Вооруженные Силы Республики Беларусь

ОБЛИК СИСТЕМЫ СБОРА И ОБРАБОТКИ ДАННЫХ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЫЯВЛЕНИИ КИБЕРАТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

начальник отдела
Бабич Максим Александрович

2022 г.

Перечень основных задач, решаемы с помощью SIEM-системы

- накопление и оперативная обработка данных о событиях информационной безопасности;
- выявление и расследование инцидентов информационной безопасности;
- инвентаризация активов и ресурсов информационной системы;
- контроль защищенности информационных ресурсов;
- мониторинг работы системы в условиях реальной ИТ-инфраструктуры;
- контроль и создание отчетов (диаграмм) о состоянии защищенности информационных ресурсов.

Перечень основных источников событий информационной безопасности в SIEM-системе

- средства антивирусной защиты;
- средства криптографической защиты;
- серверные операционные системы;
- активное коммутационное оборудование;
- системы идентификации и аутентификации пользователей;
- системы хранения и передачи файлов;
- системы виртуализации;
- системы обнаружения и предотвращения вторжений;
- системы обнаружения и предотвращения утечек информации;
- отдельные автоматизированные рабочие места пользователей.

Источники события	Категория события	Тип события
Прокси-серверы с контролем контента Средства защиты веб-трафика Средства защиты почты Средства защиты конечных узлов со встроенными модулями контроля веб-ресурсов и электронной почты Антивирусные средства защиты Средства обнаружения и предотвращения вторжений	Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый информационный ресурс модулей ВПО (malware infection)
	Распространение вредоносного программного обеспечения (malware distribution)	Использование контролируемого информационного ресурса для распространения ВПО (malware command and control)
		Попытки внедрения модулей ВПО в контролируемый информационный ресурс (infection attempt)
Межсетевые экраны Системы обнаружения и предотвращения вторжений Системы выявления и блокировки сетевых DoS-атак	Нарушение или замедление работы контролируемого информационного ресурса (availability)	Компьютерная атака типа “отказ в обслуживании”, направленная на контролируемый информационный ресурс (dos)
		Распределенная компьютерная атака типа “отказ в обслуживании”, направленная на контролируемый информационный ресурс (ddos)
		Несанкционированный вывод информационный ресурс из строя (sabotage)
		Непреднамеренное (без злого умысла) отключение информационный ресурс (outage)
Системы предотвращения утечек данных из информационной системы	Нарушение безопасности информации (information content security)	Несанкционированное разглашение информации, обрабатываемой в контролируемом информационном ресурсе (unauthorised access)
		Несанкционированное изменение информации, обрабатываемой в контролируемом информационном ресурсе (unauthorised modification)

Таблица 1 – Общая классификация событий информационной безопасности

Источники события	Категория события	Тип события
Средства защиты конечных узлов Сканеры уязвимостей Средства обнаружения и предотвращения вторжений	Несанкционированный доступ в систему (intrusion)	Успешная эксплуатация уязвимости в контролируемом информационном ресурсе (application compromise)
		Компрометация учетной записи в контролируемом информационном ресурсе (account compromise)
Межсетевые экраны Средства обнаружения и предотвращения вторжений Средства защиты конечных узлов	Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	Попытки эксплуатации уязвимости в контролируемом информационном ресурсе (exploit attempt)
		Попытки авторизации в контролируемом информационном ресурсе (login attempt)
Средства обнаружения и предотвращения вторжений Сканеры уязвимостей и средства аудита Антивирусные средства защиты	Сбор сведений о контролируемой системе (information gathering)	Сканирование информационного ресурса (scanning)
		Прослушивание (захват) сетевого трафика контролируемого информационного ресурса (traffic hijacking)
		Социальная инженерия, направленная на компрометацию информационного ресурса (social engineering)
Сканеры уязвимостей и средства аудита	Уязвимость (vulnerability)	Наличие уязвимости или недостатков конфигурации в информационном ресурсе (vulnerability)

Таблица 1 – Общая классификация событий информационной безопасности

Вооруженные Силы Республики Беларусь

ОБЛИК СИСТЕМЫ СБОРА И ОБРАБОТКИ ДАННЫХ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЫЯВЛЕНИИ КИБЕРАТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

начальник отдела
Бабич Максим Александрович

2022 г.