# OSSEC

Ayten Tonbul - Berke Can Yaman - Enes Eyüboğlu

## WHAT IS OSSEC?

OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS)

# History of OSSEC

## In June 2008

the OSSEC project and all the copyrights owned by Daniel B. Cid, the project leader, were acquired by Third Brigade, Inc.

## In May 2009

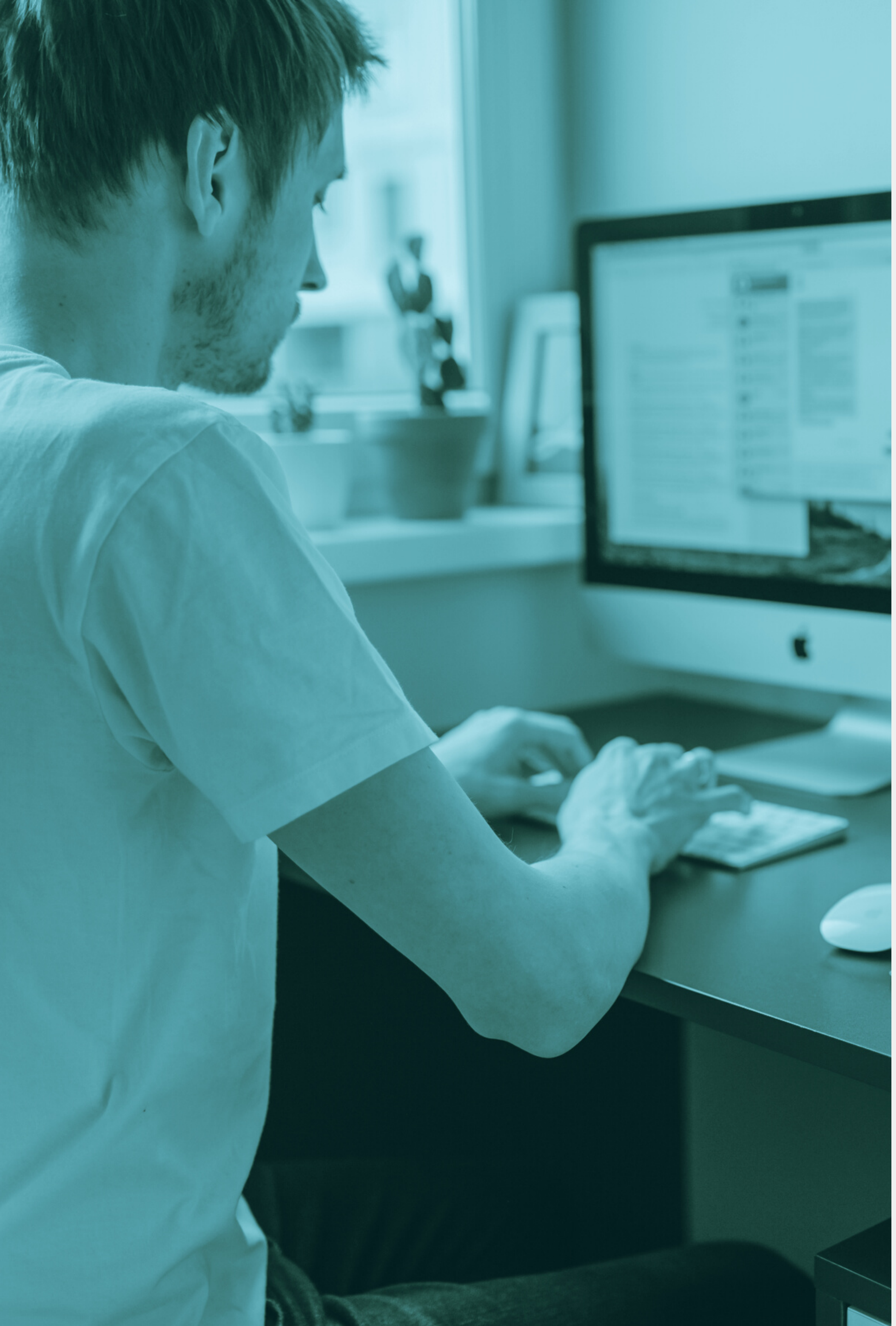
Trend Micro acquired Third Brigade and the OSSEC project, with promises to keep it open source and free.

## In 2018

Trend released the domain name and source code to the OSSEC Foundation.

## Nowadays

The OSSEC project maintained by Atomicorp who stewards the free and open source version and also offers an enhanced commercial version.



# How OSSEC Works?

-TREE MODES;

Local, client, server

-CLIENT SERVER MODEL;

Clients receive configuration from server,Clients send logs to server over an encrypted channel.

# OSSEC FEATURES

## FILE INTEGRITY CHECKİNG

The goal of file integrity checking is to detect the changes in your system and alert you when they happen.

## LOG MONITORING

OSSEC collects, analyzes and correlates these logs to let you know if something suspicious is happening such as attack, misuse, errors, etc.

## ROOTKIT DETECTION

Criminal hackers want to hide their actions, but using rootkit detection you can be notified when the system is modified in a way common to rootkits.

# Key Benefits

## Multi platform

OSSEC lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms

## Real-time and Configurable Alerts

Briefly elaborate on what you want to discuss.

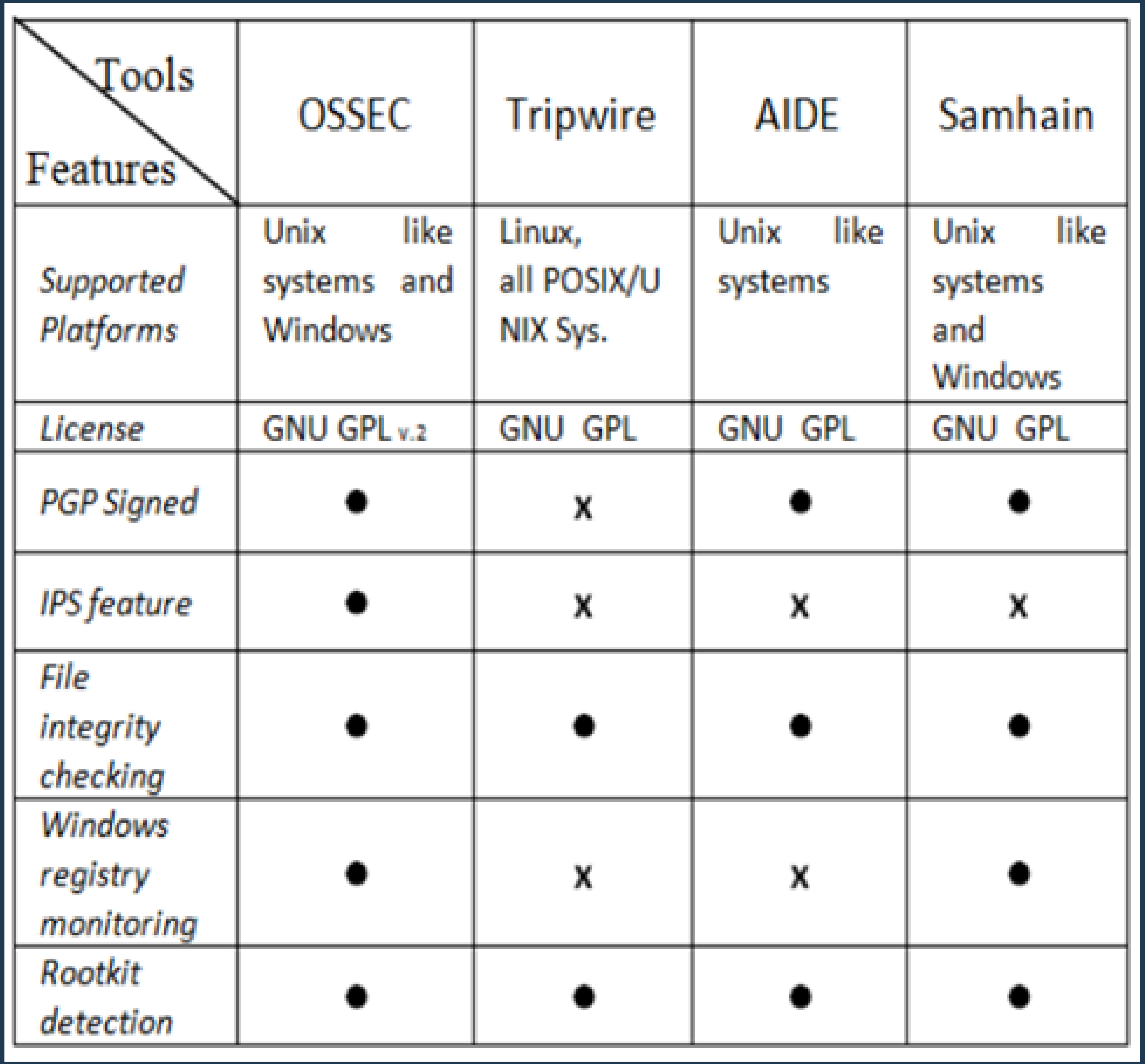
## Compliance Requirements

OSSEC helps customers meet specific compliance requirements such as PCI and HIPAA.

## Centralized management

OSSEC provides a simplified centralized management server to manage policies across multiple operating systems.

# COMPARISON OF OPEN SOURCE HIDS TOOLS



| Tools<br>Features | OSSEC | Tripwire | AIDE | Samhain |
|---|---|---|---|---|
| *Supported Platforms* | Unix like systems and Windows | Linux, all POSIX/UNIX Sys. | Unix like systems | Unix like systems and Windows |
| *License* | GNU GPL v.2 | GNU GPL | GNU GPL | GNU GPL |
| *PGP Signed* | ● | x | ● | ● |
| *IPS feature* | ● | x | x | x |
| *File integrity checking* | ● | ● | ● | ● |
| *Windows registry monitoring* | ● | x | x | ● |
| *Rootkit detection* | ● | ● | ● | ● |

# How to Install OSSEC

## INSTALLATION TYPES OF OSSEC

-Local

-Server

-Agent and Agen-less

# Thank You for Your Attention