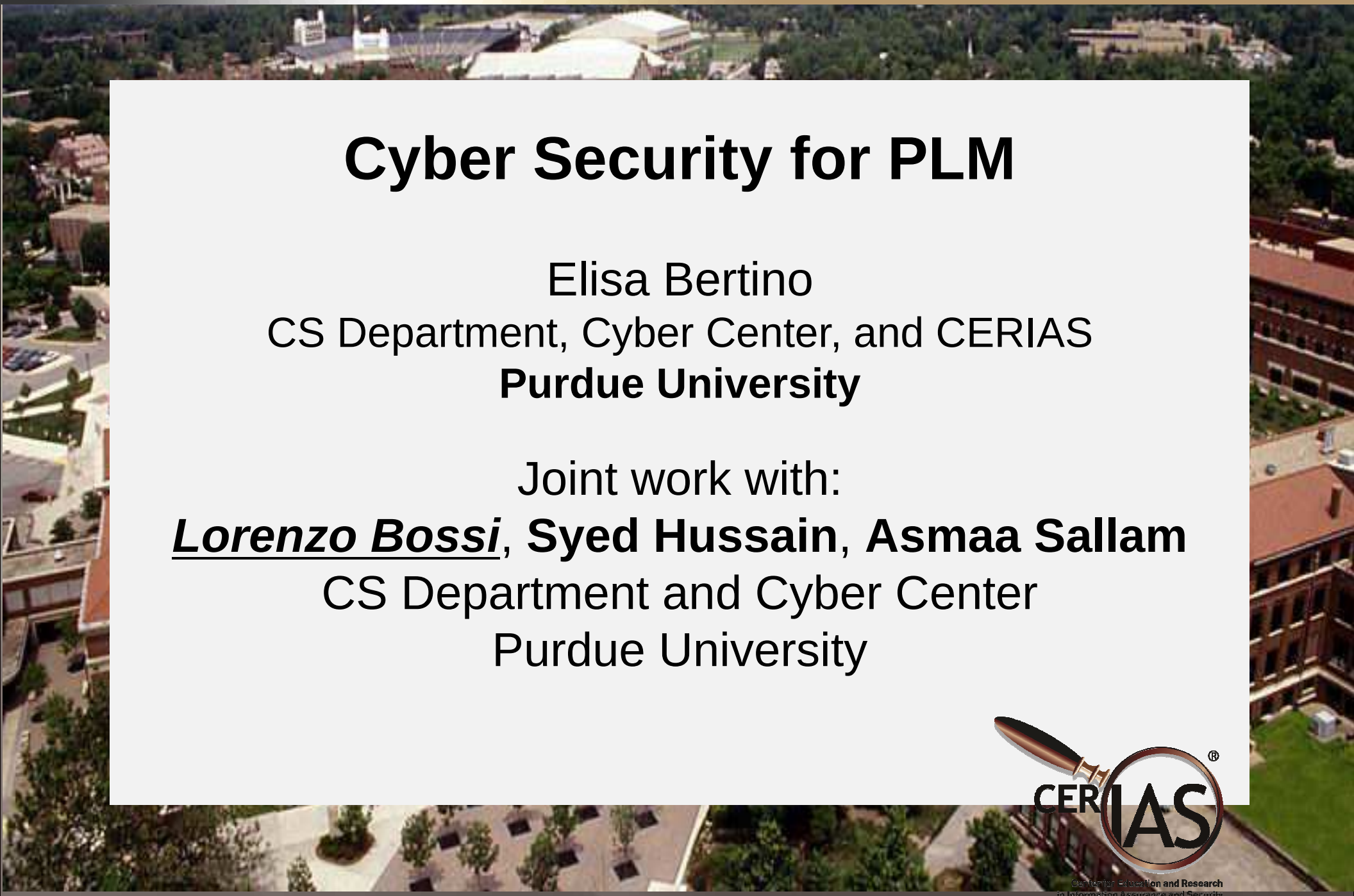
Cyber Security for PLM

Elisa Bertino
CS Department, Cyber Center, and CERIAS
Purdue University

Joint work with:
Lorenzo Bossi, **Syed Hussain**, **Asmaa Sallam**
CS Department and Cyber Center
Purdue University



PLM Cybersecurity – Research Roadmap

PURDUE UNIVERSITY Discovery Park

- Protection from insider threat
- Access control systems
- Compliance techniques
- Secure supply chain and secure remote 3D printing
- Security usability
- Security management and security cost
- Secure collaboration techniques
- Cloud security and cloud for security

Protection from Insider Threat

PURDUE UNIVERSITY Discovery Park

Some Data

2010 CyberSecurity Watch Survey (*)
(CSO Magazine in cooperation with US Secret Service, CMU CERT and Deloitte)

- 26% of attacks on survey respondents' organizations were from insiders
  (as comparison: 50% from outsiders, 24%unknown)

- Of these attacks, the most frequent types are:
  - Unauthorized access to/ use of information, systems or networks 23%
  - Theft of other (proprietary) info including customer records, financial records, etc. 15%
  - Theft of Intellectual Property 16%
  - Unintentional exposure of private or sensitive information 29%

(*)http://www.sei.cmu.edu/newsitems/cyber_sec_watch_2010_release.cfm

Protection from Insider Threat

IP Theft

https://www.cert.org/blogs/insider_threat/2013/12/theft_of_ip_by_insiders.html

Based on 103 IP theft cases recorded in the MERIT Database (since 2001)

- Industry sector in which IP theft occurred more frequently
  - Information Technology 35%
  - Banking and Finance 13%
  - Chemical 12%
  - Critical Manufacturing 10%

-Majority of insider IP theft cases occurred onsite (70% onsite as opposed 18% remotely)

- Financial impact (known only for 35 of the 103 cases)

  Over 1M USD in 48% of cases and over 1K in 71%

Protection from Insider Threat

IP Theft – Mitigation and Detection

From "*Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations*", CMU/SEI, May 2013

- Recommdendation3:

Monitor Intellectual Property Leaving the Network

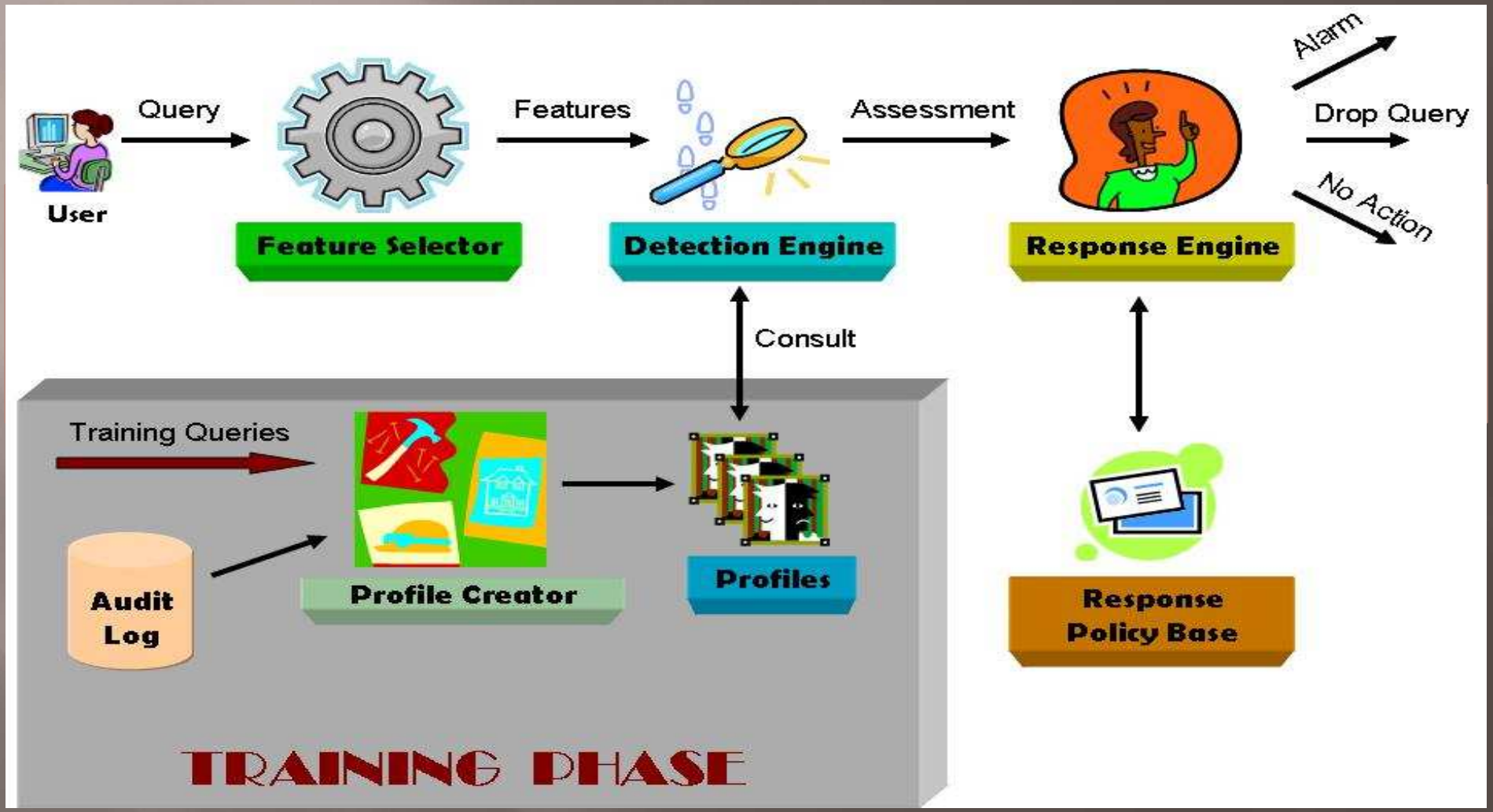
  - Identify critical information and track its location, access, modification, and transfers
  - Implement technical controls that log the access and movement of critical information that employees
    - Download from company servers
    - Email from the organization's network to personal accounts
    - Download to removable media
  - Many cases involved downloading source code, executables, or excessive amount of data before leaving the organization

- Recommendation 4:

Consider Enforcing Least-Privilege

Anomaly Detection and Response System for Databases

System Architecture



Anomalous Access Pattern
Example

PURDUE UNIVERSITY Discovery Park

Normal Access Pattern

SQL Commands

T_1

T_2

T_3

USER TABLES

Anomalous Access Pattern

SQL Commands

syscolumns

sysobjects

SYSTEM TABLES

SQL Query Representation

Key idea

PURDUE UNIVERSITY Discovery Park

- Extract access pattern from query syntax
- Build profiles at different granularity levels
  - Coarse
  - Medium
  - Fine

Coarse Quiplet: *example*

PURDUE UNIVERSITY Discovery Park

Schema T1 : {a1,b1,c1} T2 : {a2,b2,c2} T3 : {a3,b3,c3}

Query

```
SELECT T1.a1, T1.c1, T2.c2 FROM T1, T2,T3
WHERE T1.a1 = T2.a2 AND T1.a1 =T3.a3
```

Field	Value
Command	SELECT
Num Projection Tables	2
Num Projection Columns	3
Num Selection Tables	3
Num Selection Columns	3

Medium Quiplet: *example*

PURDUE UNIVERSITY Discovery Park

Schema T1 : {a1,b1,c1} T2 : {a2,b2,c2} T3 : {a3,b3,c3}

Query

```
SELECT T1.a1, T1.c1, T2.c2 FROM T1, T2,T3
WHERE T1.a1 = T2.a2 AND T1.a1 =T3.a3
```

Field	Value
Command	SELECT
Projection Tables	[1 1 0]
Projection Columns	[2 1 0]
Selection Tables	[1 1 1]
Selection Columns	[1 1 1]

Fine Quiplet: *example*

PURDUE UNIVERSITY Discovery Park

Schema T1 : {a1,b1,c1} T2 : {a2,b2,c2} T3 : {a3,b3,c3}

Query

```
SELECT  T1.a1, T1.c1, T2.c2 FROM T1, T2,T3
WHERE T1.a1 = T2.a2 AND T1.a1  =T3.a3
```

Field	Value
Command	SELECT
Projection Tables	[1 1 0]
Projection Columns	[[1 0 1] [0 0 1] [0 0 0]]
Selection Tables	[1 1 1]
Selection Columns	[[1 0 0] [1 0 0] [1 0 0]]

Supervised Case Key Ideas

PURDUE UNIVERSITY Discovery Park

- Associate each query with a role
- Build profiles per role
- Train a classifier with role as the class
- Declare a request as anomalous if classifier predicted role does not match the actual role

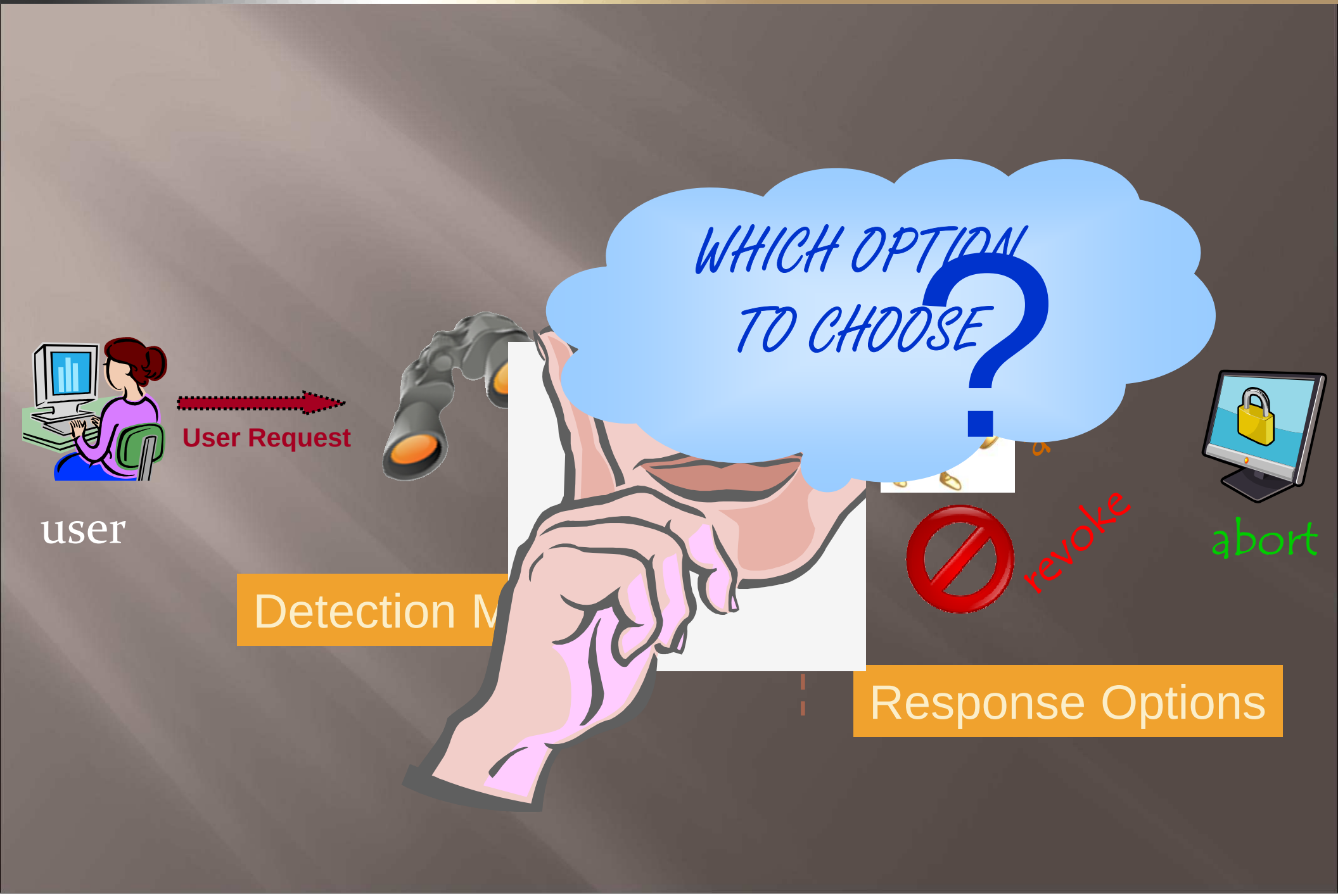
Next Steps

PURDUE UNIVERSITY Discovery Park

- Application to PLM
  - Determine and represent the units of data accesses
  - Represent and record the duration of user sessions
  - Represent and record the volume of accessed data
  - Profile data flows and use
  - Represent and record access patterns in time
  - Profile application programs

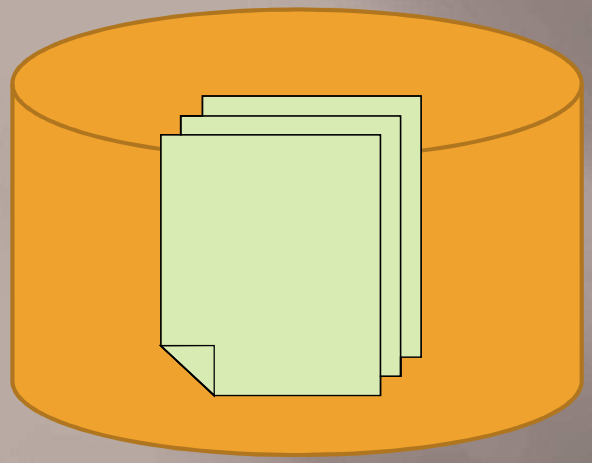
Response Mechanism - *An Important Issue*

PURDUE UNIVERSITY Discovery Park



Database Response Policies

PURDUE UNIVERSITY Discovery Park



Response Policy Language
ECA

ON	{Event}
IF	{Condition}
THEN	{Initial Action}

Policy 3 Re-authenticate un-privileged users who are logged from inside the organization's internal network for write anomalies to tables in the dbo schema. If re-authentication fails, drop the request and disconnect the user else do nothing.

```
ON ANOMALY DETECTION
IF Role != DBA                          and
   SourceIP IN 192.168.0.0/16           and
   Obj Type = table                     and
   Objs IN dbo.*                        and
   SQLCmd IN {Insert,Update,Delete}
THEN SUSPEND
CONFIRM re-authenticate
ON SUCCESS NOP
ON FAILURE ABORT,DISCONNECT
```

Is Anomaly Detection Sufficient?

PURDUE UNIVERSITY Discovery Park

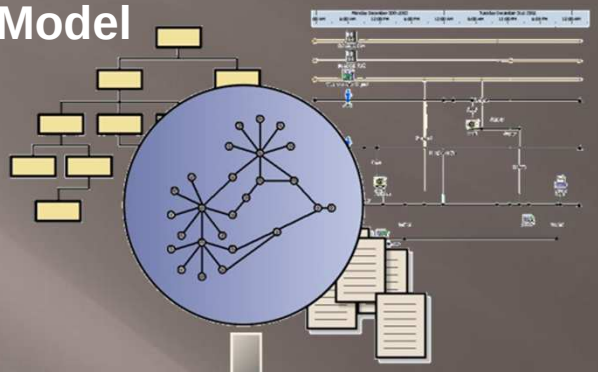
Look at the various mechanisms used by insiders
(from 2010 CyberSecurity Watch Survey)

Copied information to mobile device (USB drive, iPod, etc.)	42%
Downloaded information to home computer	38%
Stole information by sending it out via email	34%
Shared account (e.g. system administrator, DBA, etc.)	33%
Stole hardcopy information	30%
Compromised an account	28%
Remote access	25%
Used authorized system administrator access	25%
Stole information by downloading it to another computer	25%
Escalated privileges	22%
Blackberry or other mobile handheld device	20%
Social engineering	17%
Password crackers or sniffers	16%
Backdoors	13%
Rootkit or Hacking Tools	9%
Malicious code inserted as part of the software development process	5%
Logic bomb	2%
Other	8%
Don't know	11%

A Comprehensive Approach

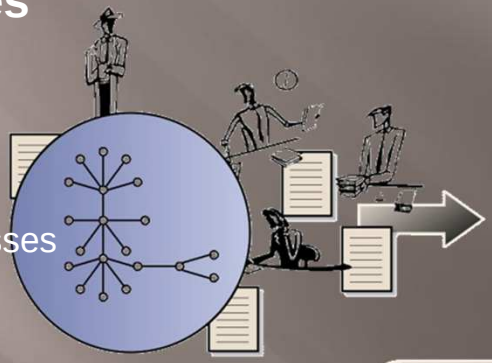
PURDUE UNIVERSITY Discovery Park

Expected Behavior Model



Observable Activities

- database accesses
- printing
- email
- file accesses
- external device accesses
- encryption



Risk Assessor

Risks & Alerts

Social Network Analysis

Database Access Analysis

Data Flow Analysis

Anomaly Detectors

THANK YOU