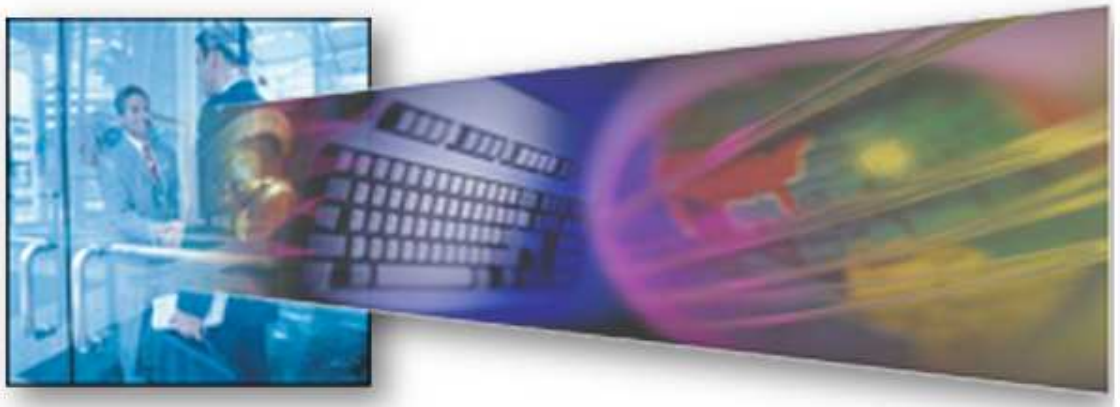
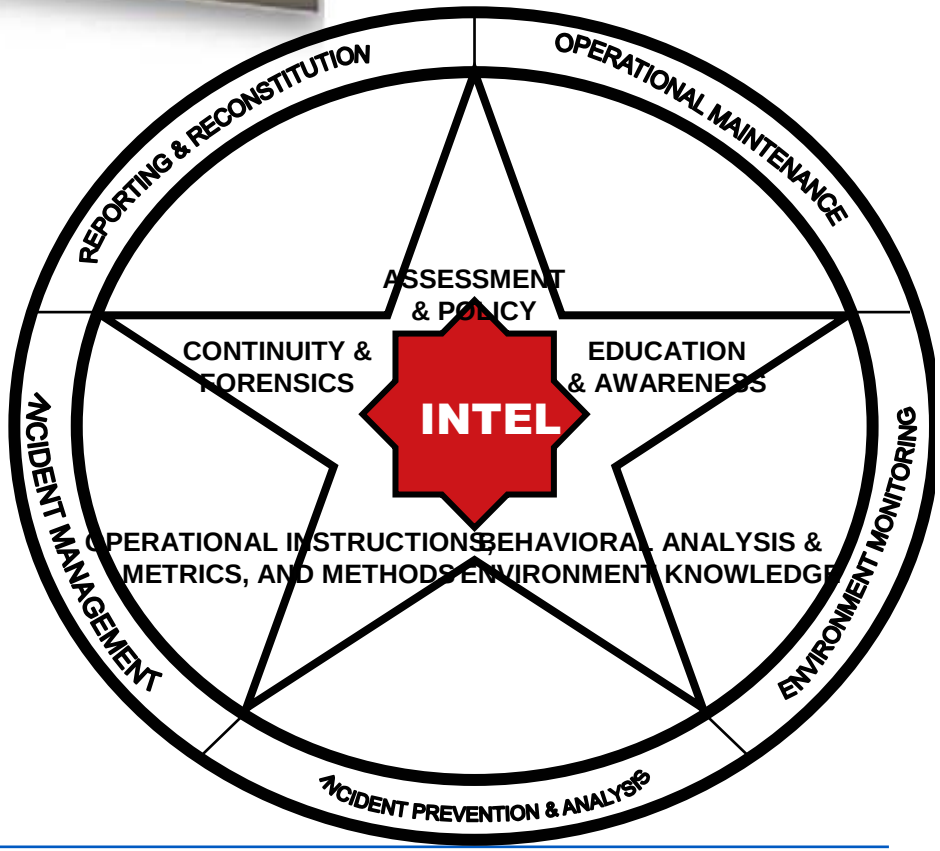
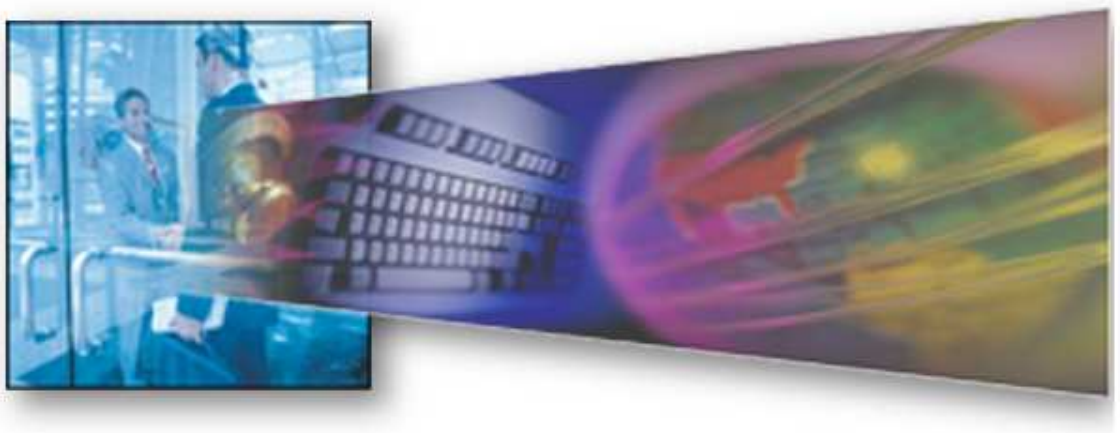


RANGER:

Incident Management & CERT Operations Methodology





Presented

by

Robert J. Bagnall

Deputy Director of Managed Security Services

SAIC

robert.j.bagnall@saic.com

202-302-1900

DISCLAIMER:

The RANGER IPR Methodology is ©MUSE iNNOVATIONS 1999-2004. Robert Bagnall is solely responsible for its content. SAIC, a market leader in Managed Security Services, is reviewing but has not yet adopted or selected RANGER as a core methodology for its global MSS operations. Any inquiries, suggestions, or comments should be directly solely to Robert Bagnall.

Contents

- The CERT Today
- The Missing Links
- Critical Components to A Complete IR Ops Process
- Remaining Problem Areas
- The Original MIPR IR Operations Process
- The Stages of Escalation Standard
- Incident Criticality Standard
- The Event Handling Delta
- 7 Critical Steps to Effective Incident Prevention

Contents

- The New RANGER IR Operations Process Defined & Explained
- Operations
- Process
- ROI & Profitability
- So Where Do We Start? Phase-1
  - Security Policy
  - End-User Training & Awareness
  - New System Fielding Decision Flowchart
- Then What? Phase-2
  - The Need for A Wizard Analyst Support Interface
- How It All Comes Together
- Conclusion / Questions

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 Standards for Security Measurement

  7. No Standardized Indicator or Event Handler Delivery or Presentation Method

  8. No Effective Measurement for Realizing Security ROI

  9. A Lack of Environmental and Global Intelligence

  10. Personnel Experience Must Make Up Gaps

The CERT Today

- **Other Existing Issues:**

  1. **Information Leaks**
  2. **Information Aging & Disposal Procedures**
  3. **No Bandwidth or Data-Flow Knowledge**
  4. **Environment Mapping & New Systems Discovery**
  5. **Configuration Management (Fielding, Updating, and Patching)**
  6. **Access Control Enforcement**
  7. **No Credible End-User Awareness or Education at Most Locations**
  8. **No Effective Measurement for Realizing Security ROI**
  9. **A Lack of Environmental and Global Intelligence**
  10. **Personnel Experience Must Make Up Gaps**

Components of 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
Environment Health & Welfare	Metrics	Prevention
Analysis & Assessment	Reporting	Training

Behavioral Modeling

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

Behavioral Modeling consists of:

1> monitoring daily enterprise use and function
2> establishing & enforcing 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 & missions
6> linking policy to agents to alert security personnel of violations
7> linking sensor alerts to system behaviors & system behaviors to agent alerts
8> educating enterprise end-users on cyber-security awareness
9> linking agents to training & certification tracking as well as violations by users
10> linking behaviors to indicator pre-processing during event correlation

Correlation Out-of-Band

- Incorporate physical and cyber security team operations to facilitate better early detection & prevention
- 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 of critical systems
- Compare COB data to Behavioral Metrics over time to facilitate anomaly detection earlier

Automated Correlation & Corroboration

The goal of indicator pre-processing is to utilize an intimate knowledge of the environment over time against known behaviors to separate anomalies earlier and, thus, reduce the "signal-to-noise" ratio which the analyst must examine. Effective behavior metrics gathering and analysis, intelligence infusion for attack and modus operandi pattern matching, will only increase the accuracy of this step over time.

- **Let the technology do what it does best: crunch numbers and gather, store, and correlate data**
- **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 outside intelligence for early detection pattern matching**

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

Intelligence, Not Information

Example-1: with only information

The CERT team discovers an acceptable use violation from a perimeter IDS system. They record the IP and, through some lengthy network discovery, discover the offending username and location. Then they call the physical security team and send two guys over with a security admin to talk to the man's supervisor about removing him. But the supervisor says that the user is out-of-town on travel and has been for two days.

Example-2: with real intelligence

The CERT team is alerted to an acceptable use violation from a perimeter IDS system. The IP is immediately cross-checked against the enterprise mission & function document which lists every IP, system, and its mission, function, and location. The system also automatically checks the server in the physical security area which services the swipe card system. It notices that the user in question has not logged in for two days. The system also notes to the analyst that this user account is NOT currently logged into the RAS dial-in server. The analyst then compares the activity against the daily intelligence archive of known vulnerabilities, malware, and cyber-threat data. The activity does not match any known recent attack activity, so the team contacts the supervisor, quarantines the system, and begins investigative measures.

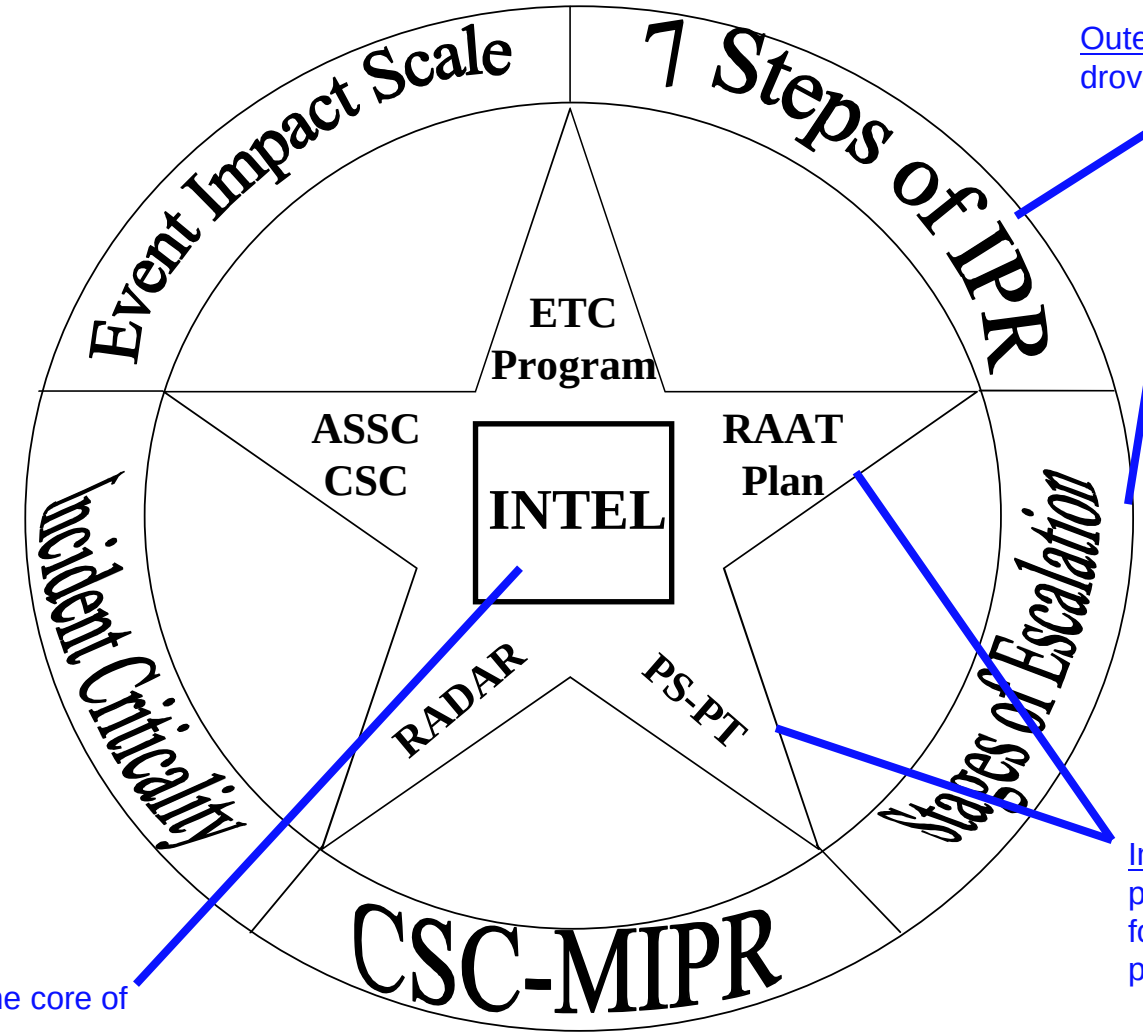
Visualizing the Threat

Human beings visualize much more efficiently than they crunch raw data. As refined, correlated, and corroborated information helps the analyst take the final steps to creating intelligence, deeper signal-to-noise reductions and greater time savings during the analysis phase of an event investigation can be achieved through visualization. Like the transition from the command line to the Graphical User Interface (GUI), intelligent information visualization is slowlyy replacing pure data feeds on the analyst console.

Visualization of various indicators, correlated with and corroborated by other information types, can offer a more immediate situational awareness picture - one where anomalies more readily stand out. They can be spikes of data, or color-coded based upon pre-process programming, or even flash when certain thresholds or policy limits are met.

Visualization also supports the proper and simple digestion of metrics and reporting data for non-technical personnel. This is key in demonstrating effective situational awareness within an operations center as well as for making the case for

The Original MIPR Methodology



Outer Ring: Standards that drove the process.

Inner Star: Specialized programs that were the foundation of the process.

Intelligence: The core of the process.

RANGER:

The New Security Operations Center Process and Methodology

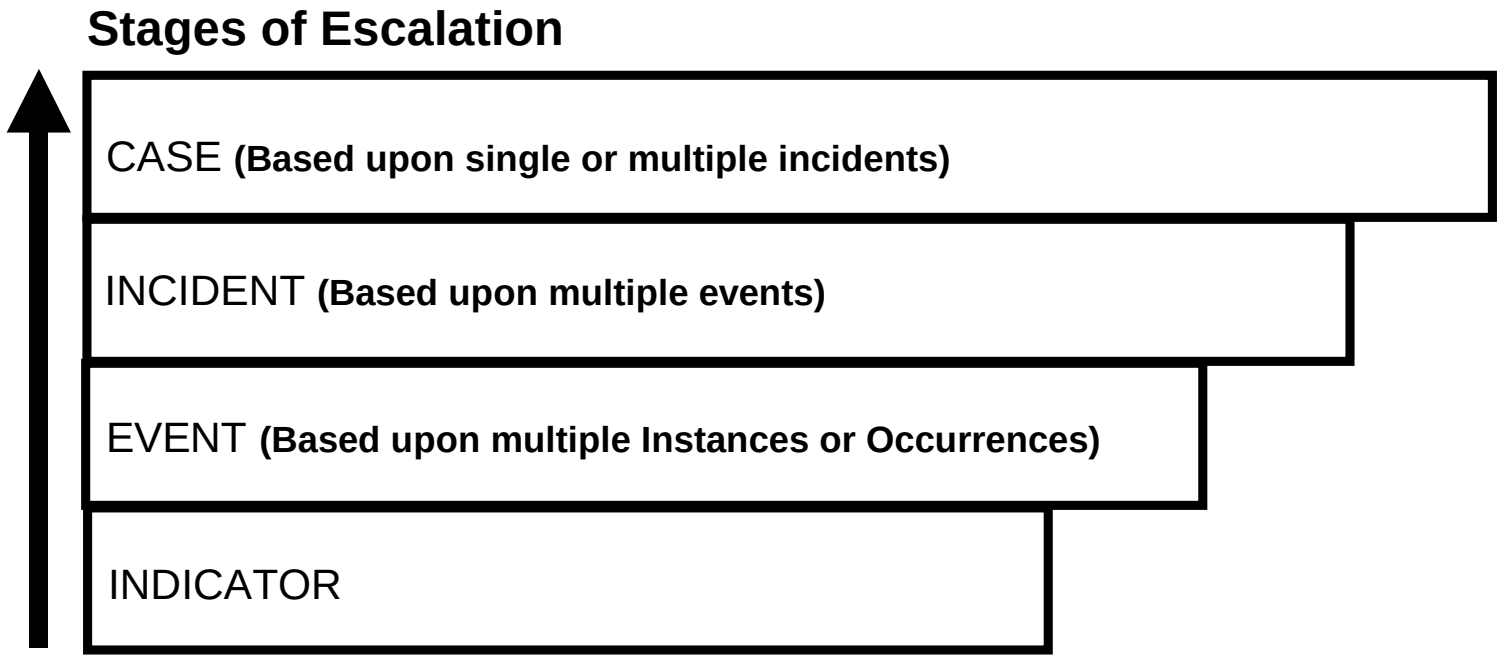
A Baseline of Standards

Operational Tasks

Operational Processes

A Focus on ROI

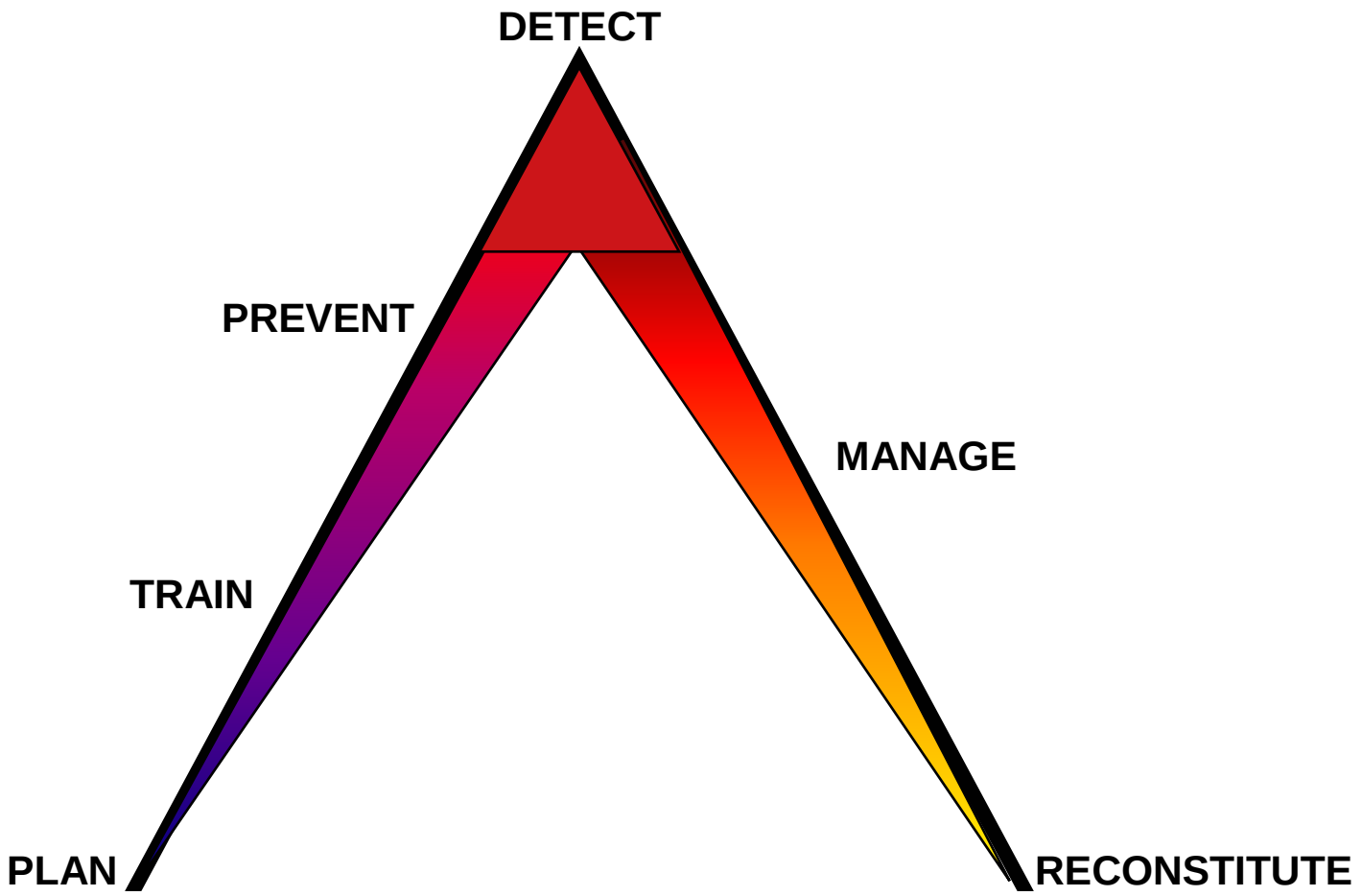
Stages of Escalation



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.

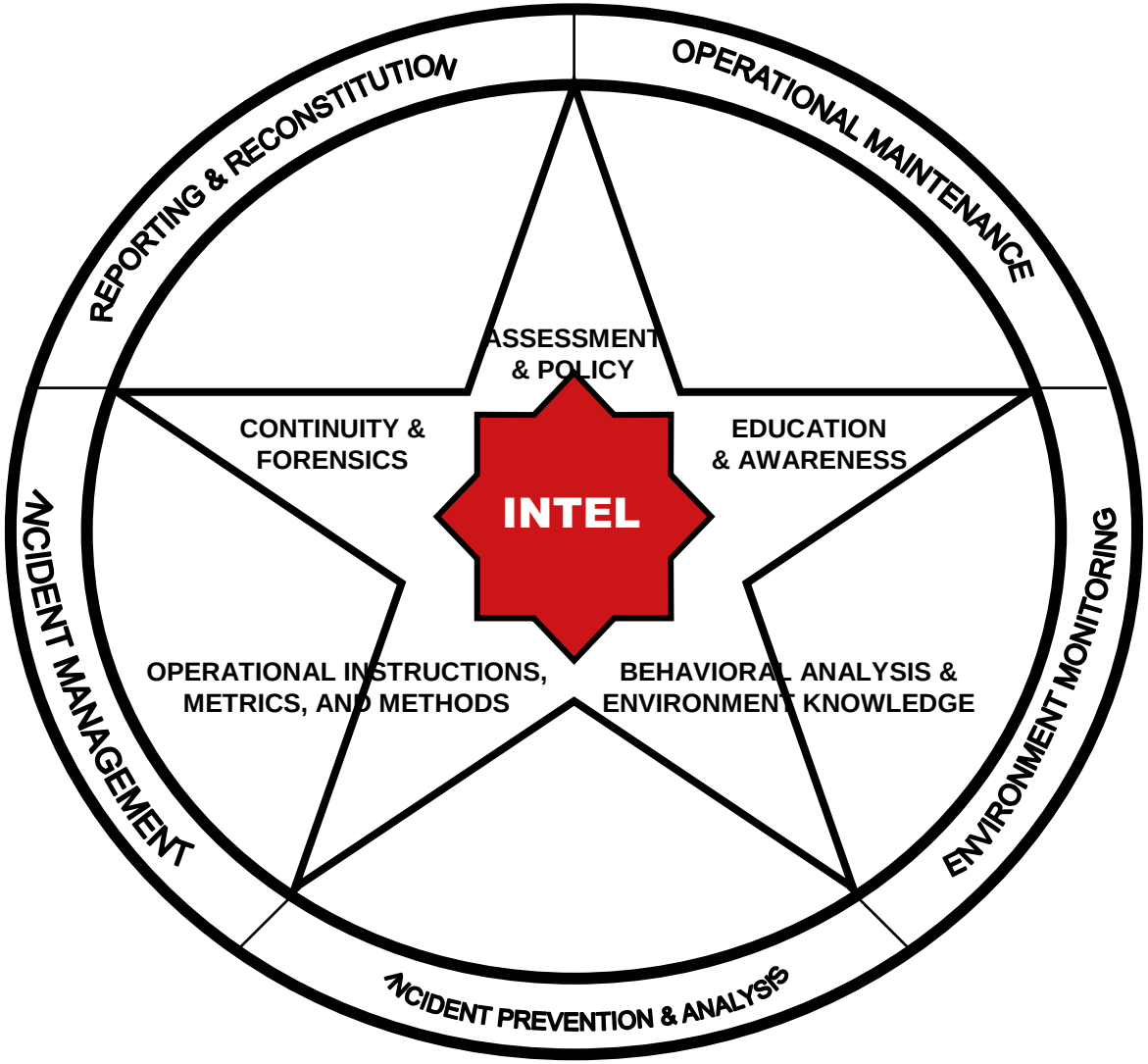
The Event Handling Delta



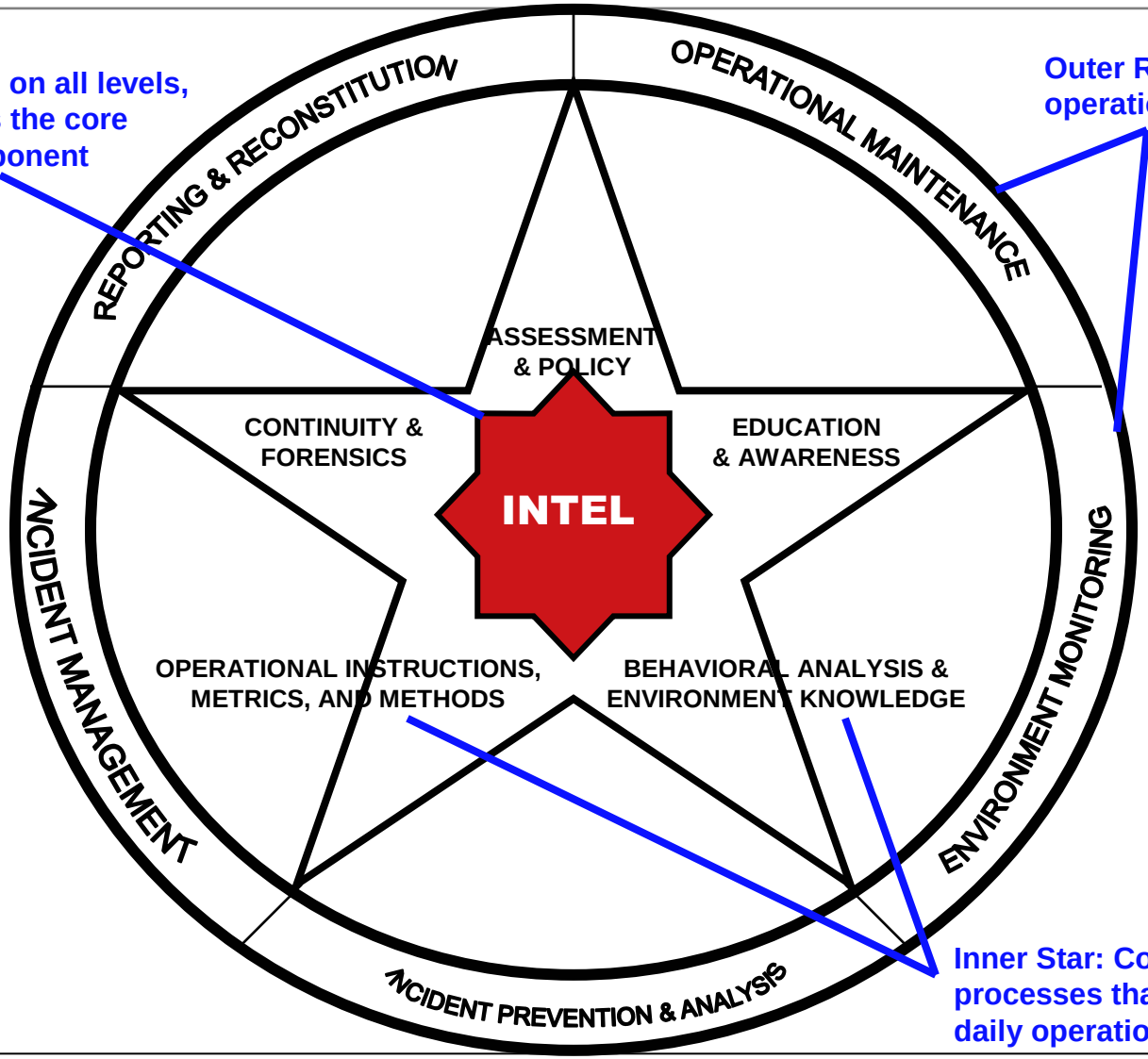
The 7 Steps of Incident Prevention & Management

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 Òbig pictureÓ?]
5. **Resultant Action** [What do we do about it?]
6. **Conclusive Reporting** [Here is what we did about it Ğplays into behavioral infusion in the future]
7. **Operations Review** [What do we fix/adjust [if anything]?]

The New RANGER Methodology



The New RANGER Methodology



Intelligence, on all levels, remains the core component

Outer Ring: Daily operational requirements

Inner Star: Cornerstone processes that facilitate daily operations

OPERATIONS

OPERATIONAL MAINTENANCE:

The process of keeping all systems, software, applications, specialized equipment, and personnel up-to-date, inventoried, categorized, baselined, and operationally current. This includes patches, hotfixes, physical systems and parts, environmental factors, personnel training & awareness, security policy, and other similar factors.

ENVIRONMENT MONITORING

EM includes perimeter and internal security devices, physical devices (such as facility access controls), wireless & other connections, bandwidth, and behavioral anomalies.

PREVENTION & ANALYSIS

PA is more than simply the process for assessing those items which have been escalated beyond indicator status. It is also the core goal of effective MSS/CERT operations. Prevention of security indicators before they become advanced, destructive incidents is the key to advancing operations from reactive today to proactive tomorrow.

OPERATIONS

SECURITY EVENT MANAGEMENT:

When potential security events cannot be prevented or mitigated prior to escalation to an actionable level, the resulting incidents must then be managed swiftly and effectively. If properly prepared, an organization will have numerous, tested scenarios which are supported by operational instructions that outline an organizationally-accepted course of action.

REPORTING & RECONSTITUTION

All indicators, events, incidents, and cases, regardless of their affect or level of escalation, are recorded for reporting purposes within the RANGER model. Reporting also includes less obvious, yet equally important, items like analyst time tracking by experience level, both in total and on a per-event basis, and such things as average time to manage or total volume by indicator type, targeted ports, services, and device types, etc. Reconstitution includes all measures, time, hours, efforts, etc. necessary to return to 100% operational capability on mainline systems and personnel. Reconstitution of critical systems, services, and personnel, should be examined as part of the assessment phase of the operations process.

PROCESS

SECURITY ASSESSMENT & POLICY

Credible security efforts begin with a fair, honest assessment of the state of the environment. Determining the current state provides a baseline by which realistic goals can be set and met over time. The assessment should include items such as accurate architecture mapping, environment inventories, connection verifications, critical systems and data identification, access control lists, and systems configurations. Once the assessment is complete, security policy can then be put in place to support the overall security goals of the organization. In the RANGER operations method, security policy is built in a template process, where the basic security theme of the document is covered in broad terms and specific addendums are attached to the end of the document to interpret the policy as it applies locally to an organization.

EDUCATION & AWARENESS

The single biggest gap in operational security today is the lack of investment in user education and security awareness by organizations. When implemented properly, E&A makes it possible to enforce security policy because the entire user base is made aware of their place and responsibility within the organization and receive periodic refresher training.

PROCESS

BEHAVIORAL ANALYSIS, ARCHITECTURE/MISSION AWARENESS

Behavioral analysis within the environment is a critical component to effective security operations. Without behavioral analysis, it is impossible to determine what behaviors within your environment are normal and which are anomalous. Nearly as important is having an accurate and intimate knowledge of the architecture of your environment. This knowledge includes a regularly-updated database of each system, its IP, mission, location, and type of OS.

OPERATIONAL INSTRUCTIONS, METRICS, & METHODS

OIs are crucial in providing security personnel with the basic template for what the organization expects to be done, in operational terms, for a given situation. The military uses OIs very effectively in equalizing the playing field between various levels of experienced personnel to ensure operational continuity regardless of who is at the helm, and this is no different. Metrics, as previously noted, are the key component in accurately determining important security factors such as normal-vs-anomalous behaviors, security effectiveness, and ROI. Other standards are missing as well, or must be evolved to meet emerging changes in the threat. Methods must become the new standards to meet those needs.

PROCESS

BUSINESS CONTINUITY & FORENSICS

As incidents are managed and resolved, the overall goal of security operations is to maintain business continuity. As a preemptive measure, organizations within the RANGER method will have templates of scenarios and suggestions for options, both within daily operations and failover, that allow for preventative measures to be in place where possible. Where not possible, scenarios for reduced-scale operations and reconstitution efforts are regularly tested within the organization.

The RANGER method also includes a forensic evidence preservation effort and preferred partner program for forensic investigation and recovery. Rather than house expensive experts in-house for only the rare occasional forensic investigation, RANGER training provides forensic evidence preservation training for normal IT and security staff with a plan to call in preferred expert partners as necessary. This is a more affordable option for organizations to realistically implement yet still meets the overall operational requirements of the organization.

PROCESS

NEW MEASUREMENTS & STANDARDS

The MAC >

The Malware Analysis Console is a standard for accurately rating malicious code, both at a general level and at the local level. Based on a tabular standard of community-sanctioned measurements, new malware is assessed and rated on a scale that is easy to understand and can be adjusted at the local level by security personnel who best understand their own environment.

SIMEN >

SIMEN rates the threat impact of new vulnerabilities against the environment. The rating results are simple and can be altered at the local level in a similar manner to the MAC.

The SPF >

Based upon five categories and over 20 individual factors, the Security Posture Factor assesses the security risk of an environment. The resultant score works like the SPF factor of sunscreen - the higher the score the lower the risk.

So Where Do We Start?

Phase-1

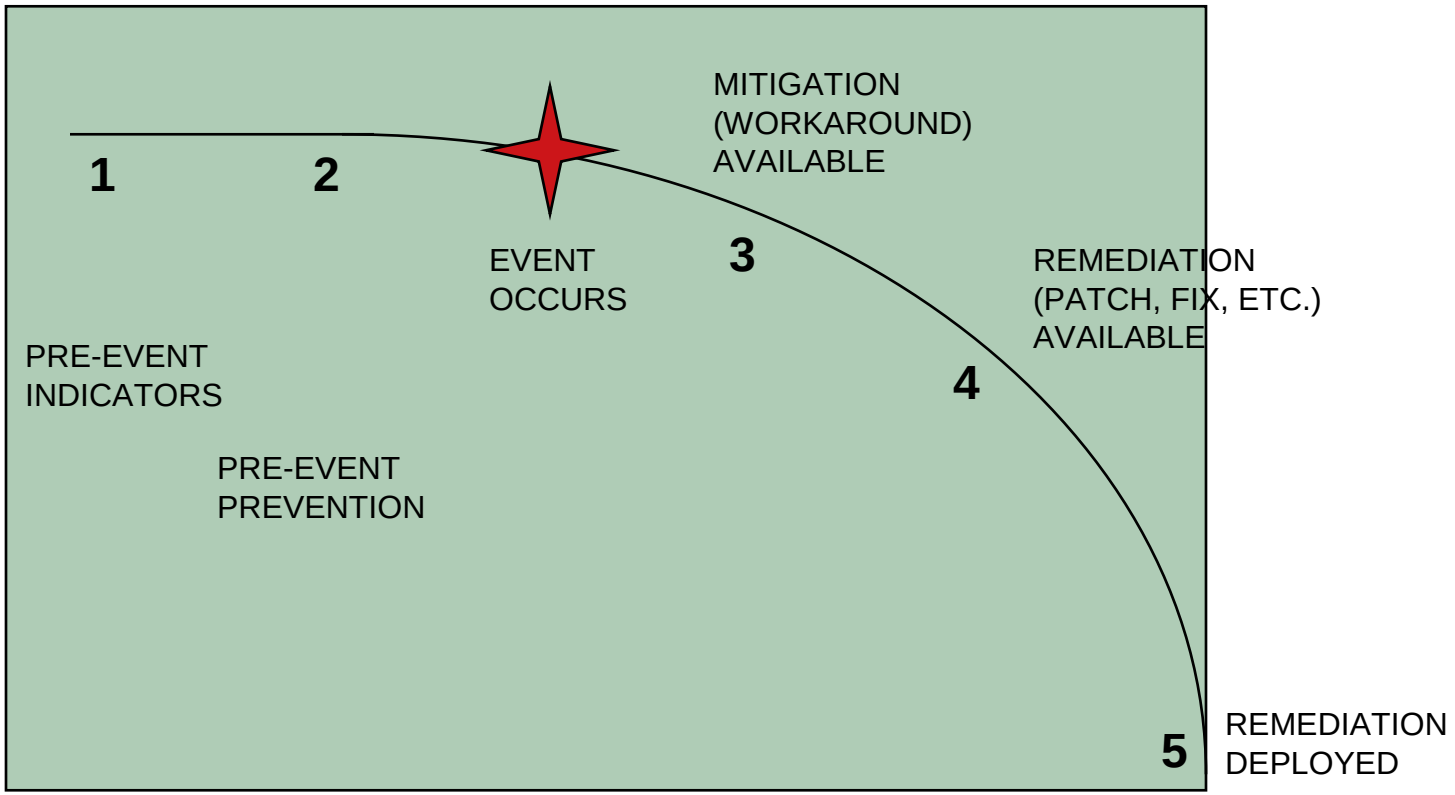
Phase-1: Awareness & Policy Automation

END-USER SECURITY AWARENESS CAN NO LONGER BE IGNORED IN THE ENTERPRISE

- **End-user awareness = end-user accountability**
- **Accountability = legal protection for the corporation**
- **The program must be automated, self-paced, supportive of policy, and regularly renewable**
- **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**

SECURITY OPERATIONS ROI

THE SECURITY ROI CURVE

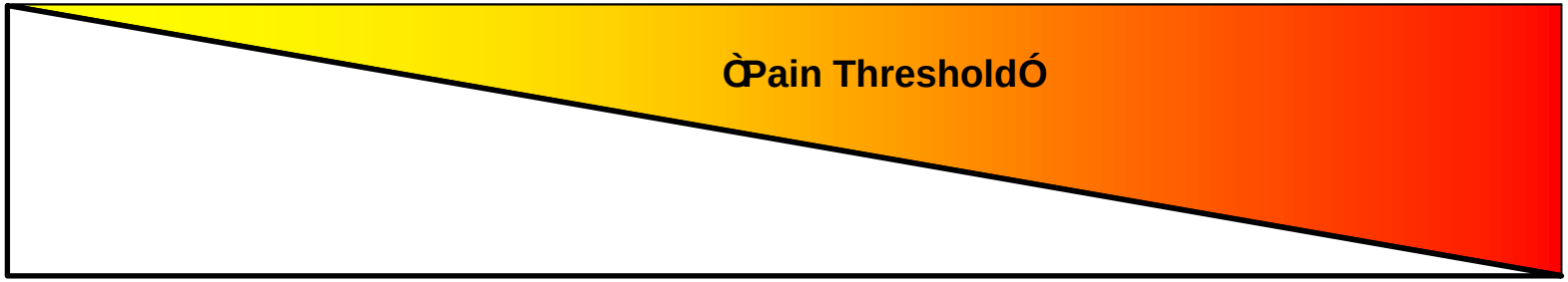


VALUE OF SECURITY, INTELLIGENCE, ETC. REDUCES SIGNIFICANTLY OVER THE TIMELINE OF AN EVENT

Event Impact Scale

Event Impact Scale

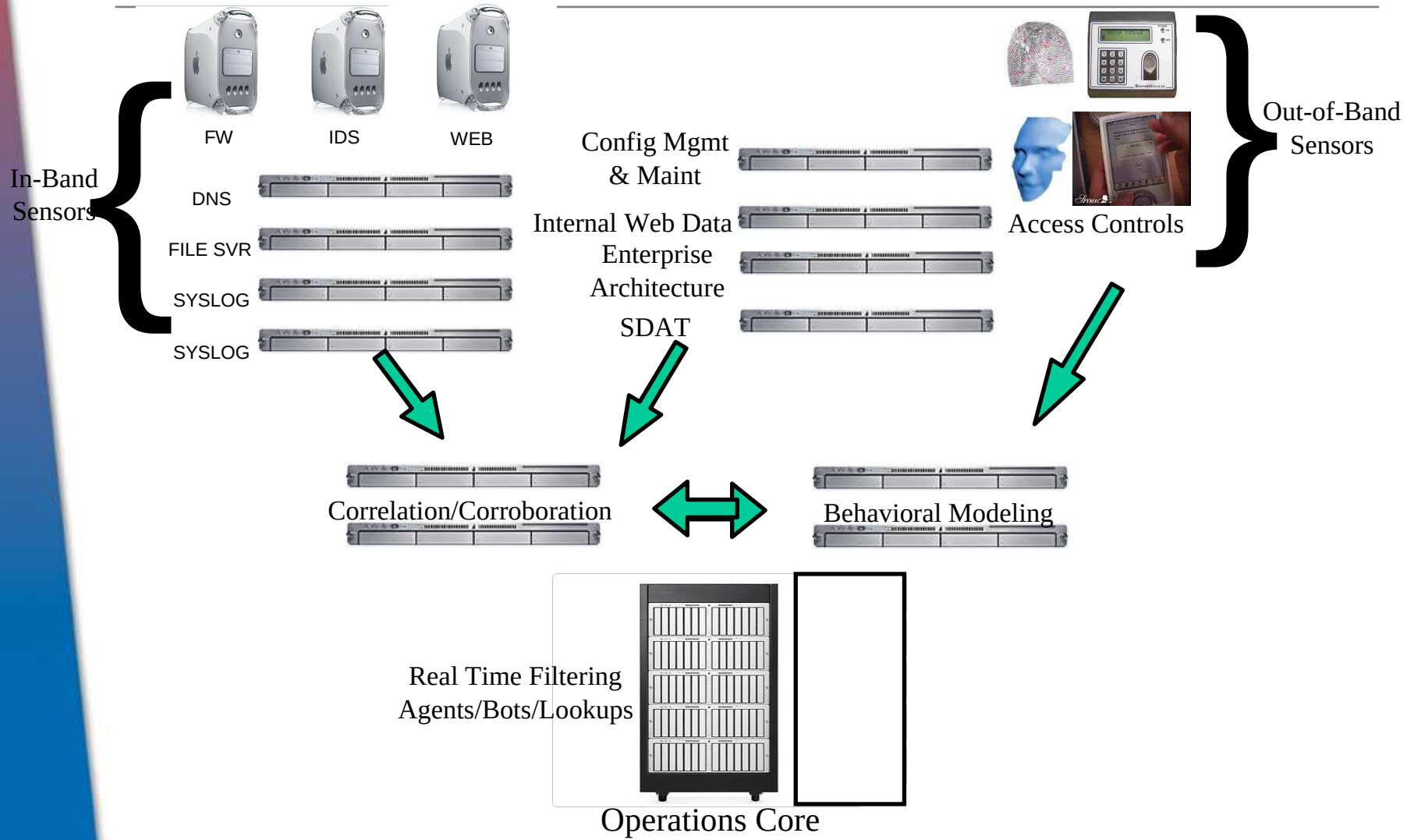
IRRELEVANT	KNOWN	UNKNOWN	KNOWN	UNKNOWN
	PREPARED FOR	PREPARED FOR	NOT PREPARED FOR	NOT PREPARED FOR



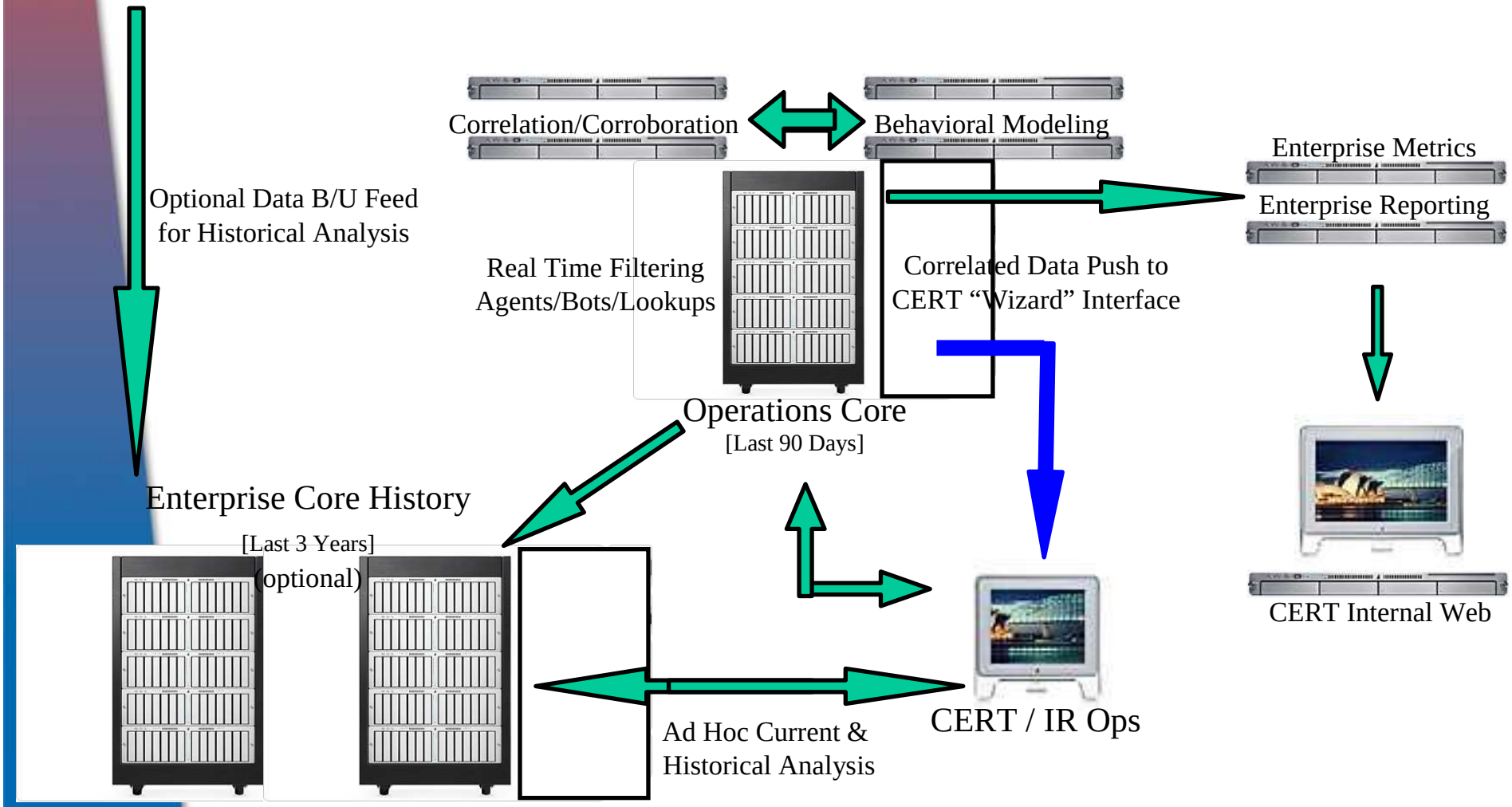
SAIC
An Employee-Owned Company

SO HOW DOES IT ALL WORK?

RANGER Security Operations



RANGER Security Operations



RANGER Pre-processing & Event Management

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

CERT Internal Web

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

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

Phase-3: A Wizard Event Manager Interface

- The WEM is A 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

- **RANGER 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**
  - **Automating those things that technology does well**
  - **Utilize human potential & expertise 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?

Presented

by

Robert J. Bagnall

Deputy Director of Managed Security Services

SAIC

robert.j.bagnall@saic.com

202-302-1900