ANGARA
SOC

COMPROMISE ASSESSMENT
И ГОТОВНОСТЬ К РЕАГИРОВАНИЮ
НА ИНЦИДЕНТЫ

ANGARA
SOC

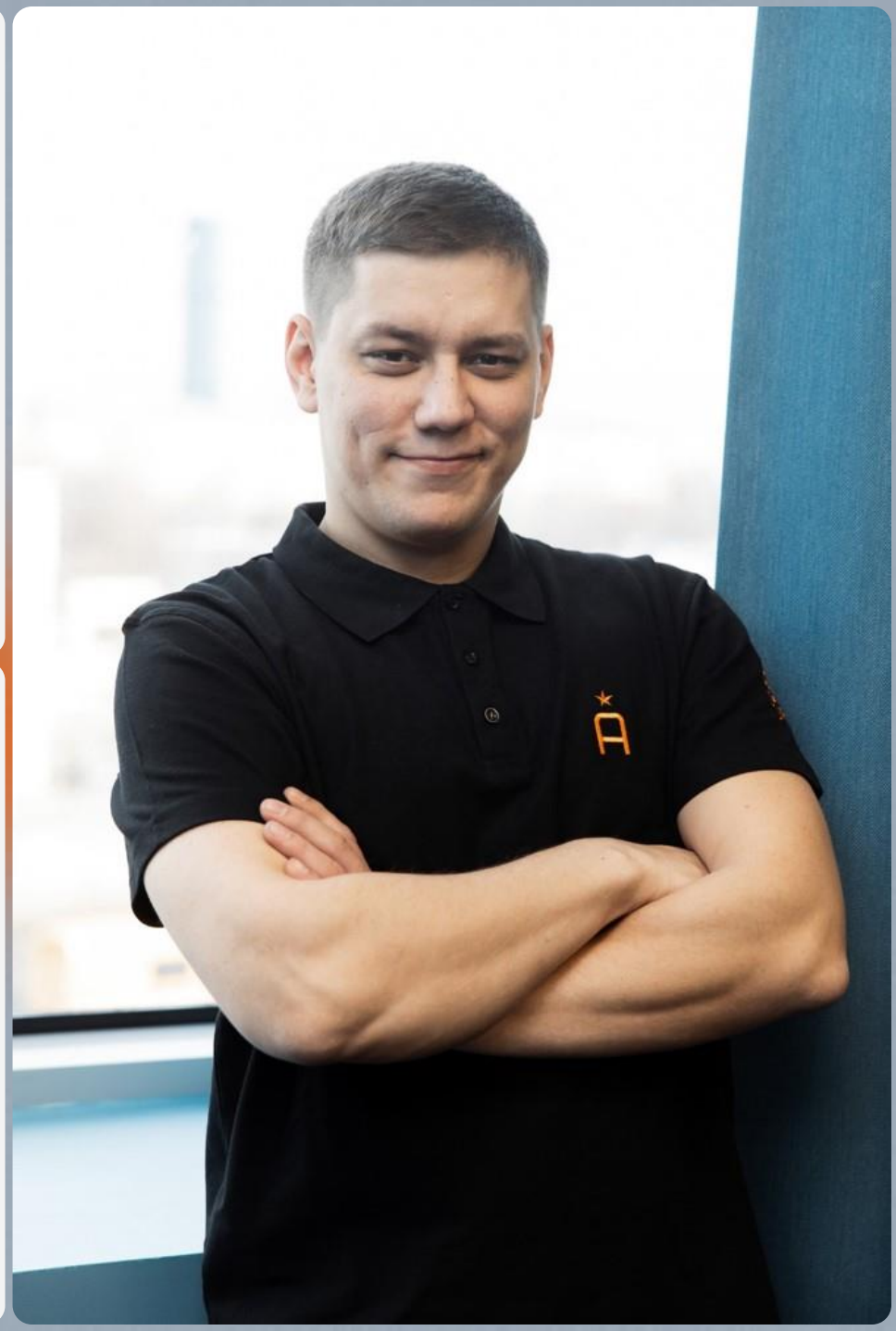
Никита Леокумович

Начальник Управления цифровой
криминалистики и киберразведки

n.leokumovich@angarasecurity.ru

+7 (914) 441-77-76

@LeokumovichN



В КАКОМ СЛУЧАЕ НУЖНО ПРОВОДИТЬ COMPROMISE ASSESSMENT

1

При поглощении другой компании и ее инфраструктуры

2

Есть подозрение, что компания могла быть атакована (например, была выявлена утечка учетных данных сотрудников)

3

Профилактика

КАК ЭТО ПРОИСХОДИТ

Гипотезы

2.4. Атакующие использовали службу управления контейнерами для выполнения команд (например, `docker exec -ti [redacted] bash`).

3. Атакующие использовали следующие **техники для закрепления**:

3.1. Атакующие модифицировали ключи реестра Run и использовали папку автозапуска.

3.2. Атакующие изменяли ключ реестра Environment пользовательского куста реестра NTUSER.dat.

ANGARA SOC

Ландшафт в виде тепловой карты

Initial Access	**T1566.001** Phishing: Spearphishing Attachment	**T1133** External Remote Services	**T1189** Drive-by Compromise	**T1190** Exploit Public-Facing Application	**T1195.002** Compromise Software Supply Chain	**T1566.002** Phishing: Spearphishing Link	
	T1566.003 Phishing: Spearphishing via Service	**T1078.002** Valid Accounts: Domain Accounts	**T1078.003** Valid Accounts: Local Accounts	**T1195** Supply Chain Compromise	**T1199** Trusted Relationship	**T1091** Replication through Removable Media	
Execution	**T1047** Windows Management Instrumentation	**T1059.001** Command and Scripting Interpreter: PowerShell	**T1204.002** Malicious File	**T1053.005** Scheduled Task	**T1059.003** Command and Scripting Interpreter: Windows Command Shell	**T1106** Native API	**T1059.0** Comman Scripting Unix She
	T1204.001 Malicious Link	**T1569.002** Service Execution	**T1059.005** Command and Scripting Interpreter: Visual Basic	**T1059.006** Command and Scripting Interpreter: Python	**T1059.007** Command and Scripting Interpreter: JavaScript	**T1204** User Execution	**T1053.0** At
Persistence	**T1547.001** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	**T1053.005** Scheduled Task/Job: Scheduled Task	**T1133** External Remote Services	**T1546.012** Event Triggered Execution: Image File Execution Options Injection	**T1574.002** Hijack Execution Flow: DLL Side-Loading	**T1574.013** Hijack Execution Flow: KernelCallbackTable	**T1037.0** Boot or L Initializati Logon Sc (Windows
	T1078.003	**T1098**	**T1136.001**	**T1197**	**T1505.003**	**T1542.001**	**T1542.0**

КАК ЭТО ПРОИСХОДИТ

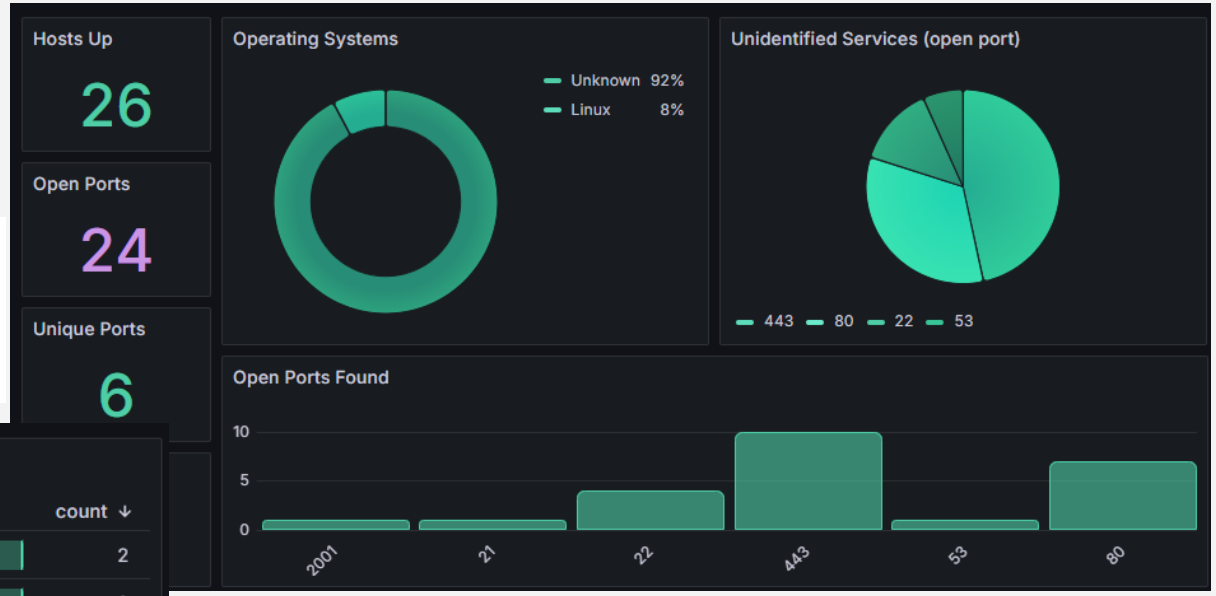
Внешнее сканирование

Таблица 1. Обнаруженные подсети для публикации ресурсов компании

Диапазон	Имя сети	ASN*	Организация	Владелец

Таблица 2. Опубликованные ресурсы в разрезе доменных имен

Домен	IP адрес	Тип DNS-записи	Имя хоста



КАК ЭТО ПРОИСХОДИТ

Внутреннее сканирование

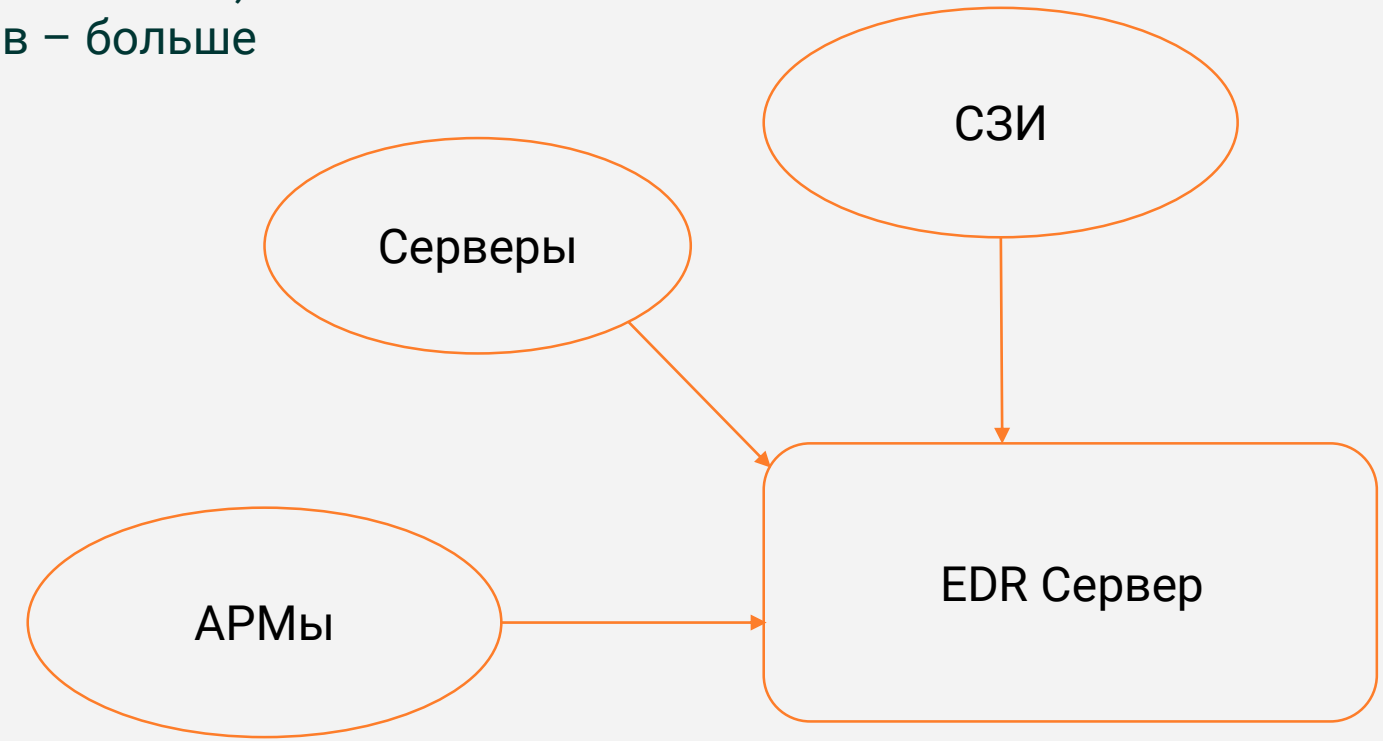
Определяем критичные активы, СЗИ, периметровые устройства и т.д.

Таблица 3. Результат внутреннего сканирования сети

Описание	Количество обнаруженных IP-адресов
Общее количество обнаруженных IP-адресов	[redacted]
Рабочие станции с исправно функционирующими EDR-агентами	[redacted]
Рабочие станции без EDR-агентов	[redacted]
VPN-сегмент	[redacted]
Периферийные устройства и сетевое оборудование	[redacted]

СБОР ТЕЛЕМЕТРИИ

После определения активов начинаем собирать
с них данные – триажи разной полноты,
с АРМов поменьше с серверов – больше



АНАЛИЗ СОБРАННЫХ ДАННЫХ

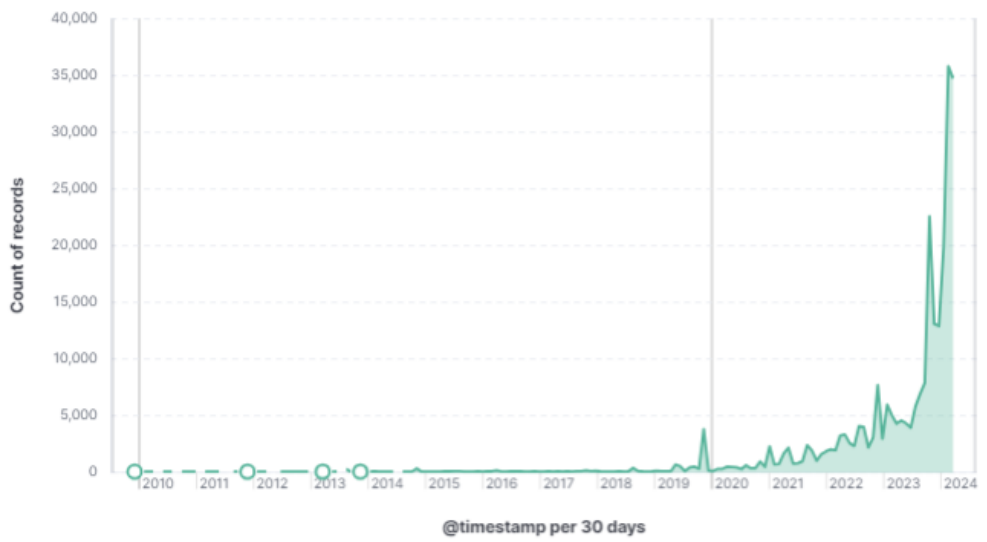
Artifacts

Source	Count
Amcache	122,689
Shimcache	88,610
UserAssist	50,617

TI

TI verdict	Count
Not found	118,603
Found	91

Timeline



ПОИСК ПО ОТКРЫТЫМ ИСТОЧНИКАМ

В рамках работ проводился поиск схожих доменов для предотвращения случаев копирования официального сайта и выдачи мошеннического сайта за сайт Компании, а также для информирования о свободных доменах, которые в дальнейшем могут быть использованы мошенниками.

- Поиск схожих доменных имен

В результате поиска было обнаружено 11 доменов со схожими названиями доменов компании Заказчика:

- программы для удаленного мониторинга и управление (RMM) - **AnyDesk**;
- инструмент **PsExec** из пакета утилит Sysinternals;
- средство **sqldumper**.exe, входит в состав Microsoft SQL Server.
- консольная утилита **nmap**;
- программа **Advanced IP Scanner** с графическим интерфейсом;
- программа **Angry IP Scanner** с графическим интерфейсом.
- **nanodump** от компании-разработчика Cobalt Strike;
- **ADExplorer**, **BloodHound**: утилиты для исследования доменной инфраструктуры Active Directory.

ЧТО ПОЛУЧАЕМ ПО ИТОГАМ CA?

Мы подсвечиваем слабые места в ИБ процессах организации, даем рекомендации по усилению. Если в сети были обнаружены недопустимые события, проводим полноценный IR с полноценным отчетом

РЕКОМЕНДАЦИИ

МЕРЫ ПО ПОВЫШЕНИЮ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФРАСТРУКТУРЫ КОМПАНИИ

В данном разделе приведены меры для повышения уровня защищенности ИТ-инфраструктуры и снижения уровня рисков информационной безопасности в порядке приоритета их выполнения, а также дополнительные комментарии по их реализации.

1. Обеспечить полное покрытие EDR-агентами. Выявленные узлы без установленного EDR-агента указаны в Приложении 1.

2. Обеспечить полное покрытие АВПО. Выявленные узлы без установленного АВПО указаны в Приложении 2.

4. Обеспечить сбор DNS-журналов в SIEM-систему с серверов [redacted].

5. Обеспечить сбор событий из DHCP-журналов, содержащих информацию о выдаваемых IP адресах в SIEM-систему.

ВЫВОДЫ

ОБОБЩЕННЫЕ РЕЗУЛЬТАТЫ И СФОРМИРОВАННЫЕ ВЫВОДЫ О ПРОДЕЛАННОЙ РАБОТЕ И ОБНАРУЖЕННЫХ ДАННЫХ В ХОДЕ COMPROMISE ASSESSMENT

В ходе проведенных работ были достигнуты следующие результаты:

4. Информационная инфраструктура Заказчика проверена на наличие известных индикаторов компрометации, в том числе замеченных в последних атаках на российские организации. В результате проверки **следов компрометации не выявлено.**

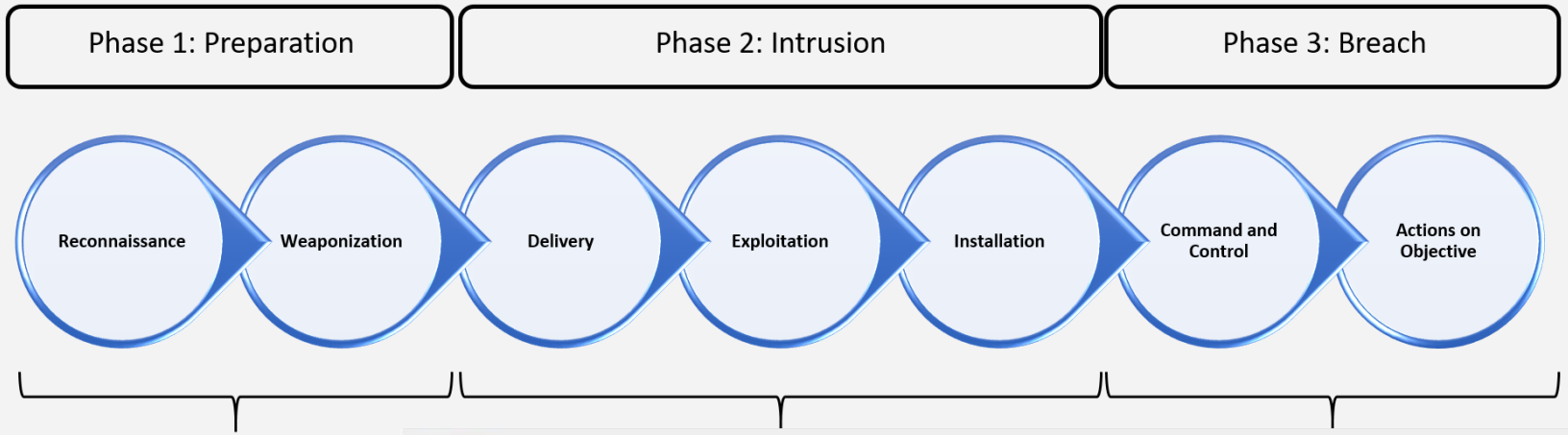
ПРИЛОЖЕНИЕ

ИНДИКАТОРЫ КОМПРОМЕТАЦИИ

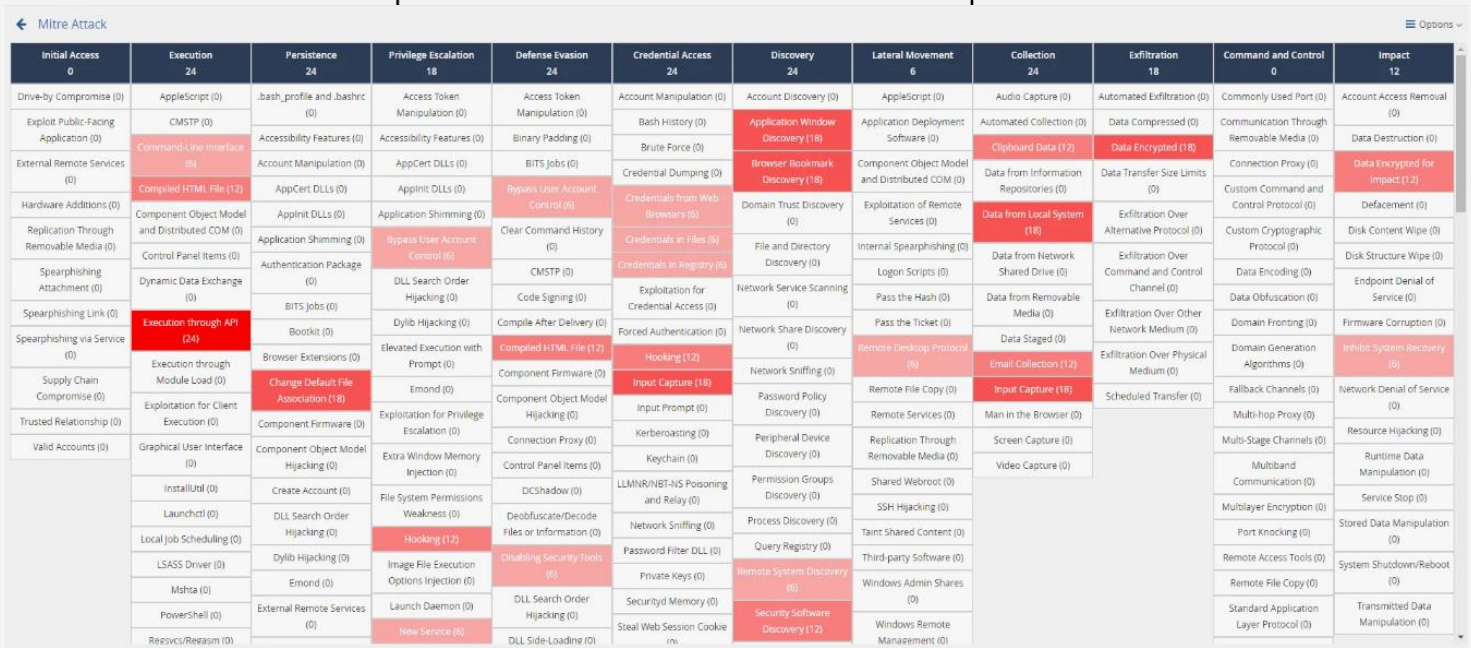
ГОТОВНОСТЬ К РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

Что такое коэффициент киберустойчивости

The Cyber Kill Chain



MITRE ATT&CK®



ЧТО ПРОВЕРЯЕМ?

Активы

Процессы

Документы

Команда

- Процессы управления
- Матрица зарезервированных белых IP и доменных имен
- Процессы оценки поверхности атаки и управление ею
- Карта сети

ОСВЕДОМЛЕННОСТЬ СОТРУДНИКОВ В СФЕРЕ ИБ

- Политика ИБ в отношении персонала
- Документы при найме и увольнении
- Процесс обучения является измеримой величиной, контролируется и/или ведется соответствующая аналитика
- Подход security buddy
- Отдельные процессы

ПРОЦЕССЫ В СИСТЕМЕ УПРАВЛЕНИЯ ИБ

- Расширенный аудит
- Классы используемых решений в сфере ИБ
- Хранение событий
- **Идентификация пользователей**
- Контроль средств RMM
- Сетевая безопасность и политика использования сети Интернет

ГОТОВНОСТЬ ВЫДЕЛЕННОЙ КОМАНДЫ ПО РЕАГИРОВАНИЮ

Проводятся учения в формате практик
по предоставлению отдельных данных,
выполнению отдельных команд

Важным параметром является оперативность
и время предоставляемой информации

ЧТО В ИТОГЕ?

Мы определяем текущий (фактический) уровень готовности к реагированию на инциденты различной степени сложности и даем рекомендации для его повышения

8. Функции структурных подразделений Компании.

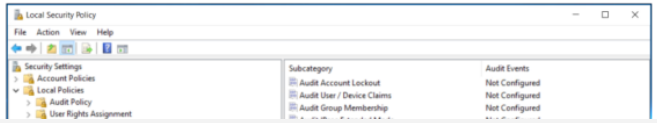
8.1. Управление информационной безопасности:

- планирует мероприятия по защите конфиденциальной информации, организует их выполнение и контроль за их выполнением;
- участвует в разработке и внесении изменений во внутренние документы и процессы Компании, связанные с обработкой и защитой конф информации;
- организует разработку и актуализацию (совместно со подразделениями Компании) Перечня сведений, составляющих конф информацию Компании;
- организует работы по оценке защищенности информационных разрабатывает предложения по повышению эффективности их защиты;

Примечание: настройку в данном пункте инструкции следует выполнять в случае, если пункт 1.1 ранее не был выполнен. В случае если настройка в пункте 1.1. инструкции выполнена, то действия, описанные далее можно пропустить.

Настройка данного события выполняется следующим образом:

1) Открыть редактор политики безопасности;
2) Перейти в меню Advanced Audit Policy Configuration > System Audit Policies > Logon / Logoff;
3) Нажать на элемент интерфейса «Audit logon»;
4) Поставить галочки около элементов интерфейса «Success», «Failure»;
5) Нажать на элемент интерфейса «Audit logoff»;
6) Поставить галочки около элементов интерфейса «Success», «Failure»;
7) Нажать на элемент интерфейса «Ок»;



ANGARA SOC

О проверке готовности к реагированию на инциденты

ФЕВРАЛЬ 2024

ANGARA
SOC

СПАСИБО ЗА ВНИМАНИЕ!

+7 495 269-26-06

www.angarasecurity.ru