do we fix/adjust [if anything]?]

Stages of Escalation



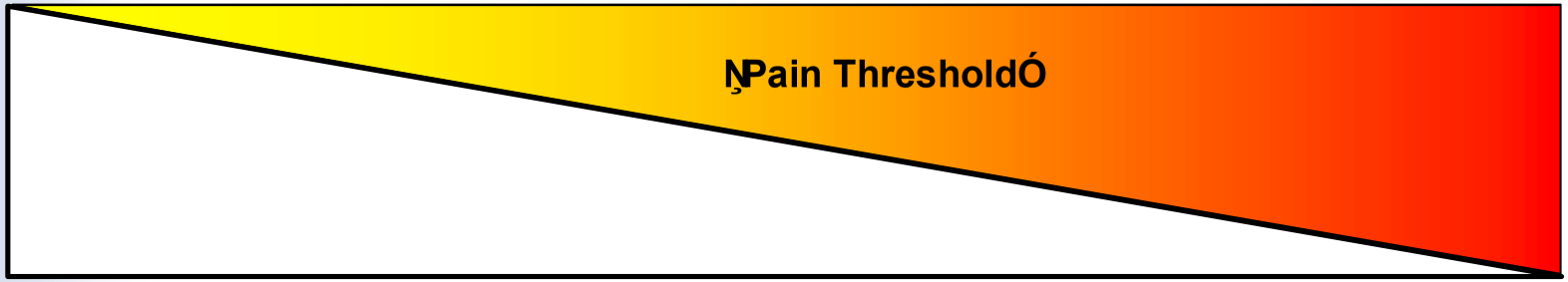
Defined Incident Criticality

Incident Criticality definitions are stated here to provide a basic template for understanding the level of threat an individual incident poses to the target enterprise. Where ICs are already predefined by the customer [ie: DoD-CERT], the MIPR adopts the customer process.	
Incident Criticality	**Definition**
Critical	Incident has a significant negative impact on security posture or continuous enterprise operations and requires immediate action.
Suspicious	Incident poses a threat to the security posture or continuous operation of the enterprise and requires investigation.
Notable	Incident exhibits anomalous behavior and requires analysis to determine its legitimacy.

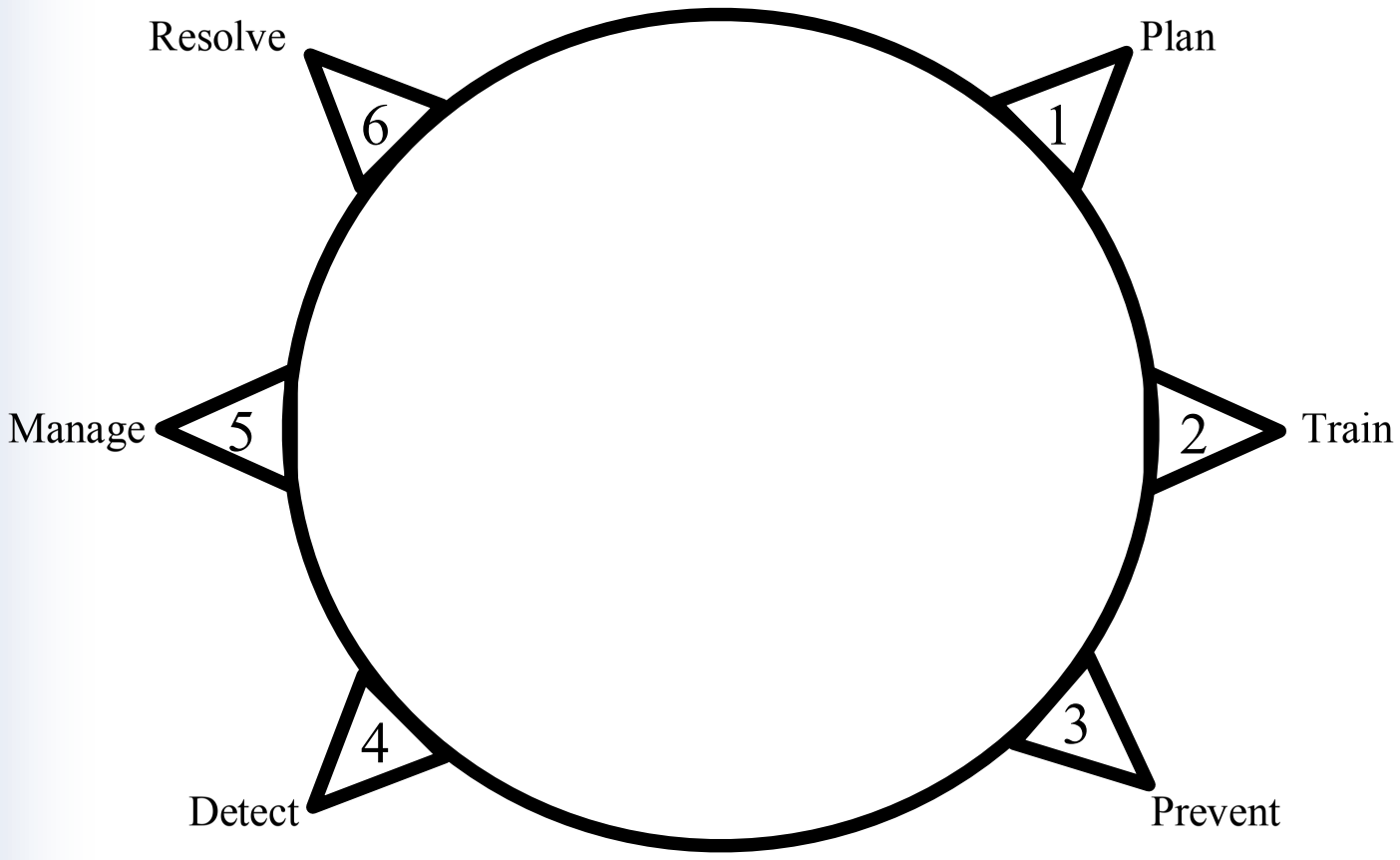
Event Impact Scale

Event Impact Scale

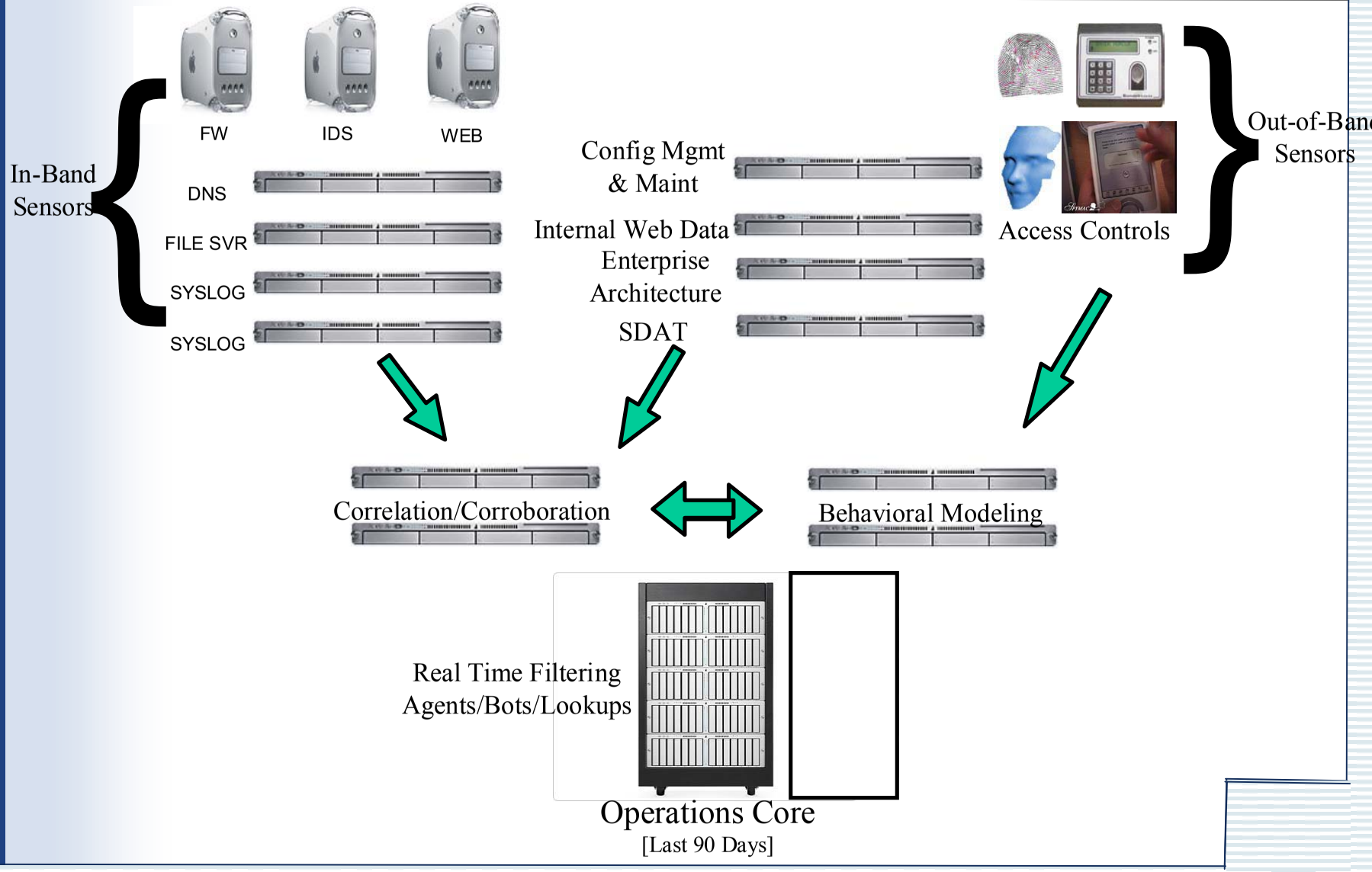
IRRELEVANT	KNOWN	UNKNOWN	KNOWN	UNKNOWN
	PREPARED FOR	PREPARED FOR	NOT PREPARED FOR	NOT PREPARED FOR



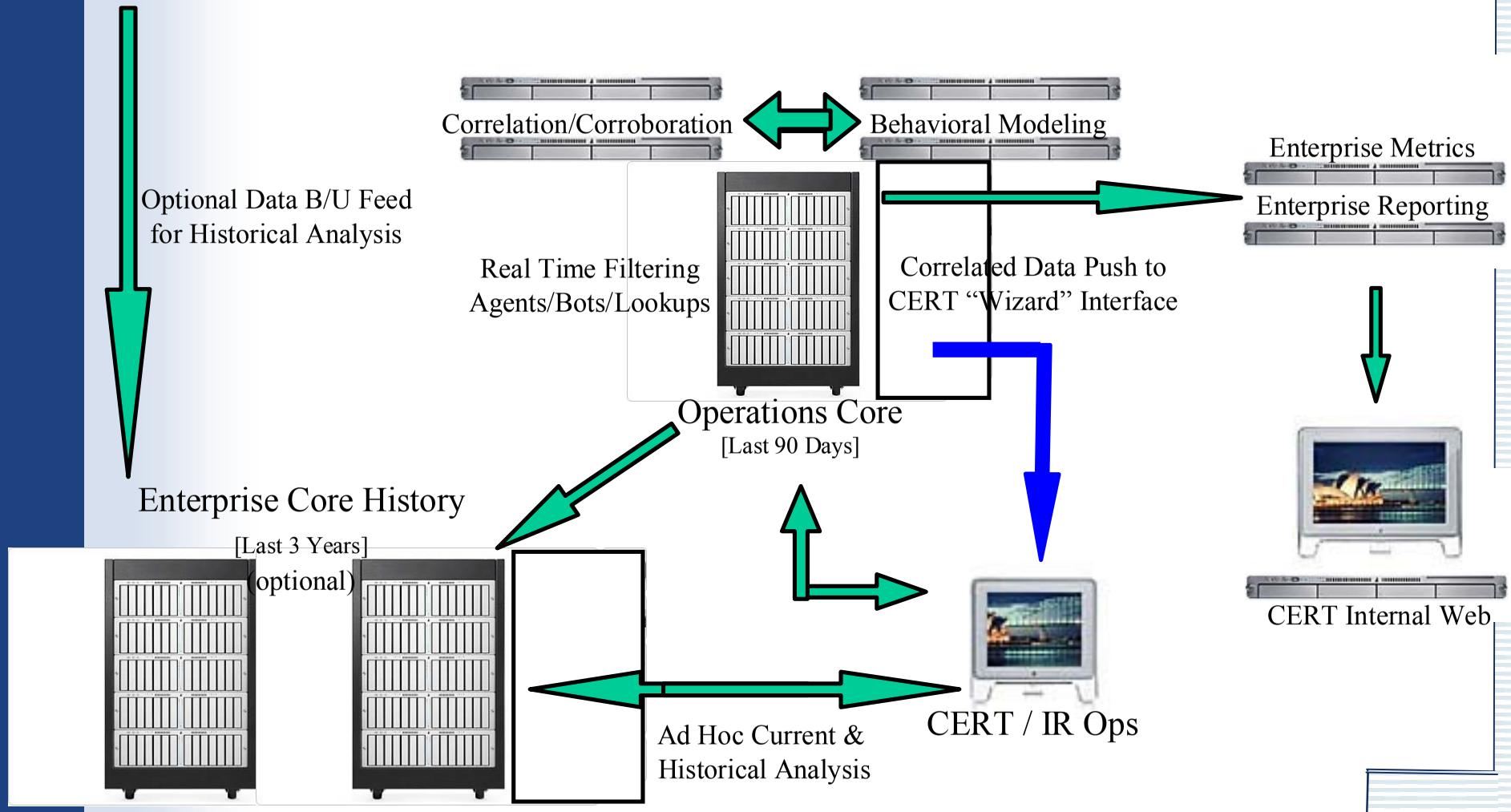
The MIPR Wheel of Event Handling



CERT Operations with MIPR



CERT Operations with MIPR



CERT Operations Process with MIPR

INDICATOR

Trigger of some sensor, in-band, out-of-band,etc.

Indicator Preprocessing
Phase 1 Correlation & Corroboration
A> Information Gathering
B> Historical Behavioral Analysis
* SDAT
* NetCraft
* NIC Lookups

Metrics & Reporting

Phase 2 Correlation & Corroboration
A> Behavioral Modeling
B> Policy Enforcement
* Recently deemed acceptable/not
* New admin acct setups after hours
* Acceptable use violations

Behavioral Modeling & Policy Enforcement

CERT Internal Web

Alert Processor

Data Push to 5-Step CIWI Wizard
A> Level 1 Analysis
B> Incident Handler Analysts
C> Case decisions & escalation made here based upon human oversight

CERT Analysis Level 1

Collected Intelligence Feed

Level 2 Case Investigations
A> Security Engineers Investigate
B> Step thru as follows:
* Manage & Mitigate
* Implement Updates & Fixes
* Close & Resolve

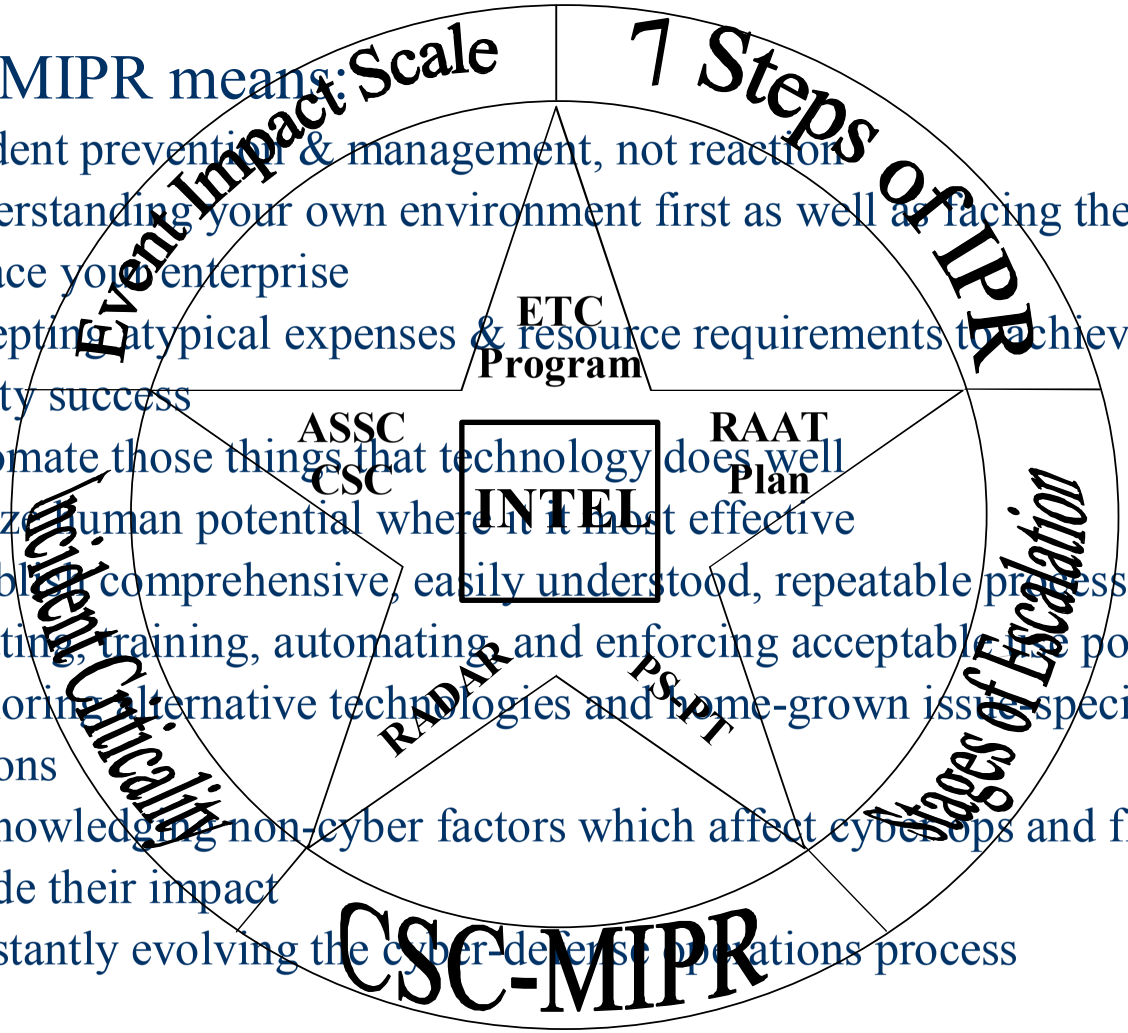
CERT Analysis Level 2

The MIPR "IR Wizard" & Other Interfaces

- The IR Wizard Interface
  - Steps analysts thru incident management "your way"
  - Pushes data, reducing response times
  - Correlates & corroborates automatically [where practical]
  - Auto-generates metrics & reporting
- The End-user Dashboard
  - Policy Enforcement & Training
  - Alerts, news items, & corporate announcements
  - One-stop shop of pushed intelligence & controlled media
  - Pop-up violation reminders
- Agent & Security Administration/Reporting
  - Agent scheduling, creation, evolution, & management
  - Metrics collation
  - Operational reporting

Conclusion

- The MIPR means:
  - Incident prevention & management, not reaction
  - Understanding your own environment first as well as facing the threats that face your enterprise
  - Accepting atypical expenses & resource requirements to achieve real security success
  - Automate those things that technology does well
  - Utilize human potential where it it most effective
  - Establish comprehensive, easily understood, repeatable processes
  - Creating, training, automating and enforcing acceptable use policy
  - Exploring alternative technologies and home-grown issue-specific solutions
  - Acknowledging non-cyber factors which affect cyber ops and flexing to degrade their impact
  - Constantly evolving the cyber-defense operations process



Questions?

?