Developing ITIL - Mature Security Incident Response With SIEM

A Plan for CSIRT Maturity Models via monitoring-driven Kanban

Part 2

alienvault
creators of ossim

CP Constantine – November 2011

Foreword

In the previous installation of this series, we took a short overview of the current status of Incident Response workflows and conjectured on possible models for maturity evolution of the Computer Security Incident Response service model.

This series of documents centers on the following assertions.

- The current status quo for effective Computer Security Incident Response is actually a very immature service model in comparison to other Service Domains within Information Technology in the Enterprise.
- Evolving IR into a more mature service model, will produce large quantities of valuable data for business intelligence and metrics.
- The information necessary to build this more mature model, does not actually create additional ongoing workload for Incident Response Teams, but actually acts as a force-multiplier to make existing work more effective and efficient.

Table of Contents

The Five States of Capability, Applied to Security Incident Response.

Picking up where we left of, let's take a look at currently-seen Incident Response workflows in comparison to the Capability Maturity Model Integration definitions. CMMI works well as a complementary model to ITIL, defining very similar measurements of Service Delivery ability. Moreover, it serves as an excellent illustrator of the broad space of opportunity to improve upon current best practices in Incident Response into new operational service models.

1 - Initial

“Processes Unpredictable, poorly controlled and Reactive”

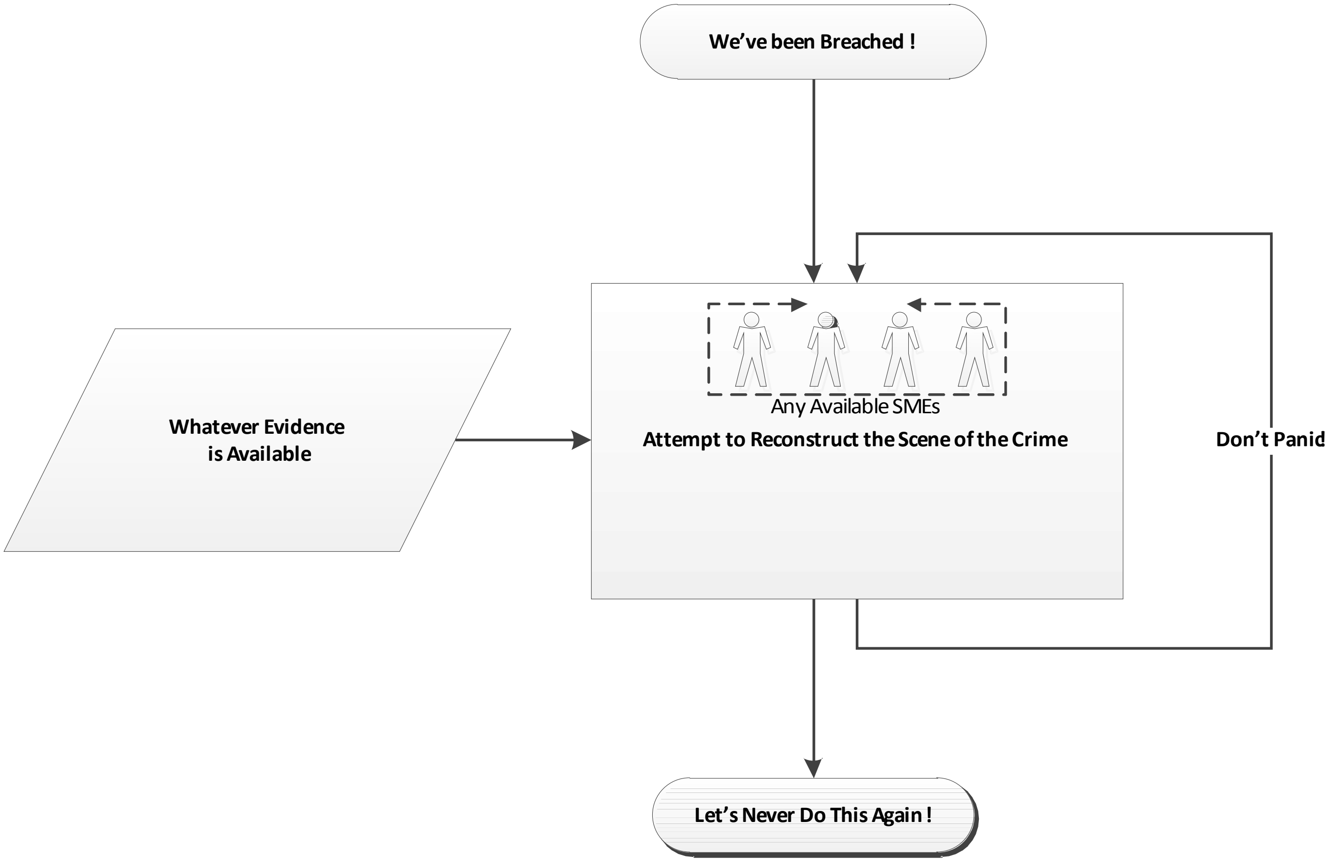
There are no dedicated Incident response personnel, detection of intrusion is left purely to the vigilance of individuals within the organization. If a breach is detected, panic mode is engaged and a temporary team is assembled from whatever expertise is available within the organization, or an outside agency is contracted. In the optimal outcome, this stage is never repeated and work commences immediately to more to stage 2.

- Incident Response as ad-hoc disaster recovery
- Point-in-time emergency teams formed from available SME's
- All process is created on the fly by the team. Workflow is according to personal judgment or emerging data.
- Usually no record of what work was done or its effectiveness, beyond the individual memory of the team.
- Metrics are impossible since nothing is repeatable.
- Intelligence data is neither produced nor actively consumed

Typical Configuration:

None: The emergency team must make use of whatever systems, logs and personal experience they have. Tracking is individualized with collaboration systems often limited to a file directory and a white board. Operational Procedure usually limited to 'Don't Panic!'

Flow Diagram



2 - Managed

“Processes Characterized for Projects, and is often reactive”

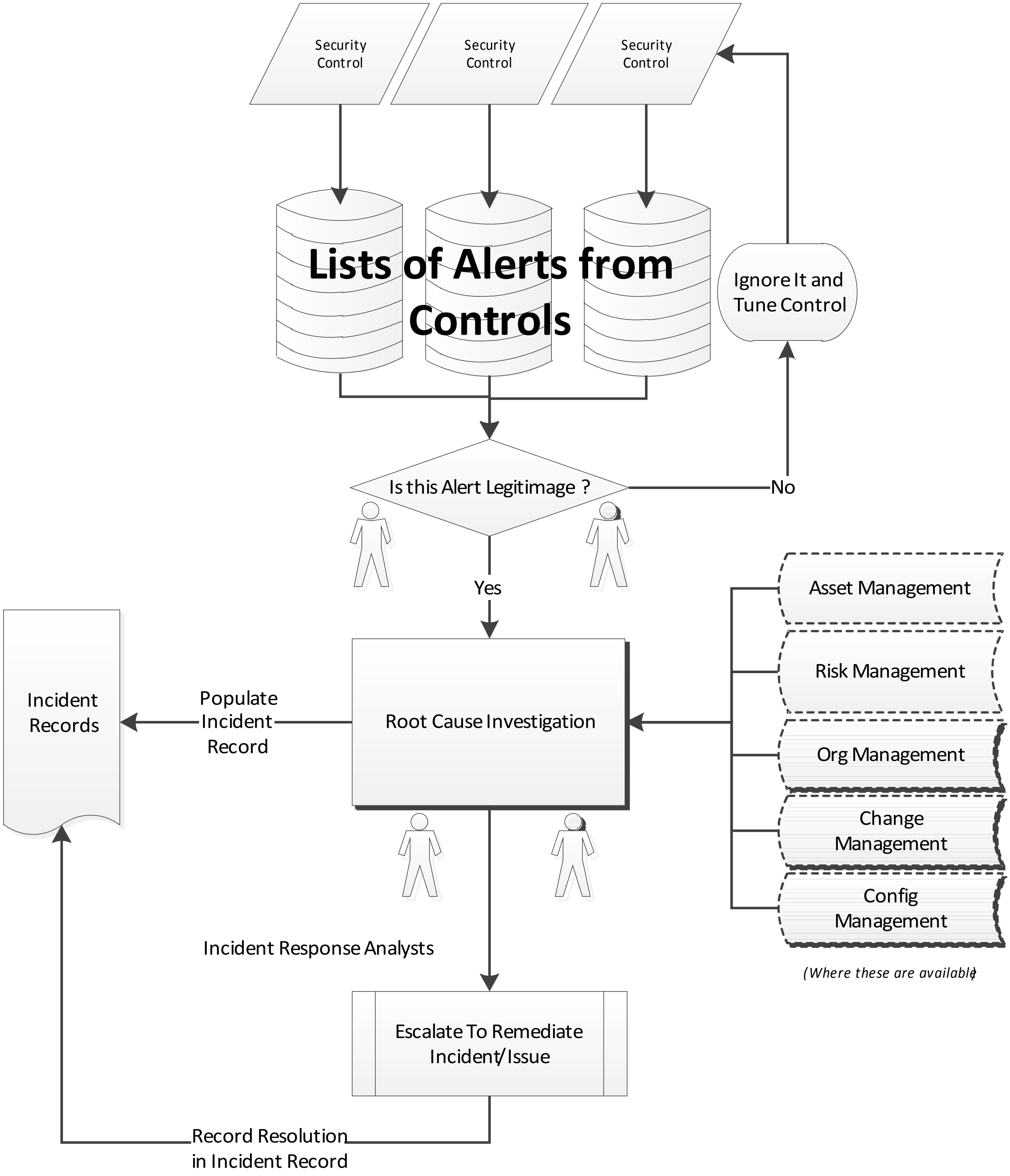
At this stage, roughly repeatable Incident Response procedures have been defined, and some semblance of ongoing process is in place. This can range from an agreed-upon amount of time exercised per week in reviewing logs, to a quantity of dedicated personnel responding to a linear queue of alerts from security controls, and incident reports from the enterprise. Alerts are based entirely from technical observations from Security Controls and are not tied to how the Enterprise does business; much time is spent tuning controls for false positives. Processes and procedures are driven entirely by technology, and little record correlation exists between investigative work and business processes. Prioritization of work queues are done by arbitrary measures of criticality that remain fixed. Metrics are often at the level of standalone numbers that lack the required compartmentalization to map them to overall business processes.

- Incident Response as intermittent quality testing or work ticketing -The 'Review during downtime” and “Linear Event Models”. Workflow often resembles a helpdesk style model.
- Initially dedicated hours and then dedicated staffing. Usually requires high-skill personnel able to follow loose processes and operate under their own specialized technical knowledge.
- Processes are loosely-defined, with no Key Performance Indicators. Procedure is often according to personal judgment with broadly-defined scopes of responsibility.
- Improvements are identified and measured by perception and consensus only
- Metrics rarely evolve beyond the level of raw numbers, and are not translatable to support the metrics of other business units.
- Intelligence data is consumed from external sources, but processed manually. Intelligence data is only produced as an incidental finding that lacks repeatability.

Typical Configuration:

Alerts generated and tracked directly in the security controls that generate them. Work tracking done in a re purposed trouble ticket system. Information gathering done manually from existing corporate asset management and organizational information systems. Extensive variety of support toolkits in place, often built by the individual. SIEM may be in place, but is likely to be an forensic control, not a direct driver of workflow via extensive correlation.

Flow Diagram


Security Control
Security Control
Security Control
Lists of Alerts from Controls
Ignore It and Tune Control
Is this Alert Legitimage ?
No
Yes
Asset Management
Risk Management
Org Management
Change Management
Config Management
(Where these are available)
Incident Records
Populate Incident Record
Root Cause Investigation
Incident Response Analysts
Escalate To Remediate Incident/Issue
Record Resolution in Incident Record

3 - Defined

“Processes Characterized for the Organization, and is Proactive”

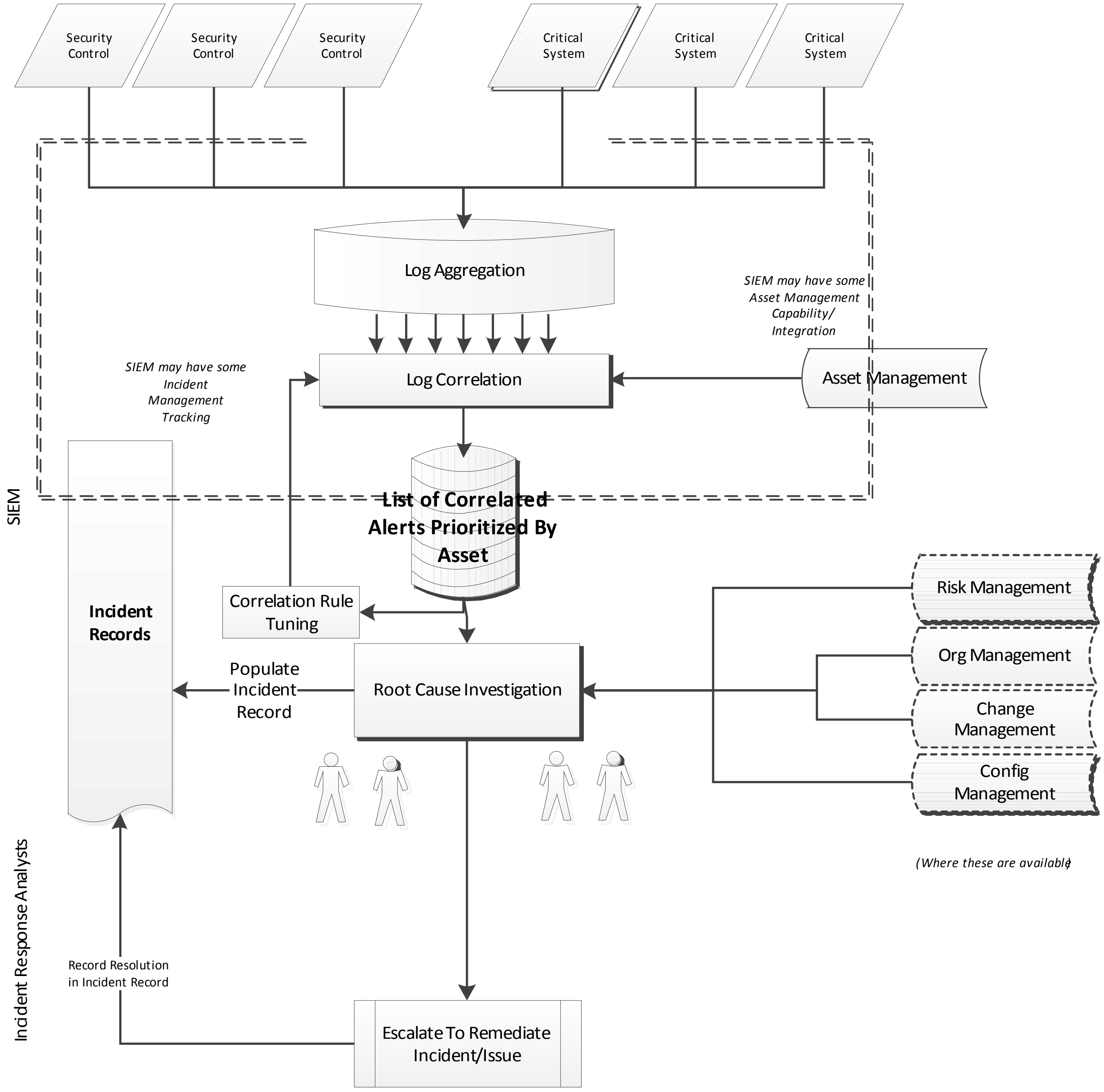
Security Monitoring is now aligned to the organization itself, alerts now trigger not only on publicly-available technically-driven detection methods, but on deviations from known business processes and policies. Incident Handling work is tracked in a system customized to track business-specific data alongside technical findings, integration with Asset Management and Change Management to pull in data directly relevant to an incident is in place. Information gathering procedures have become largely automated and workflow has evolved from a simple tracking systems towards a more pervasive Incident Management Platform. Metrics can be produced by tying activities to business components and gap-analysis resourcing begins to be possible.

- Incident Response as an ongoing Quality Assurance process for Information Security, Informed and integrated with Governance, Risk and Compliance processes.
- Dedicated staffing across several levels of experience and seniority; many repeatable managed processes in place to allow junior staffing for predictable, repeatable actions.
- Processes have a defined, multi-stage lifecycle with specific procedure requirements for transitioning between these stages. Monitoring is constructed to correlate to business risks and the majority of all alerts are predictably actionable.
- Workflow tracking is in place to identify resource costs within specific areas of the incident handling process (either within the Incident Response team, or in relation to particular business units), from actual data not perception.
- Metrics have become more normalized to the overall business, and can be consumed by other business units to support those metrics.
- Intelligence data is consumed from external sources, and programmatically mapped to workflow and alerting systems; broad scale definitions of Enterprise-specific threat trends are possible to construct.

Typical Configuration:

Alerts constructed based on business-specific knowledge, not generalized technical vectors. SIEM is the main driver of alerting and correlation rule output fuels an incident management workflow system that supports collaboration and lifecycle stages, with some document management and knowledge bases, tied into asset and project management (very likely a re-tooled Change Management system). Not uncommon to find large amounts of automation scripting tying together functions missing from COTS solutions.

Flow Diagram



4 - Quantitatively Managed

“Processes Measured and Controlled”

The Incident Management platform becomes the switchboard for all security data. Alerting is designed around identifying threats to specific business processes, not assets. All alerting is done through extensive correlation and all repeatable information-gathering tasks become automated, the Incident Management Platform becomes the primary portal to almost all information required to pursue investigation and the need to cross-train analysts on individual vendor's security products is done away with. Workflow and alerts are aggregated and cross-referenced to business processes, with prioritization dynamically adjusted as events occur. Root causes of all investigative work is directly discernible by mapping to risk decisions and exceptions, incident response becomes a direct source of data to measure the security impact of individual business units and operations.

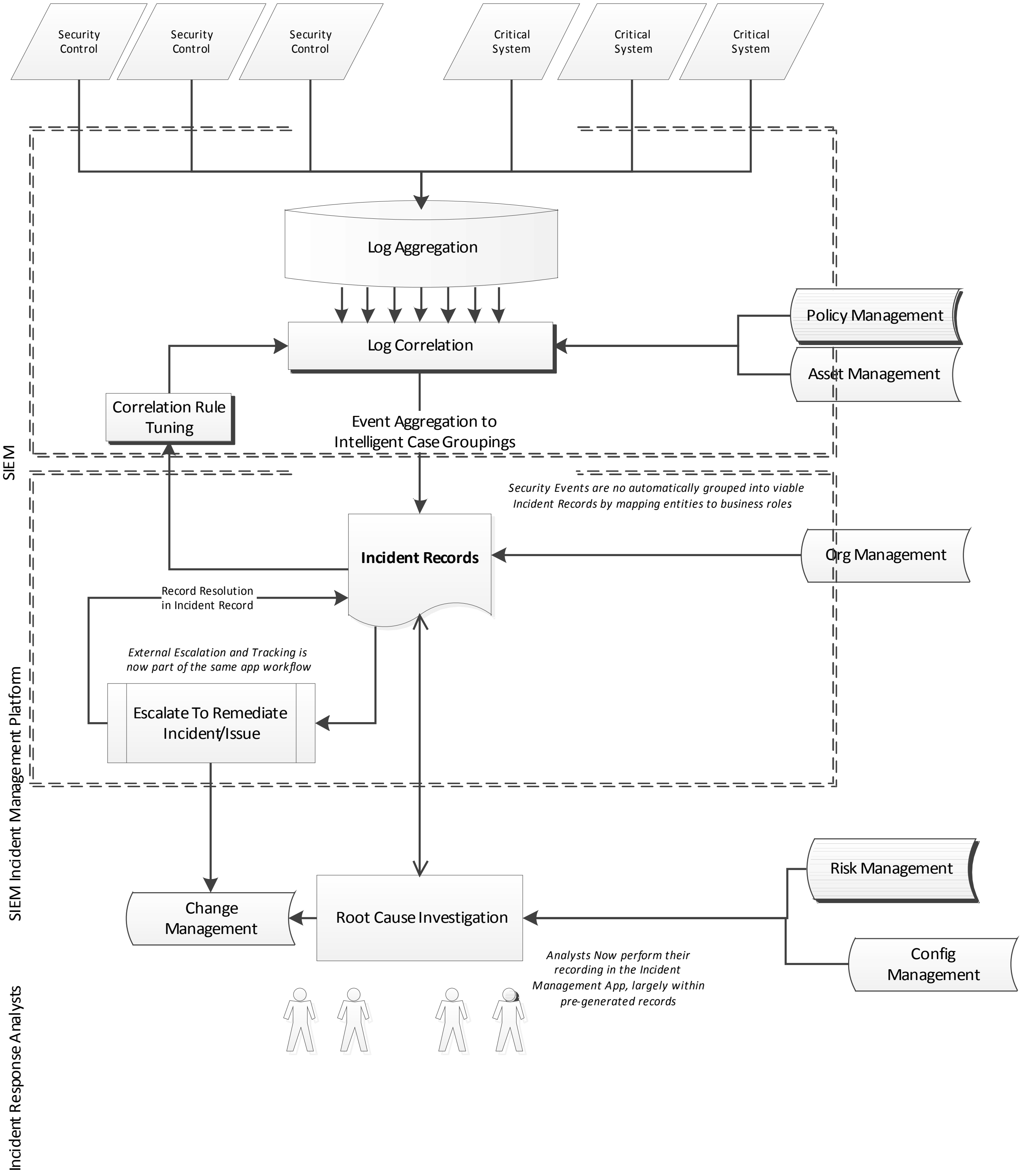
- Incident Response as as a source of Business Intelligence data, maximizing the low-level infrastructure visibility that Information Security wields, to provide an extensive service catalog.
- Teams can include a good percentage of more junior members, as the great majority of directly actionable work is tightly defined and repeatable, in a workflow system that provides the majority of contextually-relevant information within the same system.
- Processes and procedures have been adapted to conform to specific target business units and are tracked directly against workflow carried out from those directives.
- Workflow is tied to Risk Management in a closed feedback loop of continual risk outcome measurement and root cause analysis sourcing.
- Metrics are comprehensive, effective, and a significant portion of the departments Service Catalog.
- Intelligence data becomes a primary output of the Incident Response team, and the Security Impact of Business Operations and activities is an ongoing feed to Business Intelligence. Incident Response shifts towards a focus on generating advanced intelligence patterns to maximize early detection of efforts to breach.

Typical Configuration:

Incident Management and Risk Management become symbiotic, very likely working within the same software platform. System integration and automation is maximized to pre-fetch all repeatably available information required for the incident handler to make an information judgment; manual information gathering is limited to point-in-time, advanced tasks. At time of writing, no single product or vendor achieves the entire feature list required for this maturity level.

Alerting, Correlation Rules, and all activity drivers are constructed from the standpoint of the Business outward, not the attacker inward: Nearly all alerts generated are directly actionable in some way. SIEM drives pre-processing and correlation of all controls and logs, integrates with GRC systems, and automatically feeds a workflow system (likely custom built) that tracks incident patterns and relations over time, continually aggregating data together at meta levels.

Flow Diagram



Security Events are no automatically grouped into viable Incident Records by mapping entities to business roles

External Escalation and Tracking is now part of the same app workflow

Analysts Now perform their recording in the Incident Management App, largely within pre-generated records

5 - Optimizing

“Focus on Process Improvement”

Incident Response begins the transition towards Exposure Response, as Exposures and Risks are mapped together from decision making workflows and Configuration Management Systems Underlying technologies in Incident Management become effectively transparent to analysts for all predictable tasks. Threat, Risk and Configuration data is processed into a just-in-time workflow of expedient discovery and remediation of security posture weaknesses.

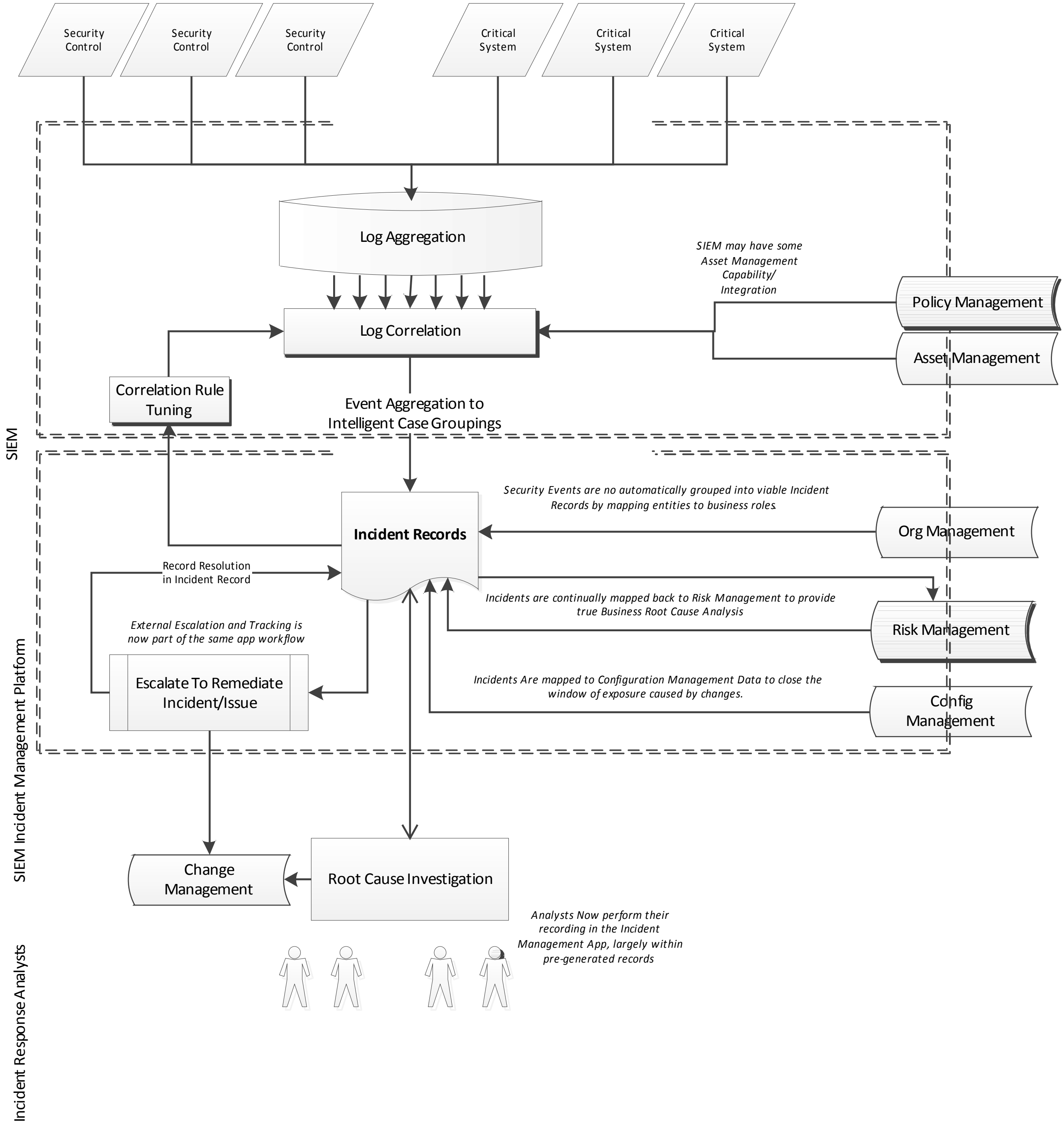
Incident Response evolves from a firefighting and garbage collection department struggling to avert disaster, into a real-time process and risk monitoring unit enabling process steering and continuous improvement.

- Incident Response as business enabler and continuous corrective control, consuming vast amount of operational data from the enterprise, correlating it all into a continuous stream of remediation and advisory output to all business units, the IT Early Warning Network.
- Teams now contain a wide range of skills and skill levels; more senior staff is less concerned with direct investigation than programmatically embedding their knowledge into the Incident Management Platform and addressing high-level patterns and recommendations.
- All Process and Procedure is embedded into and directly enabled by the SIEM and Workflow platform.
- Workflows contain almost all possibly relevant information presented inline, and handoff interfaces to any external workflow systems necessary. The single-portal model. Technical Data,Risk and Business Operations information, External Intelligence, unified into a single interface.
- Metrics now directly supporting Enterprise Risk Management via large quantities of historical correlative and causal measurements of previous results.
- Incident Response finally becomes Active Security Intelligence, directly guiding the Enterprise away from Incidents via adaptive intel generation.

Typical Configuration:

A typical configuration likely does not exist at the time of writing: this stage of maturity describes a level of integration and capability of software platforms and data processing that has not yet reached commercial availability.

Flow Diagram


Security Control
Security Control
Security Control
Critical System
Critical System
Critical System
Log Aggregation
Log Correlation
SIEM may have some Asset Management Capability/ Integration
Policy Management
Asset Management
Correlation Rule Tuning
Event Aggregation to Intelligent Case Groupings
SIEM
Security Events are no automatically grouped into viable Incident Records by mapping entities to business roles.
Incident Records
Org Management
Record Resolution in Incident Record
Incidents are continually mapped back to Risk Management to provide true Business Root Cause Analysis
Risk Management
External Escalation and Tracking is now part of the same app workflow
Escalate To Remediate Incident/Issue
Incidents Are mapped to Configuration Management Data to close the window of exposure caused by changes.
Config Management
SIEM Incident Management Platform
Change Management
Root Cause Investigation
Analysts Now perform their recording in the Incident Management App, largely within pre-generated records
Incident Response Analysts

A Service Catalog Selection for Incident Response Maturity

The first step toward building an ITIL-Mature Incident Response program is to explicitly define a service catalog from which to build metrics and SLA's around.

ITIL v3 in particular, now stressed the importance of the Service Catalog as the centerpoint for developing process maturity around. The present state of information Security makes it a difficult stand to take in focusing on the desired outcome instead of the problems, since the problems seem so insurmountable. Inevitably, for any organization born from emergency and firefighting duties, the desire to succumb to explaining away the workload as "too complicated, too unpredictable" to be derived down into discrete service operations. As with all tasks of this sort though, starting with broad strokes, and then subdividing down proves effective.

In the following sections, we present a selection of possible Service Catalog offerings to develop. As with many aspects of CMMI, not all of these are mandatory for each stage of maturity, and should be adapted to the requirements of the business they serve.

Detection

The core of Incident Response, and the portion most applicable to automation and continuous improvement. The scope of this function presents many opportunities for additional value to deliver to the business however, and need not be constrained only to malicious interference.

Remediation

Although this function has much overlap with Security Operations and Risk Management, Incident Response has a key place in coordinating effective remediation of discovered problems, advising on effective remediation procedures, validating that changes rectify the initial issue and being a point of coordination and exchange between business units tasked in remediation work.

Metrics Support

A key point of difficulty in Information Security today; providing actionable, illustrative metrics from Security Operations that can context value received in the scope of the global Theater. Security Monitoring has a unique visibility to Enterprise infrastructure that presents great potential for adding value to the Enterprise by providing metrics data to other business units they would otherwise lack visibility to. All metrics here are externally-facing metrics to support other units within the information security organization or beyond.

Intelligence

Finally, the combination of the three preceding service areas: Intelligence build from observable results of current and prior actions and events to advise and guide future tasks

1 – INITIAL

By definition, there can really be no service catalog at this stage of maturity, however we can at least list what the inferred services are, from which to use as a base to build out an evolving catalog from:

Detection

- **Intrusion Detection**
    1. Discovery of Scope of Intrusion
    2. Discovery of Vector of Intrusion

Remediation

- **Disaster Recovery**
    1. Restoration of Compromised Systems.
- **Business Continuity**
    1. Remediation of Vector of Intrusion

Metrics Support

- None

Intelligence

- None

2 – MANAGED

Here we define the core, ongoing functionality of an Incident Response team. Many of these services will be carried out 'silently' within the organization, being communicated only vertically within the organization

Detection

- **Intrusion Detection**
    1. *All services from stage 1*
    2. Discovery of Intrusion
- **Compliance Management**
    1. Discovery of Non-compliant Systems
    2. Identification of Policy Violators

Remediation

- **Disaster Recovery**
    1) *All services from stage 1*
    2) Identification of compromised intellectual property.
- **Business Continuity**
    1) Validation of Remediation for Vector of Intrusion
    2) Emerging threats modifications to security controls

Metrics Support

- **Security Posture**
    1) Trends in root causes (vulnerabilities, exposures, and departmental security postures)
    1) Trends in policy and compliance violation by department.
    1) Cost of security response per business unit.

Intelligence

1) Discovered Threat Source and Vector trends
2) Policy items that present conflict with business operations.

3 – DEFINED

At this stage, Incident Response has begun to be fundamentally aligned to business processes, evolving away from a functional fixation on security vulnerabilities and attacks towards a larger view of operational fulfillment of the enterprise, and services offerings begin to reflect this.

Detection

- **Intrusion Detection**
    1) *All services from stage 1+2*
- **Compliance Management**
    1) *All services from stage 1+2*

Remediation

- **Disaster Recovery**
    1) Validation of Restoration for Compromised Systems.
    2) Identification of compromised intellectual property.
- **Business Continuity**
    1) *All services from stage 1+2*
    2) Continuous Improvement of Security Controls Configuration
    3) Directed remediation of exposures created by business operations

Metrics

- **Security Posture**
    1) *All services from stage 1+2*
- **Resourcing**
    1) Gap Analysis of Security Controls Effectiveness.

Intelligence

1) *All services from stage 1+2*
2) Trends in Targeting of specific business units.

3) Correlations between Major Business Activities and Security Trends

4 – QUANTITIVELY MANAGED

Incident Responses reaches its potential as gap coverage/analysis for the rest of the Security Program here. Response work becomes vital not just for the defense of integrity of business operations, but the measurement of the true cost of those operations and the effectiveness of resources deployed to protect them.

Detection

- **Intrusion Detection**
  1) *All services from stage 1+2+3*
- **Compliance Management**
  1) *All services from stage 1+2+3*
- **Exposure Detection**
  1) Discovery of Threat Exposure by Configuration Change.

Remediation

- **Disaster Recovery**
  1) *All services from stage 3*
- **Business Continuity**
  1) *All services from stage 1+2+3*

Metrics

- **Security Posture**
  1) *All services from stage 1+2+3*
  2) Type Trending of configuration changes that result in exposures leading to security incidents.
- **Resourcing**
  1) *All services from stage 1+2+3*

Intelligence

1) *All services from stage 1+2+3*
2) High-Risk IT deployments and operations that require additional security oversight.

5 – OPTIMIZING

Finally we arrive at the point where Incident response becomes Exposure Response, locking in a feedback loop of continuous improvement with the rest of the Security Program.

For the sake of brevity, the prior sets do not require repeating. At this stage we come to the culmination of Incident Response:

> *The continual measurement of the outcome of risk decisions taken, resources applied, and the movements of the global theater of risk.*

Particularly though, at this level of evolution, the service catalog should be so tailored to the enterprise it serves, that providing a list of suggestions would defeat the purpose of doing so.

Summary – Part 2

Security Incident Response is not so alien as to be incompatible with CMMI and ITIL-ITSM. By focusing on value-added back to the enterprise and treating the information we collect during defensive actions as a commodity of value to the rest of the organization, it becomes possible to direct workflow in the direct of the desired level of integration and accessibility to knowledge necessary to perform more directly effective incident response. Without knowing the function of what you are defending, defense is nearly an untenable position when approached from a purely technical standpoint – detailed information of the relevance of systems and business functions should be the core advantage of any Security Program, yet all too often, our attackers know more about our networks than we do.

In truth, they only need to know *enough*, and can expend the time to learn the specific pieces of information they require. On the defensive side however, we can never know everything about the organizations we protect: we need workflow systems that can present all the contextually-relevant information on the systems we are investigating at the time of investigation.

Making all necessary information to make an informed judgment in the investigation of an incident is a problem that is not unique to Information Security Incident Response, the Intelligence field has been solving these issues for many years, and private sector Information Security Incident Response will be retracing the same steps for many years to come.

Building these first integrations to initially make information available to a Response Team and then evolve to where the information is programmatically correlated into workflow is the only effective way to address an ever-growing threat landscape with realistic resources.

Even that approach however, can only go so far: to receive the most effective return on resource investment: security practices must be tailored for the details of the enterprise, and intertwined with them. Information Security as a field protests loudly that we are not provided with the required business knowledge to formulate these models, yet we possess unique visibility to the enterprise that should allow us to construct our own from whole cloth.

For you cannot defend, that which you don't know exists.