|  |  |
| --- | --- |
|  | **Отчет мониторинга событий информационной безопасности** |
|  | |  |  | | --- | --- | | {предпр} | {Месяц} {год} | |

# Основные результаты мониторинга

В результате мониторинга событий информационной безопасности  
и управления уязвимостями (далее – SOC-центр) подключены следующие источники событий информационной безопасности инфраструктуры предприятия (далее – источники):

* Журналы событий безопасности операционной системы **Windows**  
  на конечных узлах (автоматизированных рабочих местах и серверах);
* центр управления антивирусной защиты **Kaspersky Security Center**;
* журналы событий межсетевого экрана **UserGate;**
* журналы событий активного сетевого оборудования.

В период {период} на подключенных источниках зафиксировано:

* **{число}** событий информационной безопасности;
* **{алертов}** алертов;
* **{типы}** типов алертов.

Рисунок 1 – Категорирование инцидентов по типам\*

\* Сводное описание типов, согласно классификации MITRE ATT&CK:

|  |
| --- |
| Разведка (Reconnaissance, TA0043) - попытки сбора информации |
| которая может быть использована для атак; |
| Подготовка ресурсов (Resource Development, TA0042) - попытки получения |
| злоумышленником ресурсов, с которых может быть проведена атака; |
| Первоначальный доступ (Initial Access, TA0001) - попытки проникновения в сеть; |
| Выполнение (Execution, TA0002) - попытки запуска вредоносного кода; |
| Закрепление (Persistence, TA0003) - попытки злоумышленника сохранить присутствие |
| в системе; |
| Повышение привилегий (Privilege Escalation, TA0004) - попытки злоумышленника |
| получить права более высокого уровня |
| Предотвращение обнаружения (Defence Evasion, TA0005) - методы, позволяющие |
| злоумышленнику избежать обнаружения в скомпрометированной системе; |
| Получение учетных данных (Credential Access, TA0006) - методы получения легитимных |
| учетных данных, либо их кражи с целью получения доступа к системам; |
| Обнаружение (Discovery, TA0007) - методы для получения сведений о системе или сети; |
| Перемещение (Lateral Movement, TA0008) - методы, используемые для входа и управления |
| удаленными системами, расположенными в сети предприятия; |
| Сбор данных (Collection, TA0009) - методы сбора информации, интересующей |
| злоумышленника; |
| Организация управления (Command and Control, TA0011) - методы установления контроля |
| и управление атакуемыми системами; |
| Эксфильтрация (Exfiltration, TA0010) - методы кражи данных; |
| Деструктивноое воздействие (Impact, TA0040) - методы, используемые для нарушения |
| доступности или целостности данных |

В рамках **{алертов}** алертов затронуто {ист} источников.

Таблица 1. Имена затронутых источников

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя** | **№** | **Имя** | **№** | **Имя** | **№** | **Имя** |
| 1 | SERVER-OB |  |  |  |  |  |  |
| 2 | CEH-35-11 |  |  |  |  |  |  |
| 3 | CEH-8-ATS2 |  |  |  |  |  |  |
| 4 | CEH-8-LAB |  |  |  |  |  |  |
| 5 | CEH29-ZN |  |  |  |  |  |  |
| 6 | KTOIR-5-28 |  |  |  |  |  |  |
| 7 | KTOIR-5-8 |  |  |  |  |  |  |
| 8 | OASU-101-7N |  |  |  |  |  |  |
| 9 | OASUP-DVK2 |  |  |  |  |  |  |
| 10 | OGE-10 |  |  |  |  |  |  |
| 11 | OGM-3 |  |  |  |  |  |  |
| 12 | OKITO-7 |  |  |  |  |  |  |
| 13 | OMTO-8 |  |  |  |  |  |  |
| 14 | OMTO-9 |  |  |  |  |  |  |
| 15 | SEKRETAR-GD |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |
| 18 |  |  |  |  |  |  |  |
| 19 |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |  |
| 21 |  |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |  |
| 26 |  |  |  |  |  |  |  |
| 27 |  |  |  |  |  |  |  |
| 28 |  |  |  |  |  |  |  |
| 29 |  |  |  |  |  |  |  |
| 30 |  |  |  |  |  |  |  |
| 31 |  |  |  |  |  |  |  |
| 32 |  |  |  |  |  |  |  |
| 33 |  |  |  |  |  |  |  |
| 34 |  |  |  |  |  |  |  |
| 35 |  |  |  |  |  |  |  |

# Тактики и техники MITRE ATT&CK

Таблица 2. Тактики и техники

| **Тактика** | **Техника** |
| --- | --- |
| Организация управления | R204\_Использование внешнего DNS сервера |
| Выполнение | R080\_Всплеск заражений ВПО |
| Выполнение | R262\_Подозрительный доступ к процессу LSASS |
| Выполнение | R079\_Несколько хостов заражены одним типом вируса |
| Организация управления | R205\_Обнаружен новый DNS сервер |

Подробная информация по событиями и инцидентам, собранная  
за отчетную и предыдущие даты, представлена в соответствующем разделе  
вашего Личного кабинета «Отчеты\Сформированные отчеты».