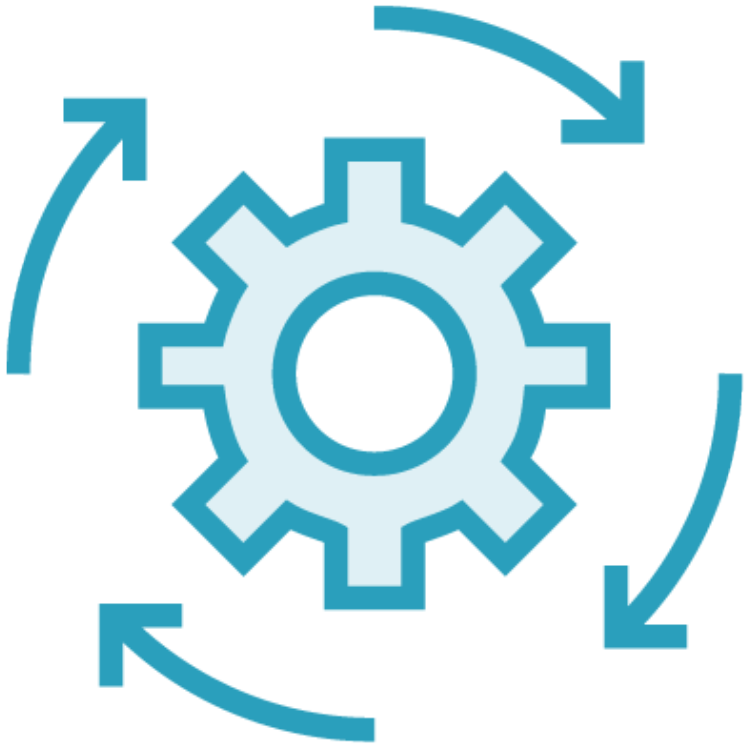
Applying an Effective Monitoring Strategy

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Module Overview



- Log Management
- Defining Response Strategies
- Existing Solutions
- Module and Course Summary

Log Management

Log File Life Cycle

Generation

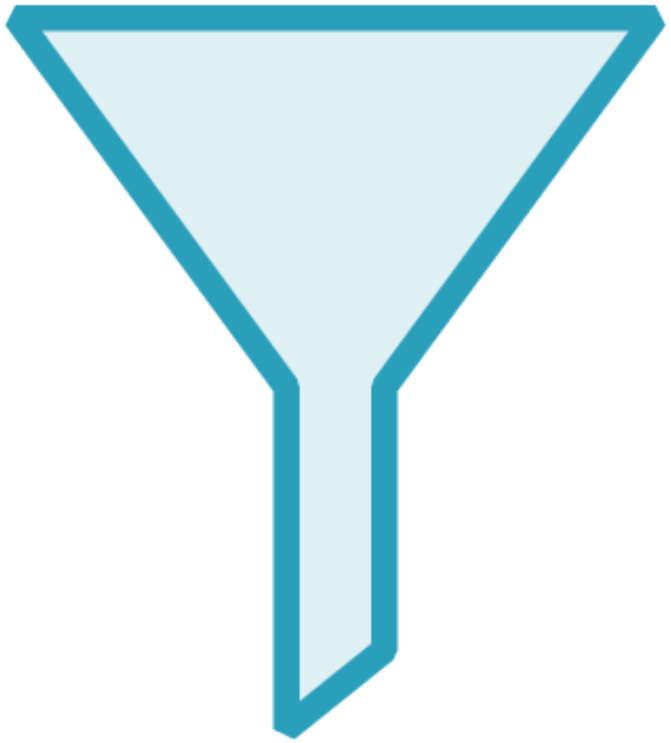
Transmission

Aggregation

Analyzing

Archiving

Log Aggregation



Consolidate duplicate events

Add structure

Remove sensitive fields

- Pseudonymization

Security

- Input validation
- Encoding
- Filtering

Analyzing

- Baselining
- Anomaly detection
- Attack signatures
- Escalation, response

Archiving

Decryption keys

Protection

Do not underestimate configuration

Software Development Life Cycle

Defining Response Strategies

Response Strategies

Security policy and plans are leading

- NIST 800-61

Preparation, identification and containment

Set reasonable limits

Use common sense

Ideal Situation

HELP! I'm under attack!

Add time synchronization to server

Log authentication and authorization

- Successes
- Failures

Log to existing log management server

Set up alerting triggers

- Authentication

Regularly check and improve logging monitoring

Talk to development department

- Add control

Available Solutions

Disclaimer

Tools are not important

Do not put tools before operation

- Know what you want to monitor beforehand

There are no silver bullets

OWASP AppSensor

Open source framework

Real time

- event detection
- analysis
- response

Add hooks and policies

www.appsensor.org

OWASP ModSecurity

Open source web application firewall

Automatic defending capabilities

Plugs in webserver

modsecurity.org

Logging and Monitoring Tools

ELK Stack

- Elastic search
- Logstash
- Kibana

Security Information and Event Management

Security Event Management (SEM)

- Analyzes log and event data

Security Information Management (SIM)

- Assesses log data

Provide real-time analysis of security alerts

If available:

- Do try to add application logs

Test, and Verify

When running tests

- Observe alerts
- Check quantity and quality of data
- Validate procedures

Periodically recheck configuration

Summary

Log Management

- Remove sensitive fields on time
- Analysis phase takes time

Follow security policy and incident response and recovery plans

Tools should support you

Course Summary

Log and monitor for

- Timely discovery
- Escalation prevention
- Forensics

Determine what makes sense

Be consistent

Re-use existing infrastructure

It's a team effort

Security is a process

Insufficient Logging and Monitoring

A lack of situational awareness

Thanks for Watching!

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com