

Ensuring and Improving the Quality of Log Files



Peter Mosmans

LEAD PENETRATION TESTER

@onwebsecurity <https://www.onwebsecurity.com>

Module Overview



Where to Record Log Data

The Format of Log Files

Logging Personal Data

Where to Record Log Data

Log Locations



Logging locally
Separate partition
Access controls



Logging remotely

Centralized Logging Management



Encryption

- Transport from application
- Storage

Access control mechanism

Integrity checks

Fail-over system

Backup

Use Existing Log Management Systems



Leverage existing

- infrastructure
- knowledge
- alerting systems



The Format of Log Files

Metadata Requirements

What

When

Where

Who

When



Different timestamps

- Source
- Destination

Synchronize time sources

Make sure to include timezone

- Standard RFC 3339

Time resolution



Where



Log source address

- Responsible for logging the entry

Originating address

- Responsible for generating the event

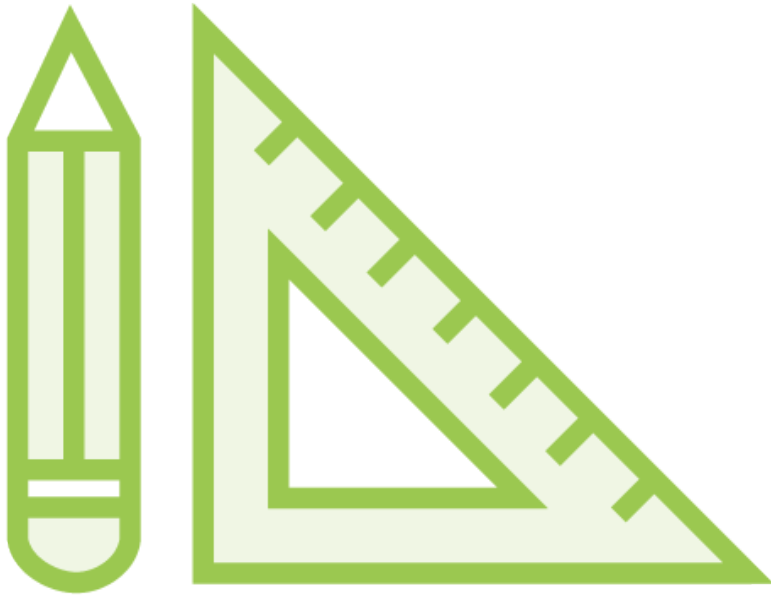
Who



Logged on user
Unique identifier



Standards



Syslog

- Standard RFC 5424

Common Log Format

Use a company standard, when available

Use the same settings everywhere

- Timestamps
- Encoding
- Severity levels

Severity Levels



- 0 Emergency: system is unusable
- 1 Alert: action must be taken immediately
- 2 Critical: critical conditions
- 3 Error: error conditions
- 4 Warning: warning conditions
- 5 Notice: normal but significant condition
- 6 Informational: informational messages
- 7 Debug: debug-level messages

Be consistent

Logging Personal Data

Logging Personal Data



Try to minimize amount

- Only with a valid reason
- Cleared with legal department

Encryption

Pseudonymization

Encryption vs. Pseudonymization

Encryption

Converting personal data to encrypted format

Encryption key

Key is used for multiple records

Key management

Strong encryption algorithm

Pseudonymization

Replacing personal data with an artificial identifier (pseudonym)

Link table

One identifier per record

Pseudonymized Log Records



2019-03-09 login **tPuBaV9s5sM6Y5ooQrD3SDuK**



2019-03-09 login **MHy24Q7AGb5rKSBukidPoQAM**



2019-03-09 logout **tPuBaV9s5sM6Y5ooQrD3SDuK**

**Privacy
Enhancing
Technique**



Consult the Legal Team



Legal Department



Team

Summary



Use (existing) remote centralized server

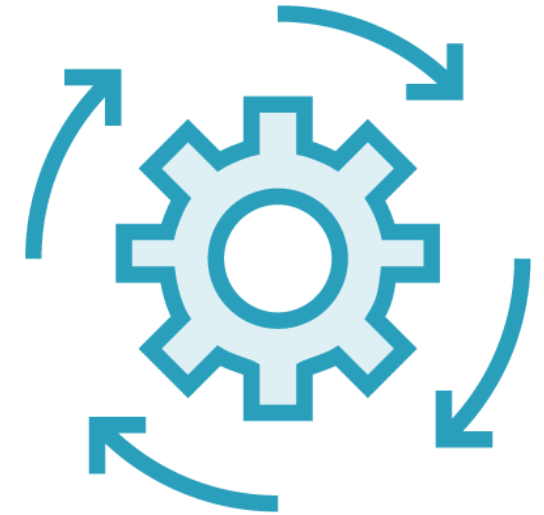
- Logging locally is insecure

Include what, when, where and who

Personal data: Pseudonymization

Be consistent

Next Up



**Applying an
Effective
Monitoring
Strategy**