**Questions & Answers:**

1. **You have security log from Firewall between DMZ and the Internet. How will you use this log for threat detection?**

А) Выяснить, какая активность считается нормальной для системы: какие протоколы, порты и ресурсы должны быть доступны, а также определить характерную нагрузку в зависимости от времени суток, дня недели, и региональной активности.

Б) Организовать автоматизированный сбор, нормализацию и корреляцию логов для упрощения и ускорения анализа.

В) Настроить уведомления и блокировку подозрительной активности на основе анализа логов.

1. **You are SOC analyst and you have got an alert from IDS system about SQL-injection on web server. What will you do? How will you investigate (technical aspects)?**

**А) Проверить оповещение, изучив логи IDS и веб-сервера. При подтверждении угрозы — немедленно заблокировать атакующий IP-адрес.**

**Б) Анализировать логи на предмет повторяющихся запросов, содержащих специальные символы, и ошибок базы данных.**

**В) Определить цель атаки, проанализировав содержимое инъекции, проверить базу данных на изменения.**

**Г) Изучить логи ОС для выявления глубины проникновения. Проверить попытки сетевого сканирования или подключения с атакованной машины.**

**Д) Изолировать активы, подвергшиеся компрометации, сменить пароли скомпрометированных учетных записей, предотвратить дальнейшее распространение атаки.**

**Е) Восстановить систему из резервной копии, устранить уязвимости, ограничить права доступа пользователей и внедрить защитные меры против повторных инъекций.**

**З) Провести постинцидентный анализ и разработать рекомендации для предотвращения подобных инцидентов в будущем.**

1. **The most frequent Windows compromise scenarios relate to password hash dump tools usage. Propose detection scenarios (the more the better) of hash dump tools usage.** **How further illegal usage of stolen credentials can be detected?**

**А) Анализировать логи аутентификации: отслеживать неудачные попытки входа, горизонтальное перемещение, повышение привилегий, доступ к конфиденциальной информации.**

**Б) Использовать инструменты EDR, XDR и threat intelligence для поведенческого анализа.**

**4. You work in a company that has two offices (Moscow and Perm) and you have logs from VPN gateway, FW,** **physical Access Control System. Suggest scenarios for detection possibly threats.**

**VPN**

* Аномальные подключения (вне рабочего времени, многократные ошибки авторизации).
* Несоответствующие геолокации.
* Одновременные подключения с разных устройств.

**Firewall**

* Частые блокировки или попытки доступа к конфиденциальным данным.
* Нестандартные протоколы, порты, домены.
* Аномальный исходящий трафик.

**СКУД**

* Проход вне рабочего времени, множественные ошибки входа.
* Использование одного пропуска в разных местах здания в короткий срок.
* Попытки получить доступ к запрещенным зонам.

**5. If you have antivirus logs, what correlation rules (detection scenarios) can you suggest?**

А) Определить тип угрозы и площадь атаки.

Б) Анализировать поведение пользователя после обнаружения угрозы.

В) Изучить сетевую активность, связанную с угрозой.

Г) Проверить логи аутентификации..

**6. You’ve received alert from the corporate proxy that one workstation has connected to the “Malicious site”:**

* 1. **What immediate actions would you take to contain the spread?**

**А)** Если инцидент произошел в нерабочее время, необходимо оперативно отключить систему от корпоративной сети. В рабочее время следует сначала связаться с администратором или пользователем, ответственным за эту систему, уточнить информацию о выявленной активности и, если потребуется, изолировать систему.

**Б)** Изучите логи и проанализируйте действия, выполненные пользователем на устройстве, чтобы выявить возможные причины инцидента.

**В)** Проверьте систему с помощью антивирусного ПО или специализированных инструментов для обнаружения вредоносных программ.

**Г)** Обеспечьте безопасность, сменив учетные данные пользователя, от имени которого был осуществлен запрос на вредоносный ресурс, либо заблокируйте учетную запись, чтобы предотвратить дальнейший доступ.

* 1. **In which system you can try to get additional information?**

А) EDR/XDR/Антивирус

Б) SIEM

В) IPS/IDS

Г) Threat Intelligence Platforms

Д) Firewall

* 1. **Which stage of the “kill chain” attack this case is?**

А) Вероятнее всего это стадия доставки (delivery) ВПО, однако запросы на вредоносные домены может происходить и на стадии команды и контроля (command and control).

7. **What system is the following log from and what could you tell about it?**

**А)** Это, вероятно, лог DNS-сервера. UDP-пакеты отправляются на несуществующие домены, что может указывать на вредоносную активность или некорректную настройку.

**8. What is happening according to the following events?**

А) Пользователь kheirkhabarov (предположительно администратор системы) через консоль запустил с повышенными привилегиями утилиту procdump64.exe, которая расположена на его рабочем столе. Цель запуска — создание дампа процесса lsass.exe. LSASS отвечает за политику безопасности, хранение данных пользователей и управление паролями.

9. **What does this message mean? Is this suspicious? Why?**

А) На удаленной системе с помощью PsExec была выполнена команда, что подтверждает создание службы PSEXECSVC. Поскольку это произошло в 1:05 ночи, такое событие вызывает подозрение и требует анализа.

10. **What can you tell about logs below?**

А) Скрипт загружает файл misa2.bin, сохраняет его под случайным именем и запускает.  
Б) Через PowerShell скрытно выполняется код для чтения данных из реестра, их преобразования и декодирования из Base64.  
В)Загружается и запускается файл encrypted.exe.  
Все действия связаны с сокрытием загрузки и запуска вредоносного ПО через PowerShell.

1. **What can you tell about this script?**

А) Скрипт проверяет версию PowerShell (3.0 и выше), отключает журналирование, выключает антивирусное сканирование, подключается к удаленному сайту, загружает данные, расшифровывает их и выполняет как PowerShell-скрипт.

**12. What event id does registry modification has? What event id does service install and Service Failure has?**

А) Изменения в реестре фиксируются под ID 4657. Установка службы — ID 7045. Ошибки служб — ID 7031–7034.

**13.Why files with «chm» extension can be dangerous?**

А) Файлы .chm (HTML Help) могут содержать вредоносные скрипты, использоваться для выполнения кода через уязвимости или в атаках социальной инженерии. Их формат снижает подозрения, что делает их эффективным инструментом для фишинга.

1. **You have logs from DNS server, and you see lot of AXFR requests from one external IP. Is it malicious? If so, why?**

А) Большое количество AXFR-запросов с внешнего IP указывает на возможную разведывательную активность злоумышленников, готовящих атаку на инфраструктуру.

1. **How can you detect Golden Ticket attack?**

**А)** Используйте SIEM и XDR для выявления подозрительного поведения. Например, следите за действиями учетных записей с административными привилегиями, которые получают доступ к ресурсам, обычно им недоступным.  
**Б)** Анализируйте события 4769 и 4768, чтобы определить аномалии в запросах TGS.  
**В)** Обратите внимание на доступ к чувствительным ресурсам или системам, особенно если он осуществляется впервые или вне рабочего времени.  
**Г)** Ищите признаки эскалации привилегий и анализируйте действия учетных записей

**16. Imagine that attacker compromises your domain controller. Propose a remediation scenario for this situation.**

**А)** Изолируйте систему и оцените масштабы компрометации, анализируя логи и определяя затронутые учетные записи.  
**Б)** Выполните сброс и замену учетных данных, перевыпустите сертификаты и отключите скомпрометированные учетные записи.  
**В)** Восстановите контроллер домена из резервной копии. Если есть подозрение на компрометацию **backup\_secret\_key**, выполните полное восстановление с новой настройкой.  
**Г)** Пересмотрите политики безопасности, усилите их и проведите аудит выданных привилегий.  
**Д)** Установите мониторинг активности после восстановления. Проведите анализ атаки и создайте рекомендации для предотвращения подобных инцидентов.

1. **What is the best PowerShell 5 feature for security team?**
2. **А)** Лучшая функция — **Script Block Logging**, которая позволяет регистрировать команды и скрипты, выполняемые в системе. Это полезно для анализа атак и выявления вредоносной активности.

**18. You have got an alert from EDR solution and you have only this information:**

**Process: flashhelperservice.exe**

**PID: 6508**

**OS Type: windows**

**MD5: 59c34bc243eb2604533b5f08d30944f8**

**SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c**

**What can you tell about this case?**

Файл FlashHelperService.exe был проанализирован с использованием антивирусных решений по хэшу , и **25 из 72 вендоров безопасности** классифицировали его как вредоносный. Анализ показывает, что файл связан с категорией угроз **adware (рекламное ПО)** и **trojan (троянское ПО)**, а также относится к семейству **flashserv**..

1. **During the investigation you see this information: **

Данная строка представляет собой закодированный PowerShell-скрипт. Он:

1. Декодирует данные в UTF-8.
2. Отбрасывает пустые строки и разделяет входные данные на две части.
3. Первая часть содержит PowerShell-код, который выполняется.
4. Вторая часть, вероятно, содержит полезную нагрузку в формате JSON.
5. **You have observed an alert from EDR solution and have this info:**

**c:\windows\system32\services.exe is launched by explorer.exe is it ok? If it is not what reason of it could be?**

1. Это подозрительно, поскольку в нормальных условиях services.exe запускается через wininit.exe. Такое поведение может свидетельствовать о наличии вредоносного ПО.
2. **You have installed an application on your PC and the application cannot connect to the Internet. There are no antivirus warnings and you can browse the Internet. What is the most likely cause of the problem?**

Возможные причины:

1. IP-адрес вашего устройства или диапазон заблокирован на сервере.
2. Файрвол блокирует сетевой трафик.
3. Приложению не хватает прав доступа.
4. Приложение повреждено и не может подключиться к сети.
5. **What can you say about this URL “www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”?**

Это доменное имя похоже на случайно сгенерированное. С высокой вероятностью оно используется для фишинговых атак, разведки или распространения вредоносного ПО.

**23.What can you say about this nmap scan report? Are there any security issues in this report?**

На сервере установлены OpenSSH версии 7.2p2 и Apache 1.1. Операционная система — Ubuntu (16.04 или новее). Порт 80 защищен файерволом. Для подключения по SSH применяются криптографические ключи, при этом длина RSA-ключей должна быть достаточной для обеспечения надежной защиты.

OpenSSH версии 7.2p2 подвержен уязвимостям, включая **CVE-2016-6210** (перебор имен пользователей) и **CVE-2023-38408**.  
Apache Struts содержит уязвимость **CVE-2011-1772** (XSS-атака).

1. **Восстановите пароль из хеша fmarket.stf\admin:1337:aad3b435b51404eeaad3b435b51404ee:bebaecb23aa18f5375628541ff3fb3b8:::**

bebaecb23aa18f5375628541ff3fb3b8 is password a6\_123