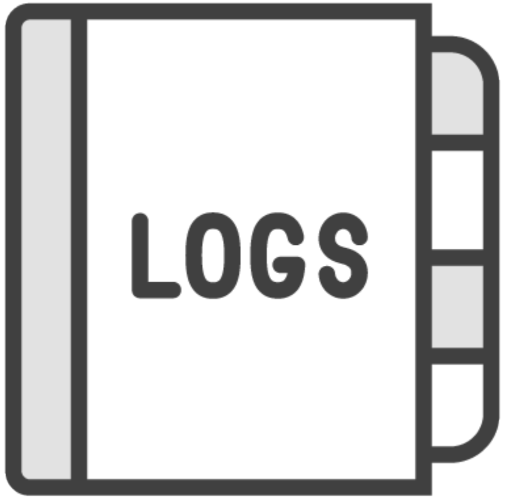
Secure Coding: Preventing Insufficient Logging & Monitoring

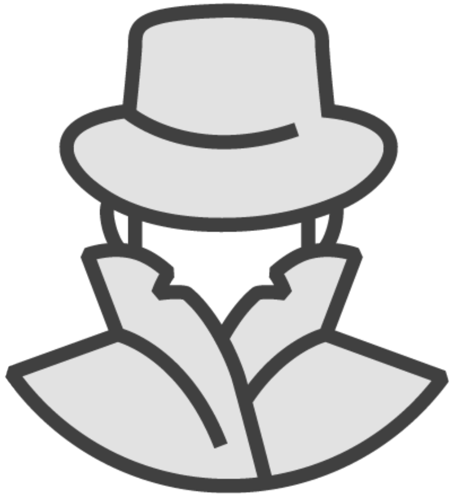
UNDERSTANDING INSUFFICIENT LOGGING & MONITORING

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Why This Course?





Course Overview

Understanding Insufficient Logging & Monitoring

What Applications Should and Shouldn’t Log

Ensuring and Improving the Quality of Log Files

Setting Up an Effective Monitoring Strategy

Setting the Scope

Security Software

Operating Systems

Networking Equipment

Applications

Determining the Audience

Software Developers

System Architects

DevOps Engineers

System Administrators

Security Professionals

Team

In order to properly defend,
logging and monitoring
is crucial

Module Overview

Introducing the Scenario

What Is Insufficient Logging & Monitoring?

Insufficient Logging & Monitoring and the OWASP Top 10

Logging, Monitoring and Alerting

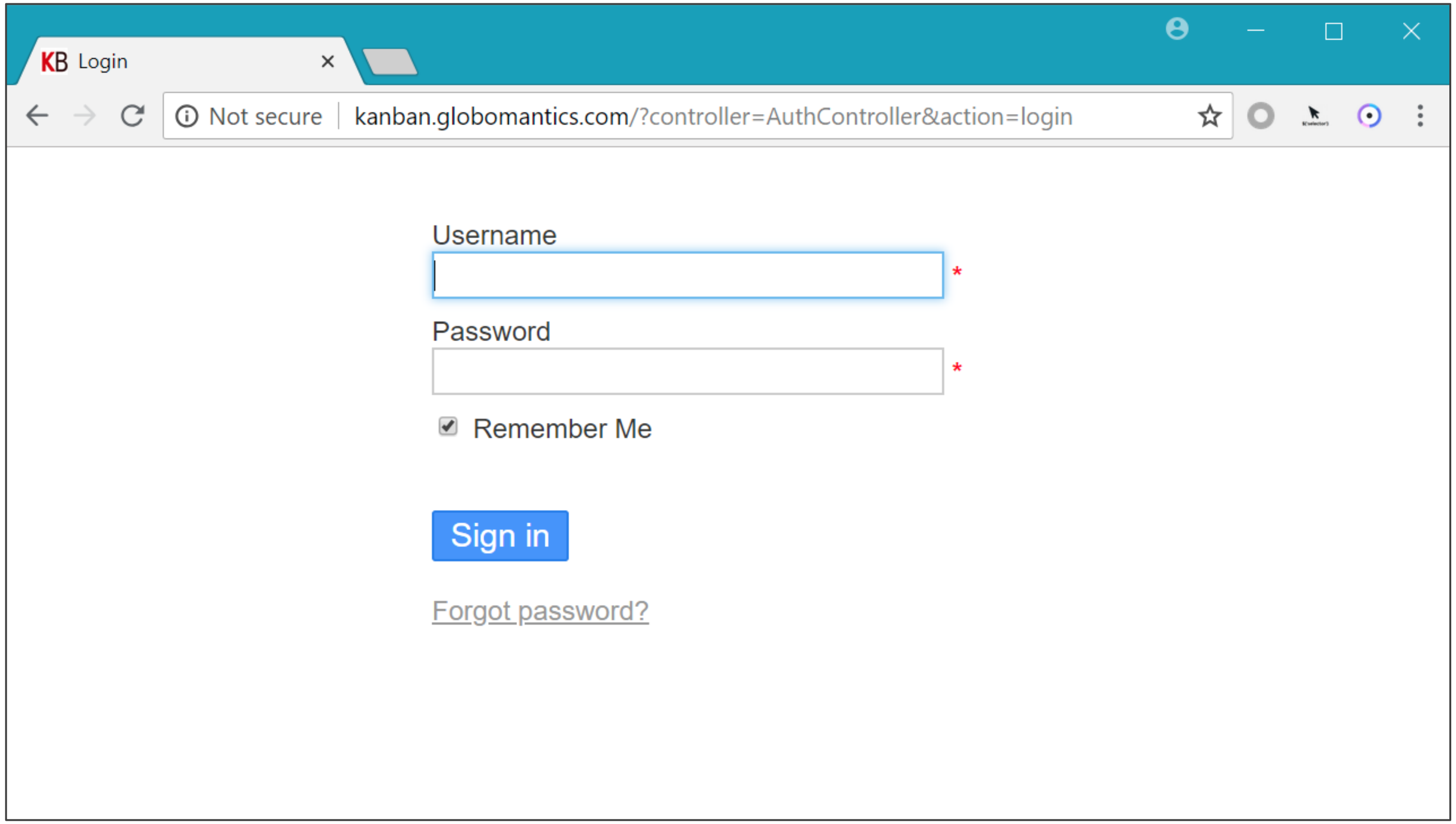
Introducing the Scenario

The Players

Dave the Defender
System Administrator

Alan the Attacker
The Bad Guy

Scenario



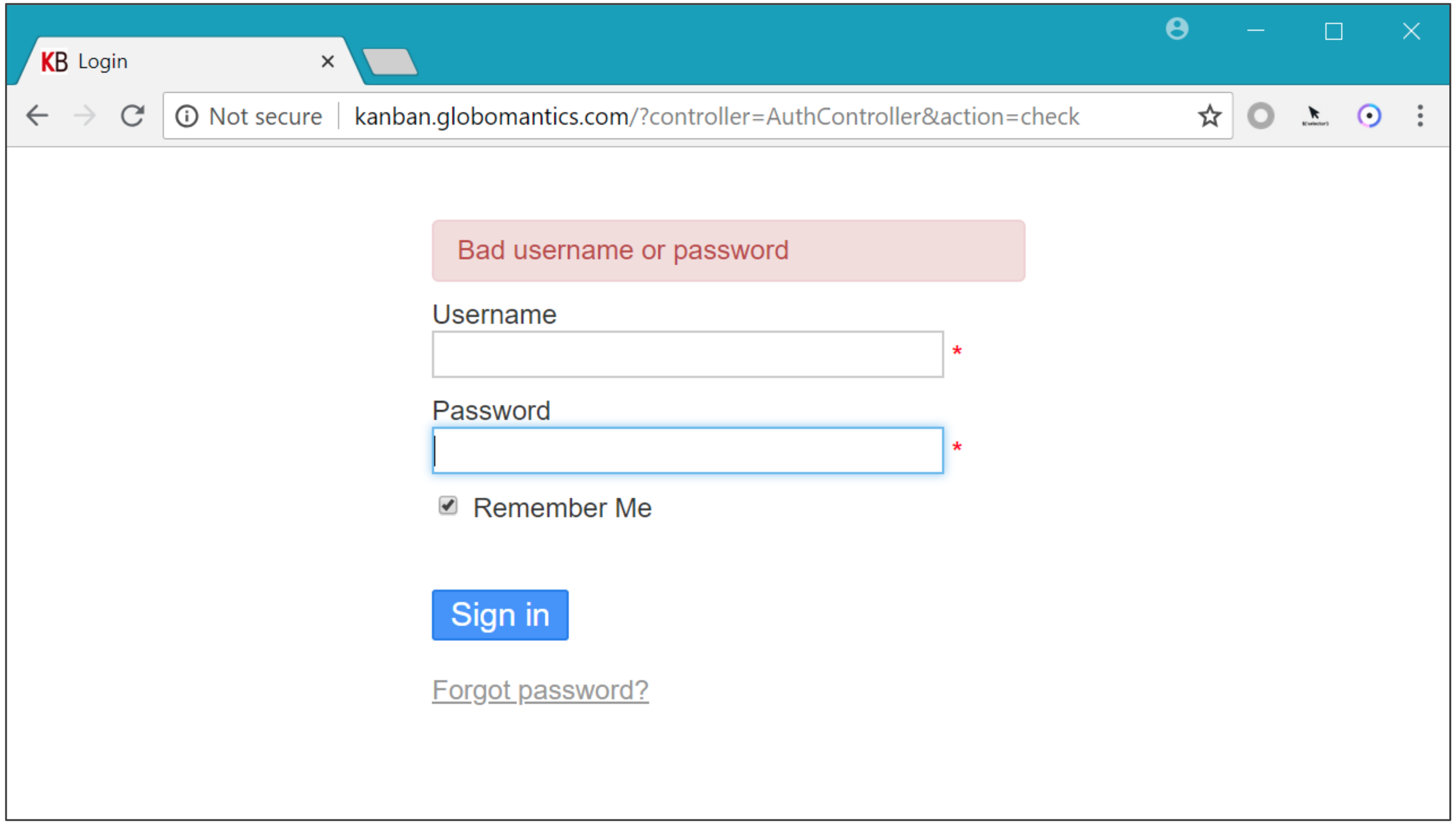
kanban.globomantics.com/?controller=AuthController&action=login

Username *

Password *

☑ Remember Me

Scenario



KB Login
Not secure
kanban.globomantics.com/?controller=AuthController&action=check

Bad username or password

Username *

Password *

☑ Remember Me

Sign in

Forgot password?

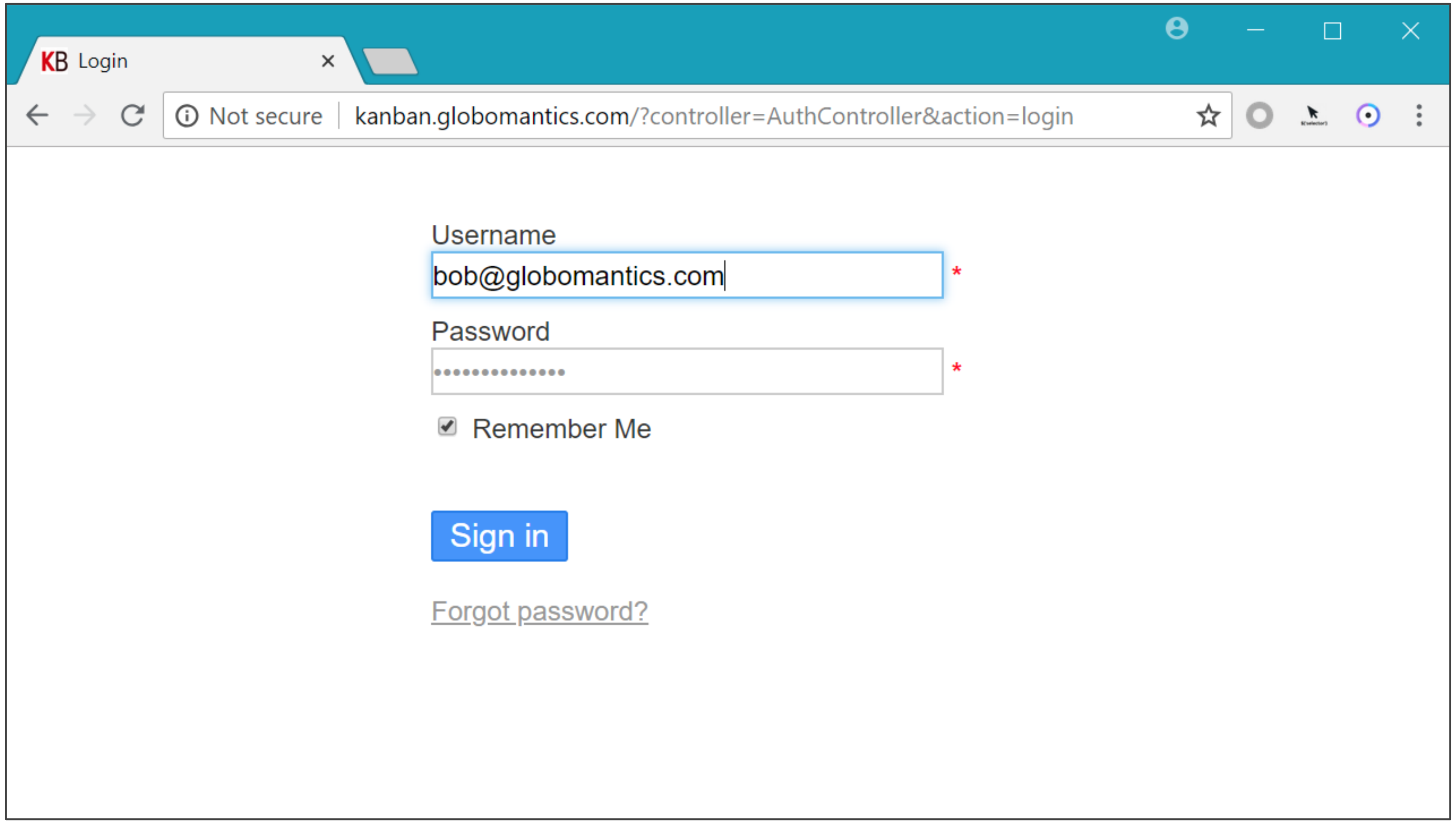
Looking for Leaked Passwords

username: bob@globomantics.com
password: ab89—PKJ

username: charlie@globomantics.com
password: goRAIDERS66

username: eva@globomantics.com
password: studio54

Credential Stuffing



kanban.globomantics.com/?controller=AuthController&action=login

Username *

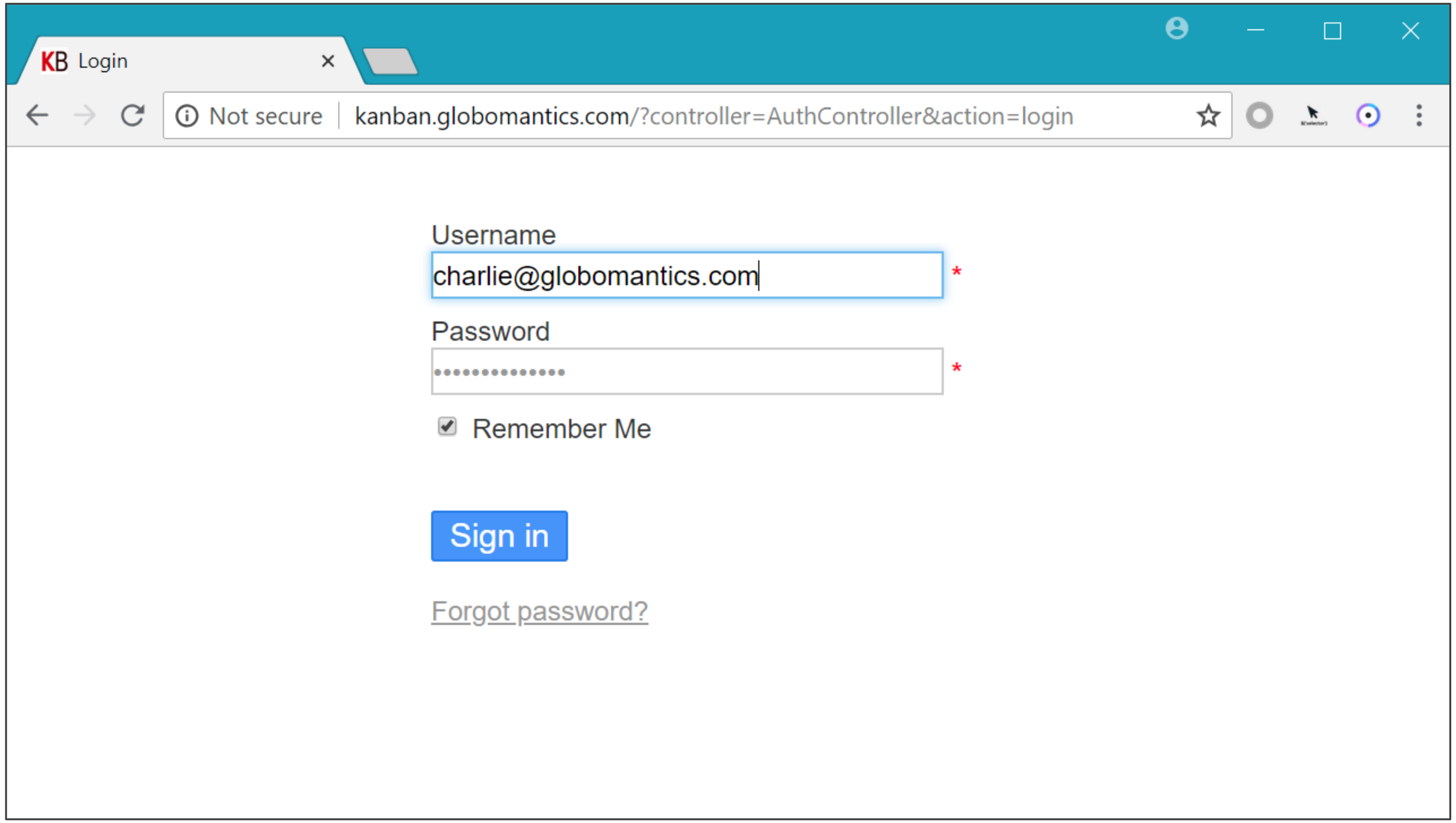
bob@globomantics.com

Password *

••••••••••••••

☑ Remember Me

Credential Stuffing



KB Login
Not secure
kanban.globomantics.com/?controller=AuthController&action=login

Username

charlie@globomantics.com *

Password

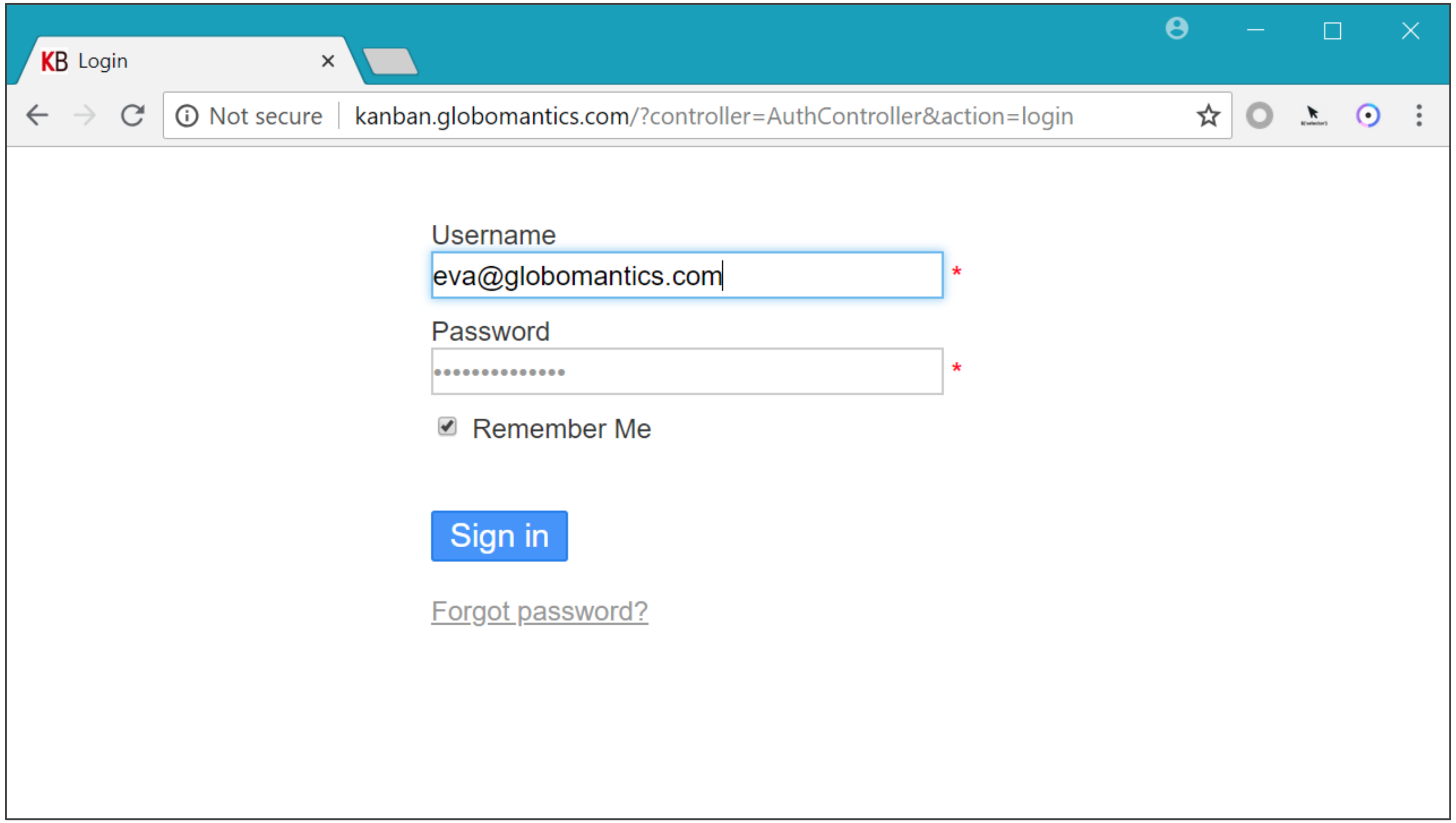
•••••••••••••• *

☑ Remember Me

Sign in

Forgot password?

Credential Stuffing



KB Login

Not secure | kanban.globomantics.com/?controller=AuthController&action=login

Username

eva@globomantics.com *

Password

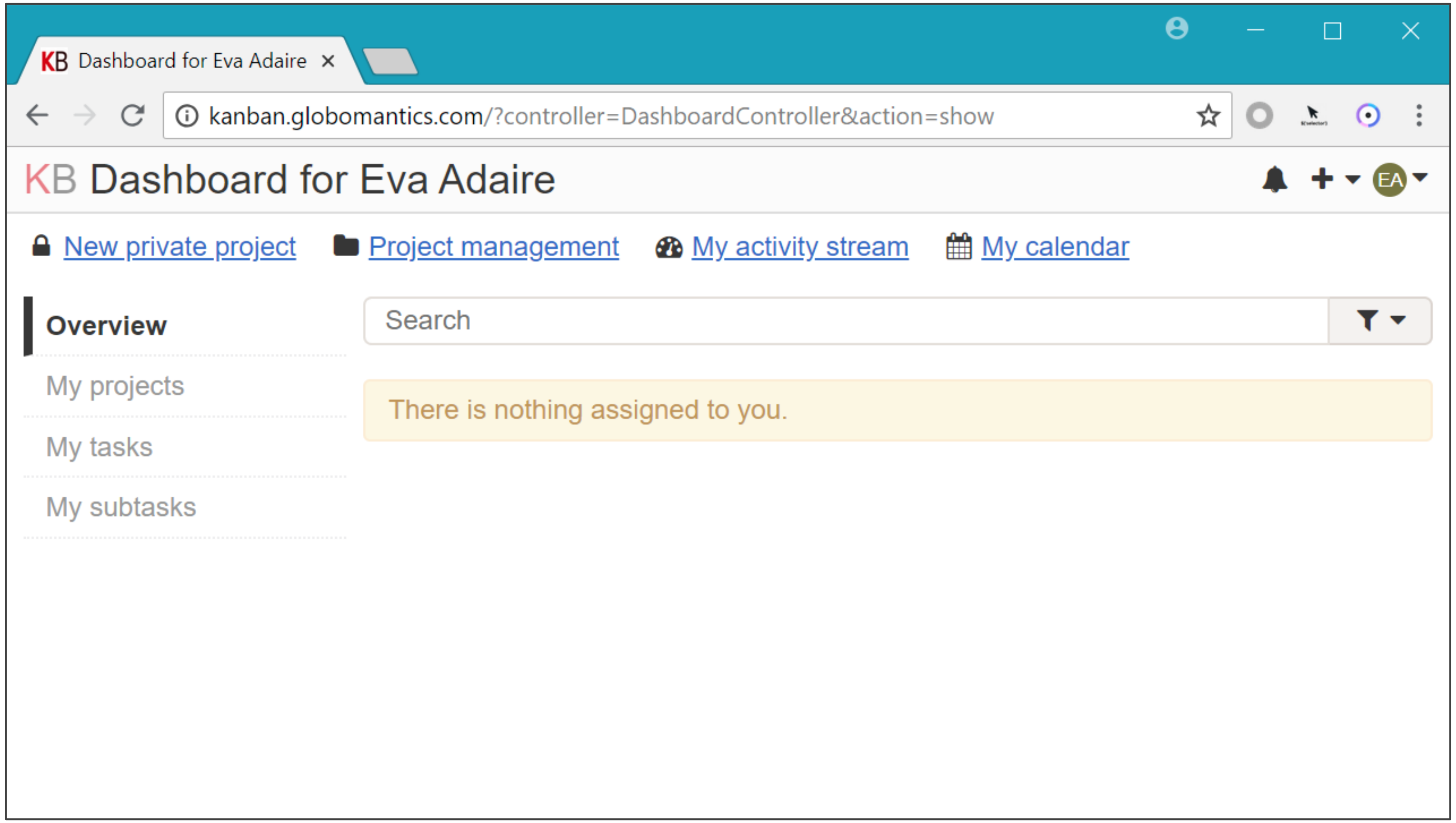
•••••••••••••• *

☑ Remember Me

Sign in

Forgot password?

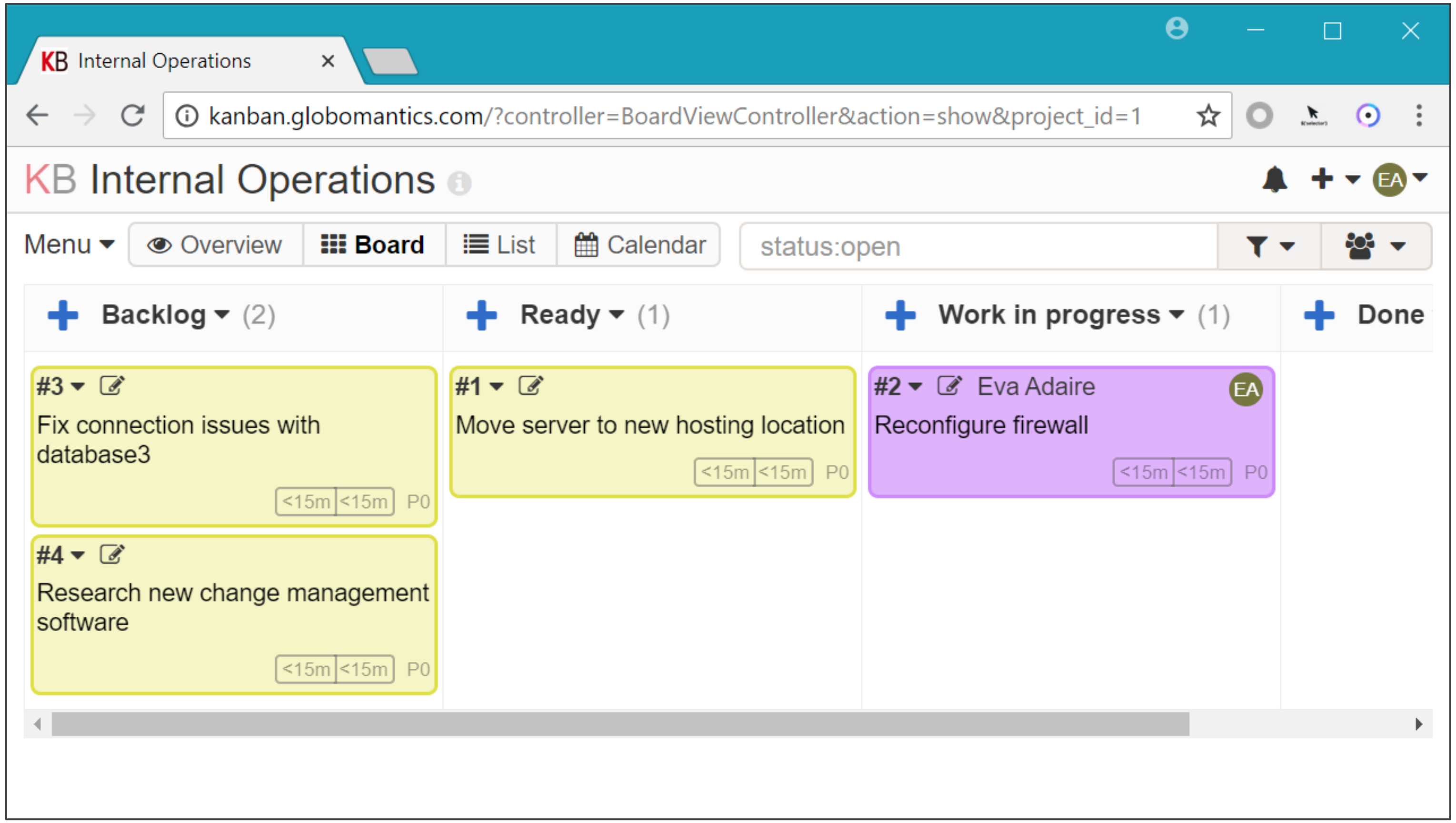
Successful Login



KB Dashboard for Eva Adaire ×
kanban.globomantics.com/?controller=DashboardController&action=show
KB Dashboard for Eva Adaire
EA
New private project
Project management
My activity stream
My calendar
Overview
My projects
My tasks
My subtasks
Search

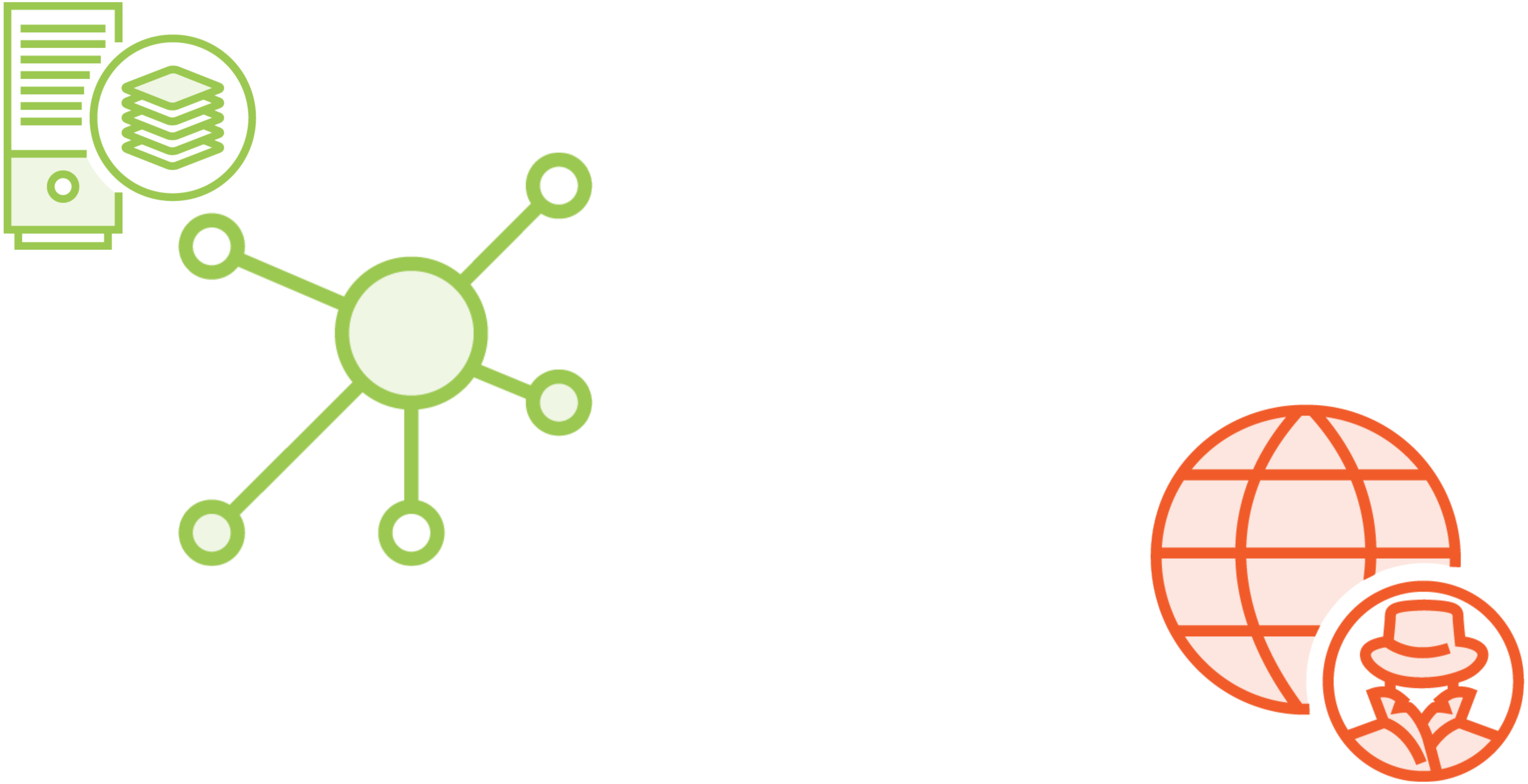
There is nothing assigned to you.

Information Gathering

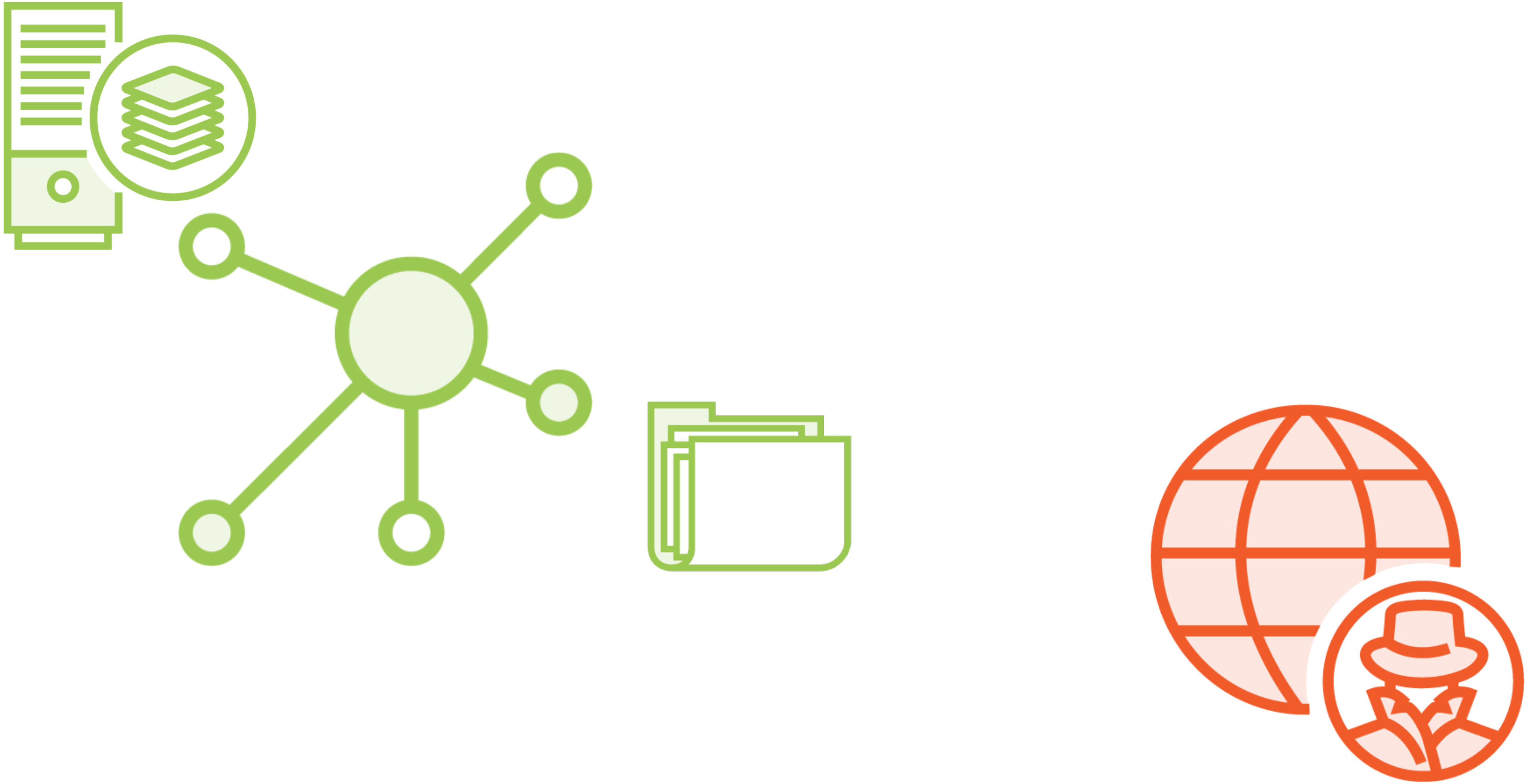


Backlog (2)	Ready (1)	Work in progress (1)	Done
#3 Fix connection issues with database3 <15m <15m P0 #4 Research new change management software <15m <15m P0	#1 Move server to new hosting location <15m <15m P0	#2 Eva Adaire EA Reconfigure firewall <15m <15m P0	

Network Pivoting



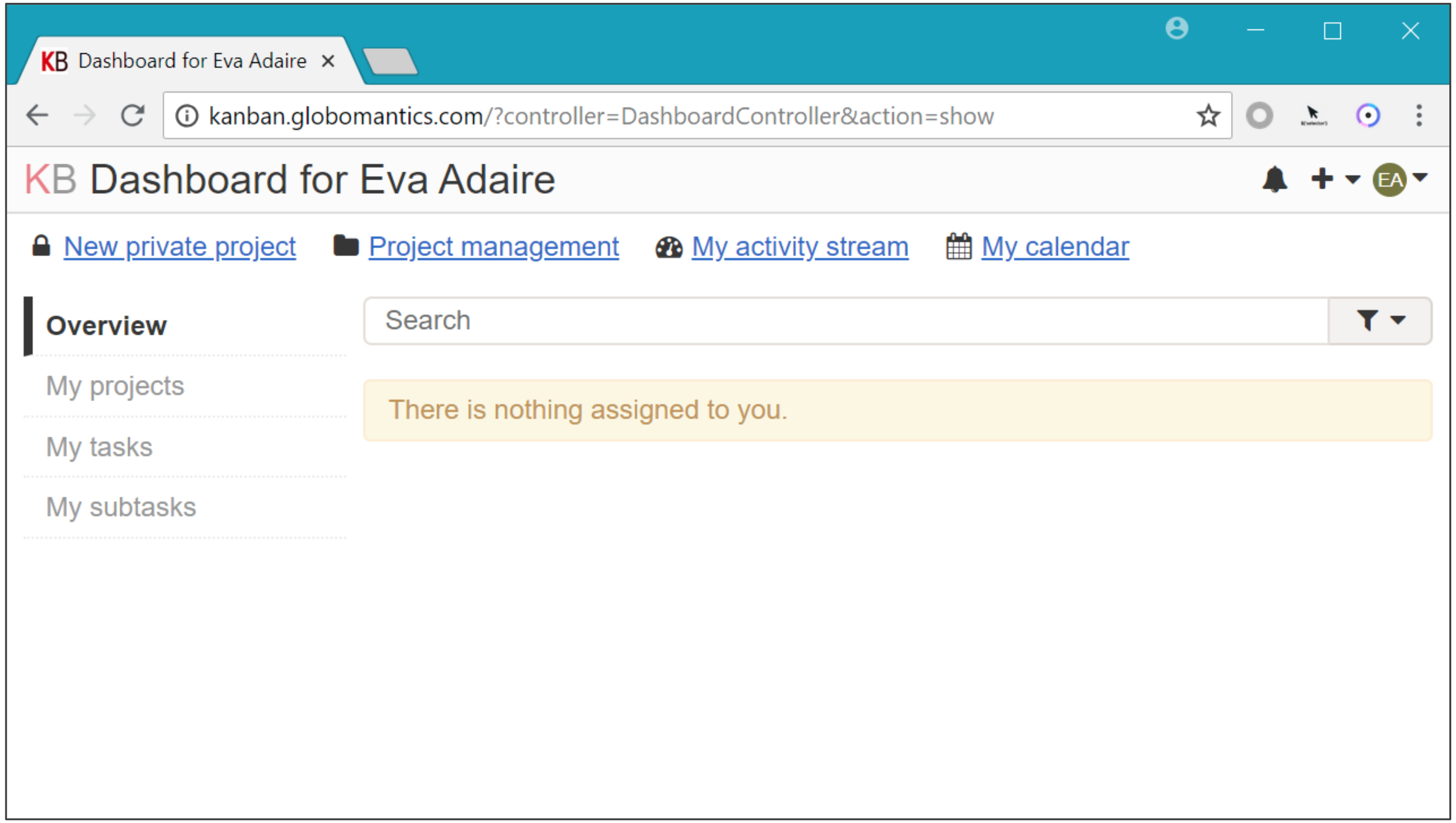
Data Exfiltration



Request for Ransom

Incident Response

Initial Intrusion



KB Dashboard for Eva Adaire ×
kanban.globomantics.com/?controller=DashboardController&action=show

KB Dashboard for Eva Adaire

New private project | Project management | My activity stream | My calendar

Overview

My projects

My tasks

My subtasks

Search

There is nothing assigned to you.

Detect intrusion on time

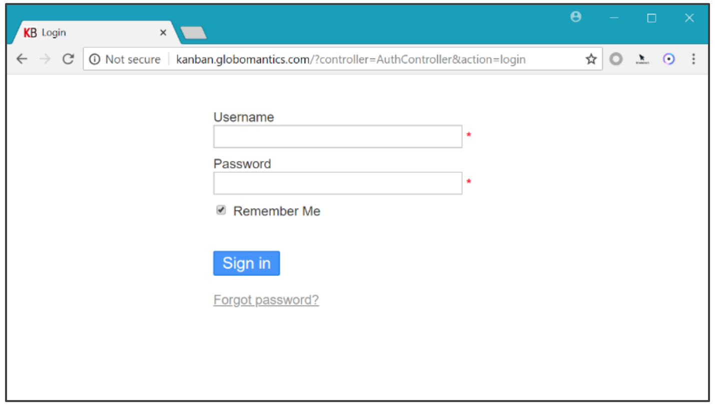
Prevent worse from happening

What Is Insufficient Logging & Monitoring?

Vulnerability

Control

Attacker


KB Login
Not secure
kanban.globomantics.com/?controller=AuthController&action=login
Username *
Password *
Sign in
Forgot password?

☑ Remember Me

Re-using Passwords

Does Not Match a Leaked Password

Attacker

Insufficient Logging and Monitoring

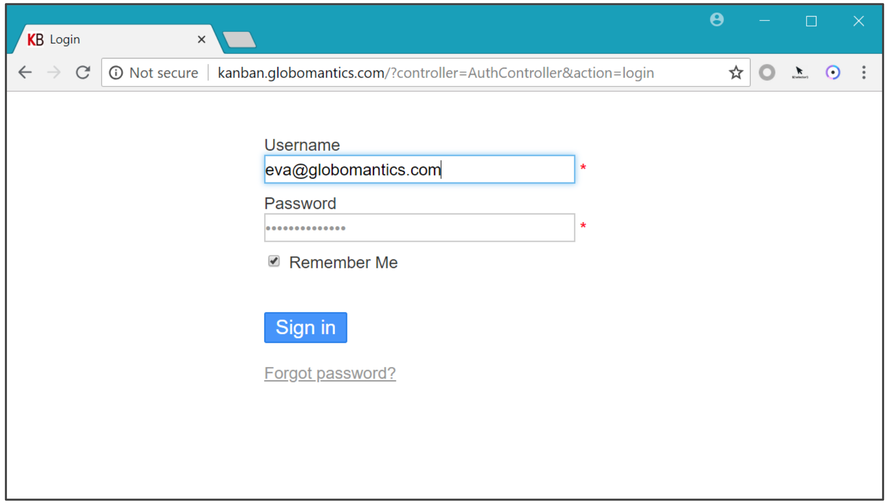
Lack of quantity of logged events

Lack of quality of log files

Lack of availability of log files

Failure to respond on time

What Is Happening?


KB Login
Not secure
kanban.globomantics.com/?controller=AuthController&action=login

Username

eva@globomantics.com *

Password

•••••••••••••• *

☑ Remember Me

Not Knowing What Is Happening

Lack of Quantity

Lack of Quality

Lack of Availability

No Timely Response

Lack of Situational Awareness

Insufficient Logging and Monitoring

A lack of situational awareness

Logging and Monitoring Is Necessary For

Situational awareness and timely discovery

Escalation prevention

Forensics

The initial compromise
is usually just the beginning

Insufficient Logging & Monitoring and the OWASP Top 10

Open Web Application Security Project

OWASP

Open Web Application
Security Project

Not-for-profit organization

Make software security visible

Content from volunteers

OWASP Top 10

OWASP Top 10 - 2017

Most critical web application security risks

Main goal to educate people

Input from

- data submissions
- industry survey

10: Insufficient Logging and Monitoring

A10
:2017

Insufficient Logging & Monitoring

MITRE

Not-for-profit organization

Solve problems for a safer world

Common Weakness Enumeration

List of software security weaknesses

No ranking

Categorization

Around 700 different weaknesses

CWE-778: Insufficient logging

When a security-critical event occurs, the software either does not record the event or omits important details about the event when logging it.

CWE-223: Omission of security-relevant information

The application does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.

Logging, Monitoring, and Alerting

Detective control

- Detects security violations

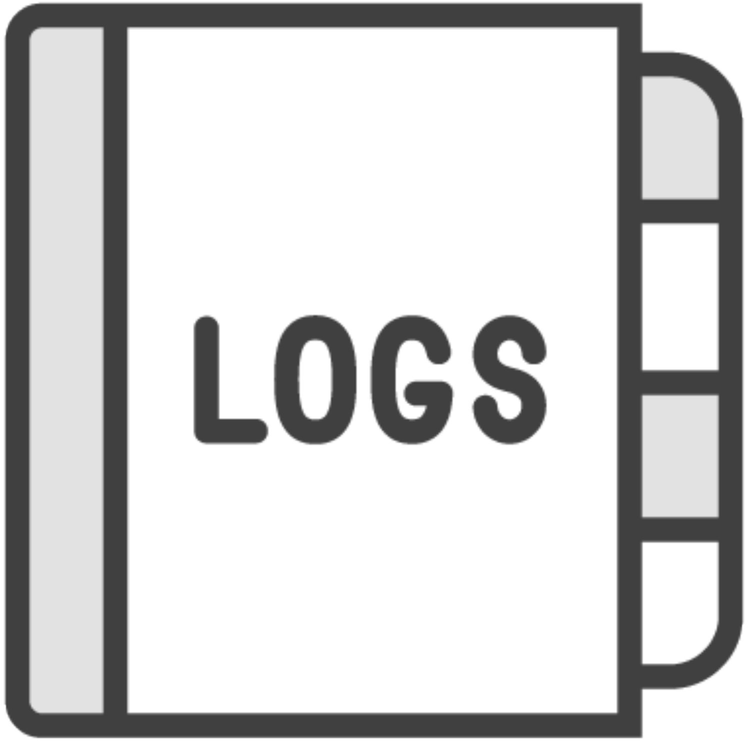
Event

- Generates log entry

Logging

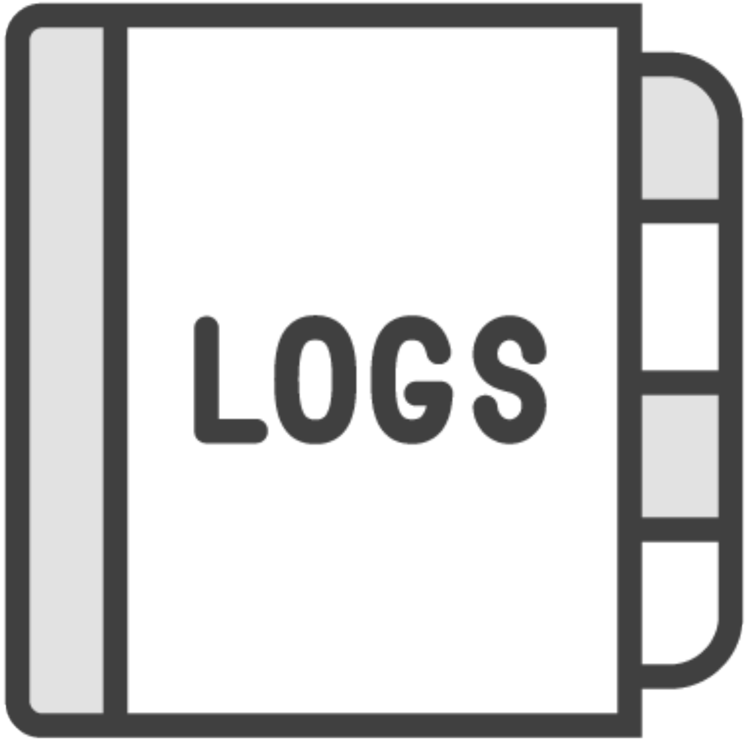
- Adding an entry to a log file

Log



A record of events that have occurred

Objective of Logging



Providing clues

- What
- When
- Where
- Who

Monitoring

Keeping an eye out on interesting events

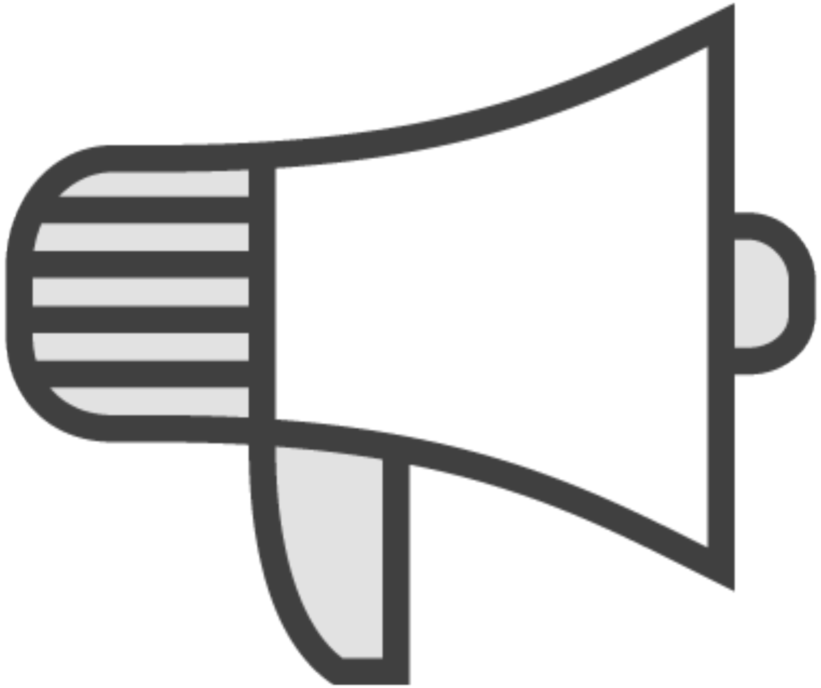
- Dependent on what is logged

Detective control

Objective of Monitoring

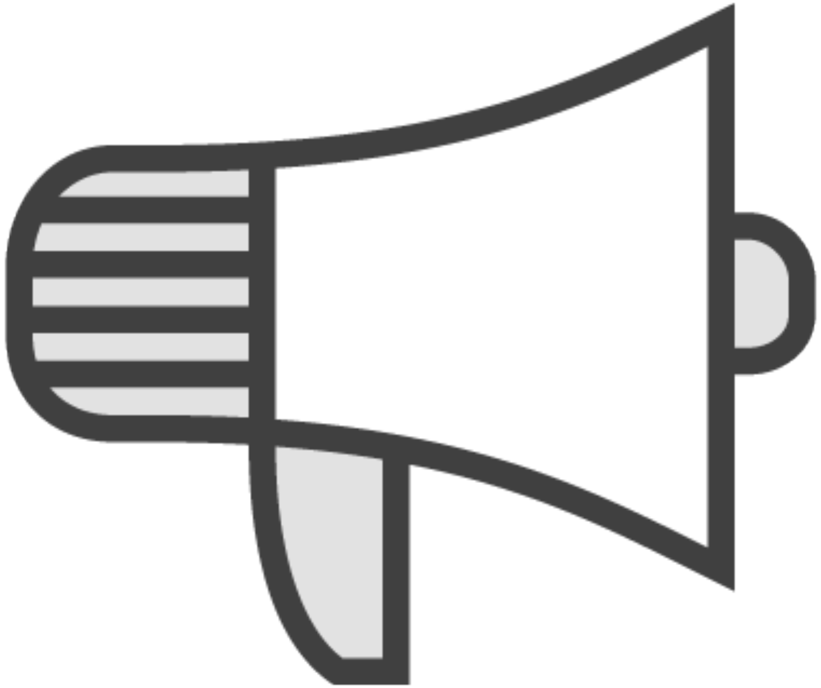
Providing timely detection

Alerting



Actively informing something / someone

Objective of Alerting



Generating a timely response

Objective of Logging and Monitoring

Creating situational awareness

Summary

Visibility

Escalation prevention

Forensics

- What
- When
- Where
- Who

Situational awareness

Next Up...

What Applications Should and Shouldn’t Log