

**Домашнее задание № 23**

***Event Management***

***SIEM, ELK, syslog, auditd, Zabbix, Splunk***

* **делаем предыдущие ДЗ!**

**1. Изучаем на лабораторных стендах Splunk SIEM**

* [Лабораторная практика с SIEM системами](https://cyberdefenders.org/)

**2. Установка EFK стэка с помощью docker-compose**

* [Установка EFK](https://docs.fluentd.org/container-deployment/docker-compose)

**\*3. Установка SIEM Wazuh с помощью docker-compose**

* [Установка Wazuh docker-compose](https://documentation.wazuh.com/current/deployment-options/docker/docker-installation.html)

Ссылки на дополнительные ресурсы

* [Сравнение SIEM систем](https://www.anti-malware.ru/compare/SIEM-systems)
* [Работа auditd linux](https://www.redhat.com/sysadmin/configure-linux-auditing-auditd)
* [Лабораторная практика с SIEM системами](https://cyberdefenders.org/)
* [Pozitive портал обучения](https://lms.edu.ptsecurity.com/)