

# Evaluating And Choosing Insider Threat and Extrusion Detection / Prevention Controls: An Executive Summary

Craig Chamberlain  
[summary@craigchamberlain.com](mailto:summary@craigchamberlain.com)

## Summary

Insider threat is one of the more complex problems in information security and requires a sophisticated response to detect the subtle variations in access patterns that separate intentional misuse from authorized use. Figure 1 below depicts a typical decision process in considering technical controls. This document describes strategy and tactics for detection of insider misuse of computer-based information assets.

## New terms

A term you may be seeing for the first time is *event correlation*. Event correlation is the process of monitoring networks and other systems in order to identify patterns of events that might signify attacks, intrusions, misuse or failure.

*Extrusion* and *exfiltration* are the converse of intrusion and infiltration; they describe the process of removing something of value, which is the end goal of any professional intruder. This is where the focus of the investigator often arrives after following a convoluted trail of alerts and logs.

Another is *anomaly detection*, which is, simply put, monitoring and flagging strange system behavior. Anomaly detection has been the central aspect of many auditing practices for a very long time. It is the basis for much of the fraud and misuse detection systems used in financial and transaction processing organizations. In the computer world,

the concept stems from a paper fundamental to the field of security - [An Intrusion Detection Model](#), by Dorothy Denning. In it, she describes building an "activity profile" of normal usage over an interval of time. Once in place, the profile is compared against real time events. Anything that deviates from the baseline, or the norm, is logged as anomalous. Anomaly event reports can be generated according to statistical models, specifications, or both.

## Tenets

In general, I found most of these to be valid most of the time. Trying to break them is somewhat like trying to break or approach the speed of light; as you get closer, the costs increase exponentially until finally there is not enough energy (or money) in the known universe to keep going.

- Some users are "expert users" of their applications and are sophisticated enough to devise clever ways to bypass simple security controls in order to make their job easier, no matter how much effort has gone into obfuscating security flaws.
- Some of these users will use this knowledge to bypass simple security controls and misuse and / or exfiltrate data.
- No matter how good your controls are, there is often a hole you didn't know was there that can be used to exfiltrate data. In addition to misuse detection at the applications server or database layer, prevention of misuse generally requires having client side controls.
- Some or all users will have administrative user accounts or privileges on their desktops.
- Some or all users have Internet access or know how to obtain it.
- Disabling Internet access for a user population is often hard or impractical.
- Once data has left an organization's control, the only effective protection is encryption.

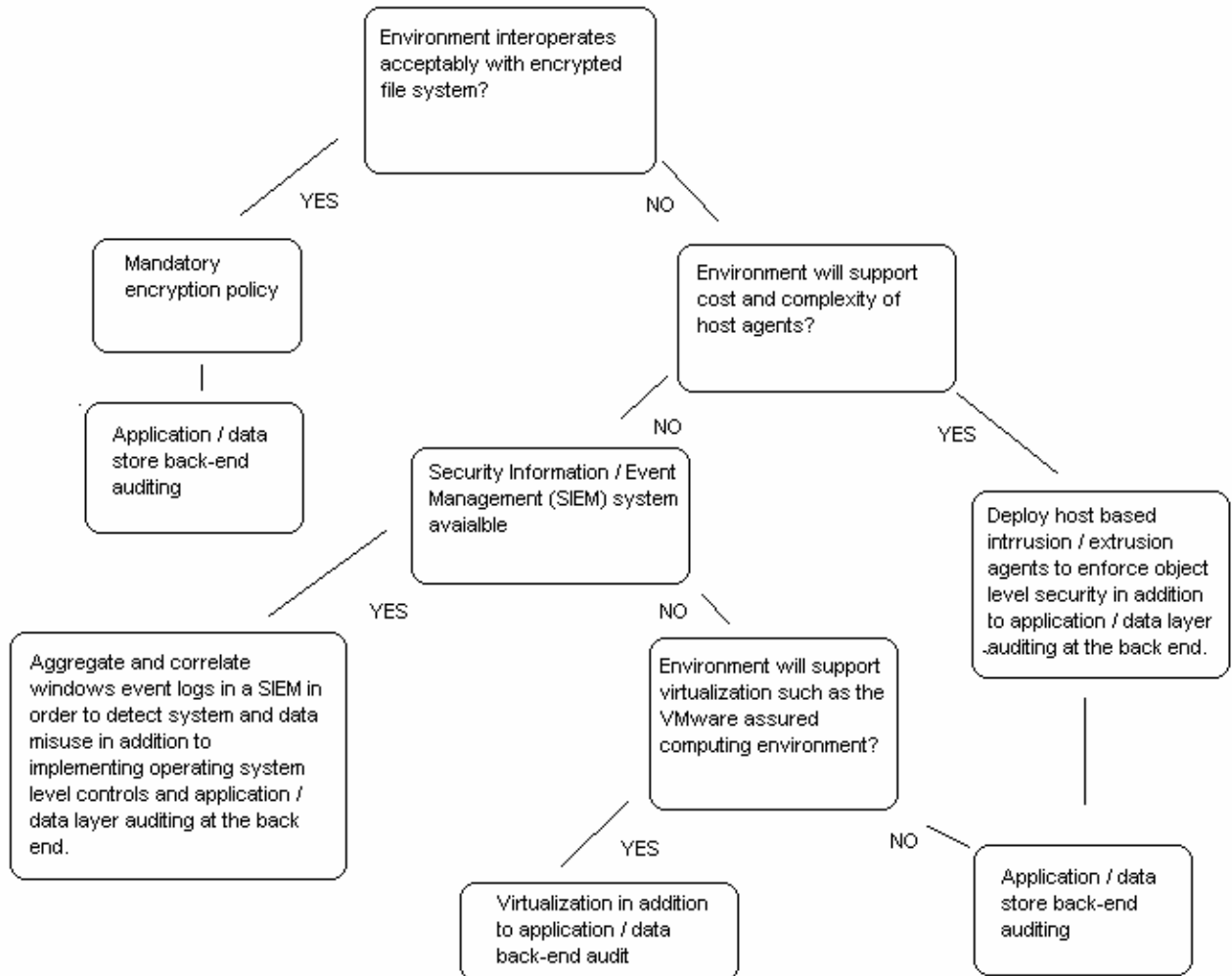
- Security is a process, not a product.

## Methodology

The following general methodology works well in selecting and implementing insider misuse controls:

1. Construct a threat model of the data at risk and the threats it faces.
2. Conduct an insider threat assessment. This can be done by having members of the security organization assess and learn the user environment and applications or by identifying an expert user to use as a resource.
3. Design technical controls to mitigate the threat and test them in a pilot or proof-of-concept deployment.
4. Assess the effectiveness of the controls, apply lessons learned and make improvements or refinements.
5. Deploy controls and monitor for effectiveness and interoperability with business process. Re-assess and refine threat model(s) and risk mitigation controls as necessary.

Figure 1. A typical technical control selection decision tree.



## Phase One: Threat Modeling

*Threat modeling* is a method of assessing and documenting security risks associated with an asset. Constructing a threat model requires understanding the goals of the perpetrator or *threat source* in assailing a system and its assets of value. The model considers the attack paths and attack surface of a system from the perspective of a threat source in order to identify assets at

risk. This allows development teams to enumerate attack goals, or *threats*. Vulnerabilities are discovered when a threat exists for which insufficient safeguards or controls are in place.

Threat modeling is *not* the process of evaluating available technical controls or products, nor should it be focused around products.

In order to construct an insider threat model to digital information assets many details need to be fleshed out:

- Which applications and systems house customer data?
- Where and how is this data stored or cached?
- What are the interfaces between the applications and the data?
- Who are the application users and what are the sizes and locations their populations?
- How sophisticated are they? What is their combined experiential and intelligence pool?
- What is the expected and observed business process for the application and the application user population?
- What is the expected and observed workflow of the application user population?
- What, if any, history of misuse exists in the population?
- Which, if any, populations are at risk of misuse?
- What behavioral patterns and thresholds exist for application and data use?
- What is the required vs. actual privilege level of the user population?
- What data exfiltration vectors exist?
- Which exfiltration vectors can be closed with existing controls and which cannot?

Phase Two: Categorization, Prioritization and Proof-of-Concept (POC) Implementation

In Phase Two, the population of at-risk employees is divided into groups with approximately equal risk levels. These divisions will be based on several factors including past history, data classification and the availability of exfiltration paths. Groups can be formed of similar user sub-populations, business lines, application or data access boundaries depending on how risk factors map to the internal characteristics of the organization.

At the completion of phase two a user sub-population will be selected which presents the most immediate or significant risk of information asset misuse. This sub-population and their information systems will be the starting point where technical controls are developed, deployed and fine-tuned to accomplish risk mitigation without disrupting business continuity. Once developed and sufficiently refined, these controls can be adapted and deployed to additional at-risk populations throughout the organization.

Phase Three: Solution Architecture and Deployment; a process we are all familiar with.

Table 1. Insider Threat Technical Controls

	COST	EFFORT	ASSURANCE	ADVANTAGES	DISADVANTAGES	COMMENTS
Mandatory encryption policy	High	Medium	High	High assurance, preventive, no IPS rule development cycle, effective when operating system is offline;	Some users may disable; may require business process or workflow re-engineering; may interfere with legitimate workflow	
Agent based intrusion / extrusion prevention	High	Very high	Medium	Careful rule development and deployment can minimize impact on business process and workflow; can be preventive; can be	Rule development cycles can be prolonged, difficult and expensive; agent deployment and maintenance can be expensive; some users may learn to disable	

				adapted to address new threats		
Agent-less intrusion / extrusion detection (e.g. nessus policy compliance audits, event log correlation)	Low	Medium	Medium	No agent deployment and maintenance, minimal changes to desktop configuration	Detection only, no prevention; limited visibility, users may learn to disable or evade detection	
Virtualization (e.g. Citrix, VMware assured computing environment)	Medium	Medium	Medium	Provides control over user environment resulting in lower administration and remediation costs	Large startup effort, highly network dependent	
Operating system	Low	Medium	Low	No licensing costs, no new	Difficult to guarantee and	

controls (desktop lockdown through group policy, etc.)				products to learn or maintain	monitor compliance; difficulty in removing existing privileges (e.g. Internet access) subject to human error; users may learn to disable or circumvent;	
---	--	--	--	-------------------------------------	---	--