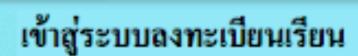
# LOG ANALYSIS

Computer Security
Computer Engineering, Chulalongkorn University

Instructor: Kunwadee Sripanidkulchai, Ph.D.



Chulalongkorn University Registration





Chulalongkorn University Regis...

TABLE W. Chertaron shouldakamen SEZ Wile SEZENCEDES CENE OF TRANSPORTENSE. 5 SAM ARRESTS SERVICES MY ZL. SAM REALISM MARKALET. The ARROSSO NA PR. SAM (A. 1548) CONTRACTOR MY N. DES SAN EXIST SETTIMENTAL MARKET MY P. E. 5000

| Section | Sect

IS NO DECIDE ON 

tome with

สำนักงานการทะเบียนและประมวลผล จูฟาดงกรณ์มหาวิทยาดัย

DETERMINENT Field Technology

ESPORT OF RECORD AND PARTY OF STREET, CE-DR man need room

Discussive 2012
100204 management
111-101 managemen

26 3-20 307 317 31-27

4 1

TEXT-ADDRESS CHORN

LNINERN TE RANDOS HON TRALANO

SPECIAL SECURITY OF SPECIAL SECURITY SPECIAL SPECIAL SECURITY SPECIAL S

200 SERVITE 1000 2012-0 LALINUT 12 2001-5 SER SON 12 2005-6 SER SON 12 2005-6 SER SON 12 2005-0 SER SON 14 2005-2 SER SON 14 2005-2 SER SON 11

DAMES SUCION ZOES

OCCLUDE THE PUR PERSONNEL P. SPECIAL STREET STREET P. SPECIAL STREET STREET

THE TO SEE THE PROPERTY OF THE

HEATHER.

กรุณาป้อนเลขประจำตัวนิสิต/เลขประจำตัวเจ้าหน้าที่ และรห

เผ่านที่ใช้กับระบบอินเตอร์เน็ดของสำนักงานจัดการระบบเทคโนโลยีสารสนเทศ **เ** 

เจ้าสู่ระบบการจงทะเบียนเรียนของสำนักงานการทะเบียนและประมวลผล มีจั

องคำเนินการด้วยตนเอง และท้ามคำเนินการแพนนิสิตผู้อื่น มิละนั้นนิสิตจะถูกล ับคิดขอบผลการลงทะเบียนเรียนที่เกิดขึ้นจากรทัสผ่าน (Password) ของนิสิต การทะเบียนและประนวลผลกำหนดให้นิสิตแต่ละคนฮืนอันการลงทะเบียนเรือ

หรวจสอบผลการลงทะเบียนเรียนพันพีทุกครั้งหลังจากที่ทำการลงท งอนเรียนค่านทางอินเทอร์เน็คและควรพิมพ์ผลการลงทะเบียนเรีย วา เพื่อครวจสอบและเก็บไว้เป็นหลักฐาน

ใช้ตกระทำการใดๆ อันเป็นการเข้าถึงระบบคอมพิวเตอร์โดยมีขอบ การลัก อกวนระบบคอมพิวเตอร์ หรือการอื่นใดซึ่งอาจทำให้ระบบคอมพิวเตอร์เฉี มหาวิทธาลัย ว่าด้วยวินัฮนิสิต ฉบับที่ ь จ๊อ ๙/๒)เร่นเขียนโปรแกรมฮินฮัา เป็นค้น นิสิตจะถูกลงไทษทางวินัอ และ ท้ามเข้าระบบ

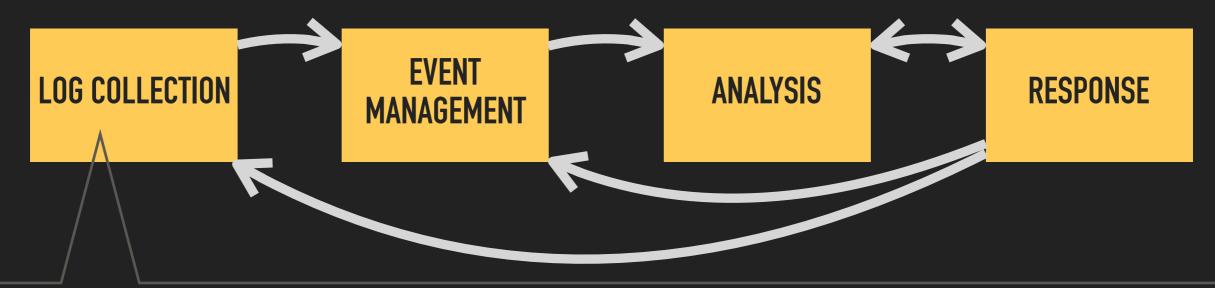
ของกับระบบกำลังปรับปรุงสามารถรองรับได้เฉพาะ Internet Explorer Browser เท่านี้

เลขประจำตัว

รหัสผ่าน

IS NOT AN OFFICIAL.

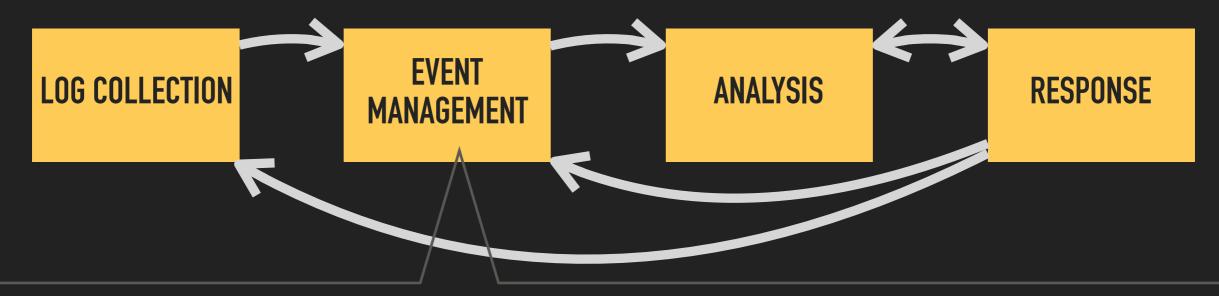
...ทยาลัย



#### 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"

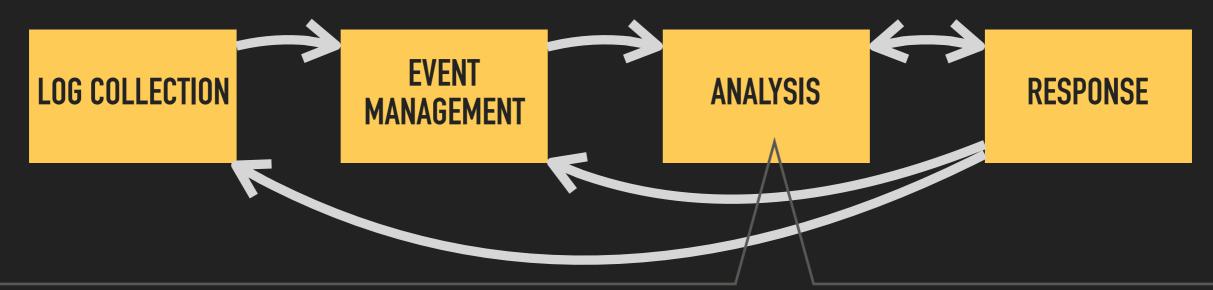


What to keep: all vs. filtered?

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



Manual

**Alerts** 

**Automated** 

Deep dives

Statistical analysis

Anomaly detection

Association analysis

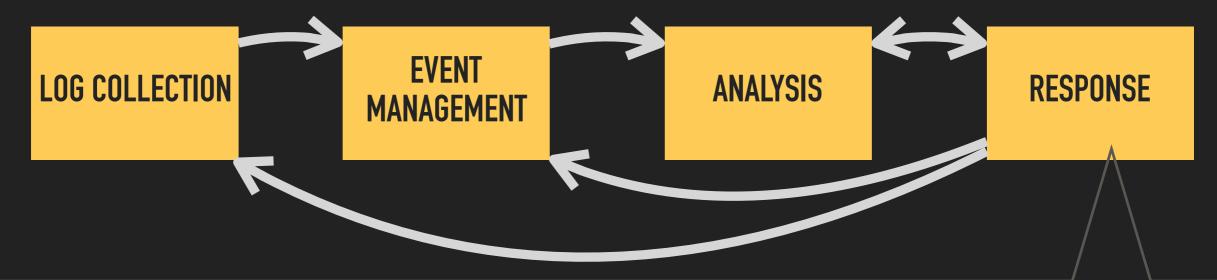
Al/Machine Learning

Real-

time

Post-

mortem



Reporting

Incidence response

Evidence preservation

Lessons learned

# LOG ANALYSIS ACTIVITY



