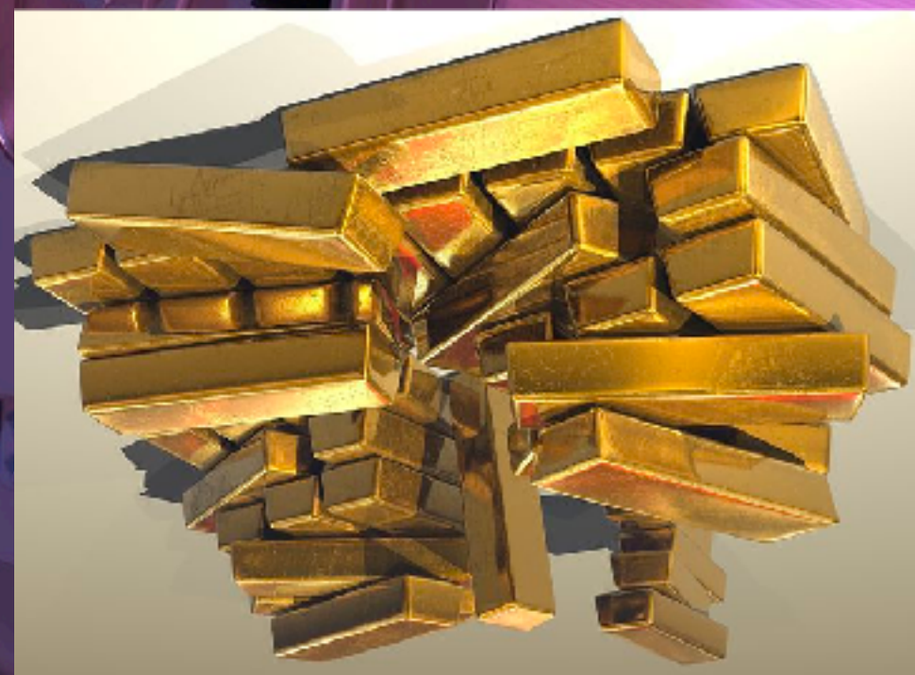
LOG ANALYSIS

Computer Security
Computer Engineering, Chulalongkorn University

Instructor: Kunwadee Sripanidkulchai, Ph.D.

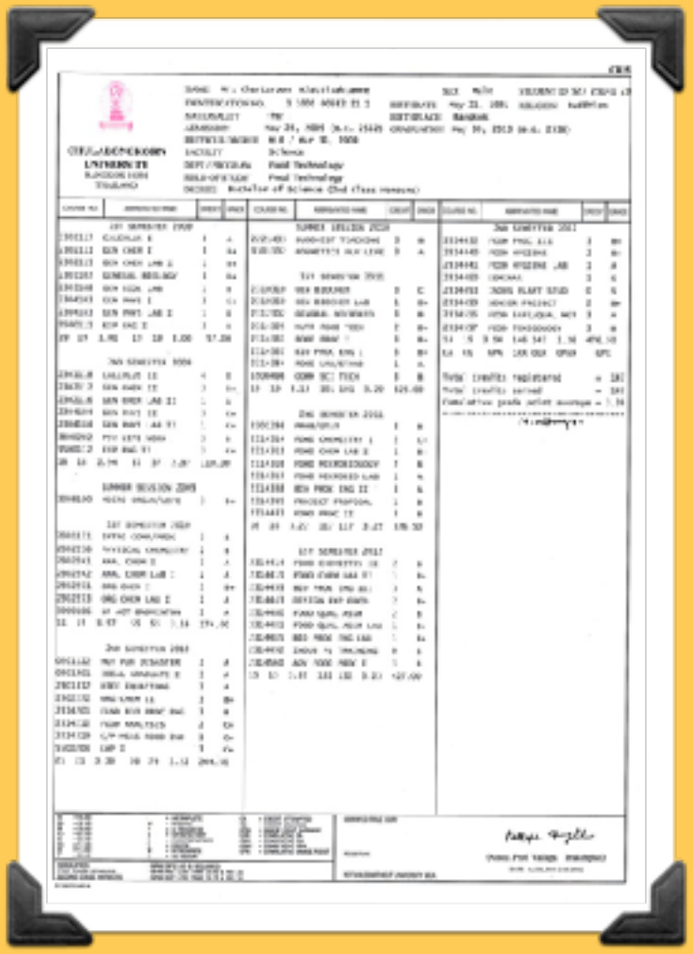


Chulalongkorn University Registration

Chulalongkorn University Regis...

สำนักงานการทะเบียนและประมวลผล
จุฬาลงกรณ์มหาวิทยาลัย

เข้าสู่ระบบลงทะเบียนเรียน



กรุณาป้อนเลขประจำตัวนิสิต/เลขประจำตัวเจ้าหน้าที่ และรห

ผ่านที่ใช้กับระบบอินเตอร์เน็ตของสำนักงานจัดการระบบเทคโนโลยีสารสนเทศ วิทยาลัย

เข้าสู่ระบบการลงทะเบียนเรียนของสำนักงานการทะเบียนและประมวลผล มีข้อ

องดำเนินการด้วยตนเอง และห้ามดำเนินการแทนนิสิตผู้อื่น มิฉะนั้นนิสิตจะถูกล

รับผิดชอบผลการลงทะเบียนเรียนที่เกิดขึ้นจากรหัสผ่าน (Password) ของนิสิต

การทะเบียนและประมวลผลกำหนดให้นิสิตแต่ละคนยืนยันการลงทะเบียนเรี

รวจสอบผลการลงทะเบียนเรียนทันทีทุกครั้งหลังจากที่ทำการลง

อนเรียนผ่านทางอินเทอร์เน็ตและควรพิมพ์ผลการลงทะเบียนเรี

ิชา เพื่อตรวจสอบและเก็บไว้เป็นหลักฐาน

นิสิตกระทำการใดๆ อันเป็นการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การลัก

อกวนระบบคอมพิวเตอร์ หรือการอื่นใดซึ่งอาจทำให้ระบบคอมพิวเตอร์เสี

มหาวิทยาลัย ว่าด้วยวินัยนิสิต ฉบับที่ ๒ ข้อ ๙/๒)เช่นเขียนโปรแกรมยืนยั

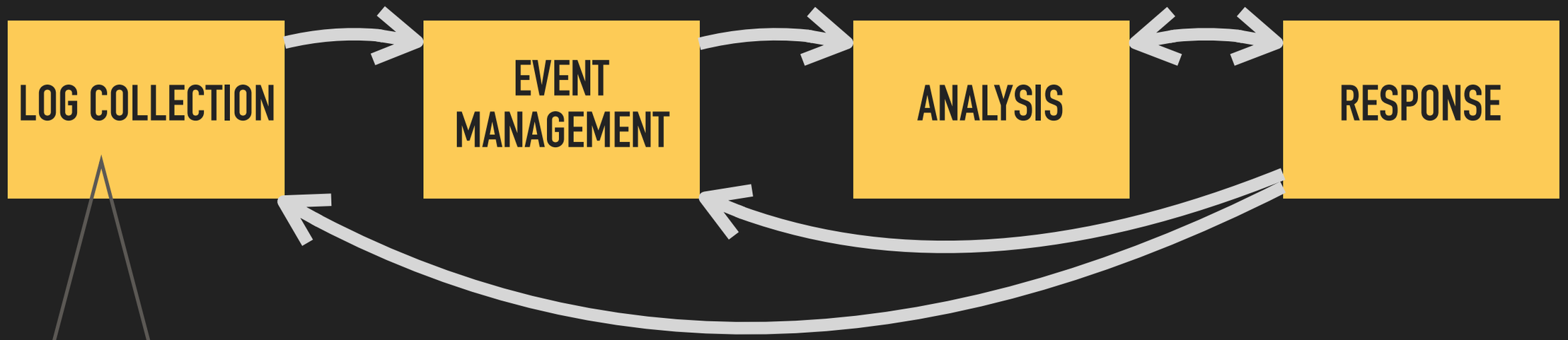
เป็นต้น นิสิตจะถูกลงโทษทางวินัย และ ห้ามเข้าระบบ

ขออภัยระบบกำลังปรับปรุงสามารถรองรับได้เฉพาะ Internet Explorer Browser เท่านั้

เลขประจำตัว

รหัสผ่าน

LOG ANALYSIS WORKFLOW

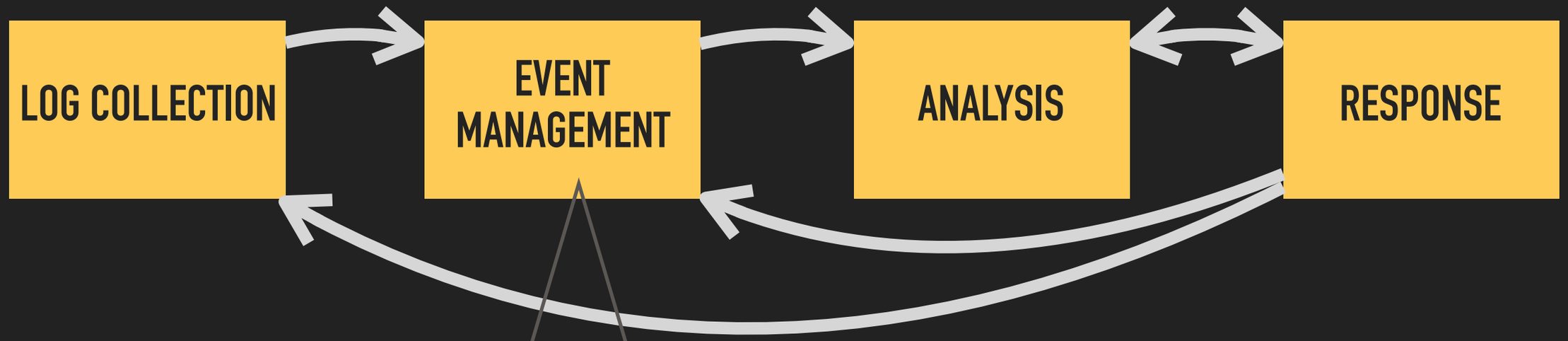


Logs

Sources: syslogs, event logs, app logs, IDS/IPS/firewall logs, network logs, infrastructure logs

Warning: no standard format! sort of like this “date time event”

LOG ANALYSIS WORKFLOW



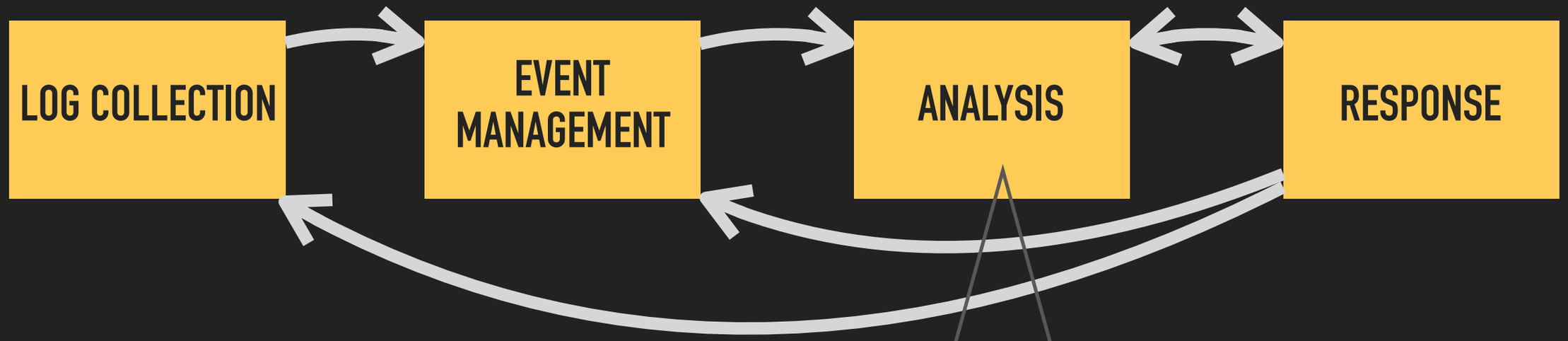
What to keep: all vs. filtered?

How to store: centralized, backup/archived, what format, raw vs. parsed,

Preprocess the logs: index, summaries

Who can access them: direct access vs. programmatic access, dashboard, sensitivity of the data

LOG ANALYSIS WORKFLOW

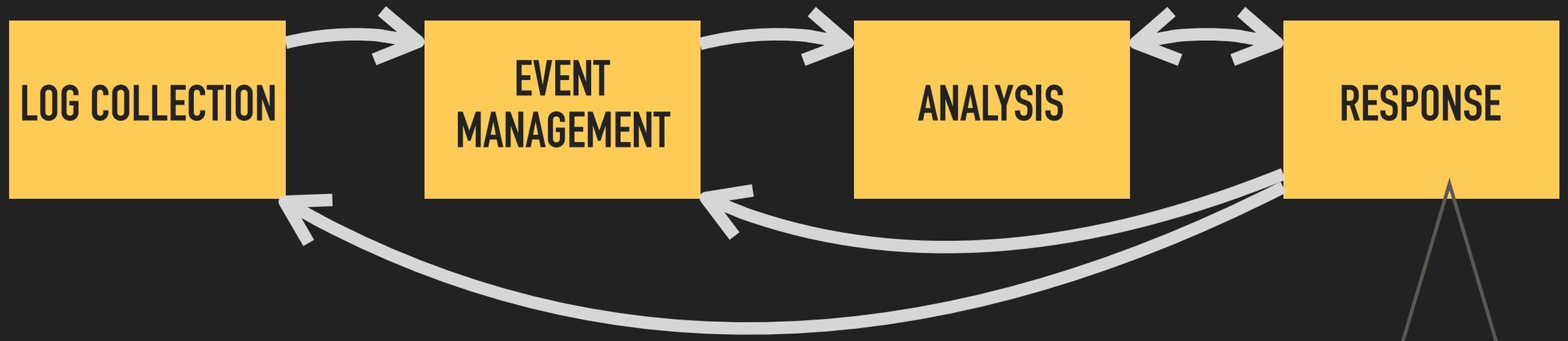


- Manual
- Alerts
- Automated
- Deep dives

- Statistical analysis
- Anomaly detection
- Association analysis
- AI/Machine Learning

- Real-time
- Post-mortem

LOG ANALYSIS WORKFLOW



- Reporting
- Incidence response
- Evidence preservation
- Lessons learned

LOG ANALYSIS ACTIVITY

?