kaspersky

Средний уровень

Мониторинг ИБ и поиск угроз

Познакомьтесь с современными тактиками, техниками и процедурами атак и узнайте, как SOC помогает справиться с ними

Благодаря этому тренингу вы сможете:

- Понимать структуру операционного центра безопасности (SOC) как части услуг по защите безопасности
- Использовать различные источники информации об угрозах для поиска новых современных угроз
- Изучить инфраструктуру поиска угроз на основе ELK (Elasticsearch, Logstash, Kibana).
- Уметь планировать и организовывать мониторинг безопасности в своей организации/компании
- Обнаруживать и исследовать вредоносную активность в инфраструктурах Windows и Linux на основе тактики, техники и процедур злоумышленника

Язык курса - Английский

Требования

- Базовые знания и общий опыт работы с ОС Windows, знакомство с командами ОС Linux.
- Базовые знания о сетевом домене (архитектура, протоколы, атаки).
- Базовые знания о методах атак.

Для кого

Организации, которые стремятся повысить квалификацию своих команд:

- SOC-центры
- Группы реагирования на инциденты
- Группы исследования угроз

Отдельные эксперты, которые хотят расширить свои компетенции в ИБ:

- Специалисты по реагированию на инциденты
- SOC-аналитики
- Исследователи киберугроз

Эксперты

Роман Назаров

Руководитель SOC Консалтинг “Лаборатории Касперского”

Дмитрий Учакин

Исследователь безопасности

Сергей Солдатов

Руководитель Центра мониторинга кибербезопасности “Лаборатории Касперского”

Программа курса

1 Introduction to SOC

- General Cybersecurity Concepts: the nature of targeted attacks and SOC's role in responding to them
- SOC people: structure of and roles in the SOC team
- SOC service model
- SOC use cases and playbooks
- SOC process tree
- Security monitoring and incident handling
- Threat intelligence and threat hunting
- TTP hunting
- WMI consumer hunting
- Linux service hunting
- Domain anomaly hunting

2 Windows environment threat hunting

- Windows OS main cybersecurity features
- Processes, places and sensitive information storage
- Kerberos attacks and exploitation
- Windows active directory audit management
- Preventing account manipulation, privilege escalation and lateral movement
- Mapping offensive activities onto logs
- Searching for the actions of adversaries from the logs
- Matching attacking techniques with the MITRE ATT&CK matrix
- Using Windows audit for investigations

3 Linux security, attack vectors and hunting

- Linux general info: distros, package management, important features, etc.
- Linux security components
- Linux monitoring
- Linux capabilities and auditing system
- System tool privilege abuse hunting and investigation (openssl)
- Auditd telemetry for hunting and investigation
- Sudo misconfiguration abuse hunting and investigation

4 Network threat hunting

- Basics of network technologies
- Common approaches to the network security
- Network security monitoring
- Specialized network devices
- Investigation spoofing and replying attacks
- Investigation server-side attacks

Связаться с нами:

support@kaspersky.happydesk.ru