

Полезные ссылки по ИБ

Регуляторы

- Нормативные акты в РФ по отраслям и меры защиты: <https://regulhub.kaspersky.ru/>

KUMA

- Онлайн-справка по KUMA: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/217694.htm>
- Группа в Telegram: <https://t.me/kumasiem>
- База знаний: <https://kb.kuma-community.ru/>
- Коллекция API на Postman: <https://www.postman.com/kl-ru-presales/workspace/kaspersky-products-apis-ru/overview>

Windows

- Рекомендации по аудиту событий Windows: <https://github.com/JSCU-NL/logging-essentials>
- Рекомендации от Kaspersky MDR: <https://support.kaspersky.com/MDR/ru-RU/204200.htm>
- Скрипты для **быстрой настройки политики аудита по рекомендациям MDR**: <https://box.kaspersky.com/d/48e696a683c04340926e/>
- **✓ Рекомендуется** ID событий отправляемые в MS Sentinel: <https://learn.microsoft.com/en-us/azure/sentinel/windows-security-event-id-reference>
(Строка с Common)
 - **✓ Рекомендуется** Дополнительные полезные ID событий (пресейл рекомендация дополнение к MS Sentinel): <https://box.kaspersky.com/f/8c71107f71054d3981c3/>
- Рекомендации от ManageEngine: <https://www.manageengine.com/products/active-directory-audit/guide-to-configure-group-policy-object-auditing-in-adauditplus.html>
- Рекомендации от MS:
 - <https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>
 - <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

- Что наиболее интересно собирать с Windows — <https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding>
- Рекомендации сбору событий с Sysmon, конфигурация:
<https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml>

Linux

- Описание Audit системы: <https://access.redhat.com/articles/4409591>
- **✓Рекомендуется** Конфиг для AuditD (Florian Roth): <https://github.com/Neo23x0/auditd>
 - **✓Рекомендуется** улучшение конфига на странице настройки AuditD:
<https://kb.kuma-community.ru/books/podkliucenie-istocnikov/page/nastroika-auditd-na-unix-sistemax>
- Конфиг для AuditD (с маппингом MITRE): <https://github.com/bfuzzy1/auditd-attack/tree/master/auditd-attack>
- Конфиг для TrendMicro DS: <https://github.com/deep-security/auditd-config/>
- AuditD на GoLang: <https://slack.engineering/syscall-auditing-at-scale/>
- Конфиги для AuditD (по различным стандартам): <https://github.com/linux-audit/audit-userspace/tree/master/rules>
- Агрегация событий AuditD по ID: <https://github.com/simple-evcorr/sec> ,
<https://docs.nxlog.co/refman/current/pm/evcorr.html>

Cisco

- Настройка Netflow:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

Примеры событий различных систем

- <https://github.com/elastic/beats/tree/master/x-pack/filebeat/module>
- <https://docs.trellix.com/bundle/enterprise-security-manager-data-sources-configuration-reference-guide/page/GUID-49F19CE4-38BC-4322-B0C1-E1CF3AB277CB.html>
- <https://docs.cyderes.cloud/parser-knowledge-base>
- <https://github.com/izysec/linux-audit/tree/main/LogSamples>

Прочее

- Написание регулярных выражений: <https://regex101.com/>

Revision #20

Created 10 August 2023 08:10:16 by Koala

Updated 30 September 2024 12:48:23 by Boris RZR