K2 кибер безопасность

О дивный новый мир, или Как безболезненно провести настройку расширенного аудита

Кирилл Рупасов
Руководитель группы инженеров SOC

Что входит в состав аудита

01

Расширенный аудит

02

SACL объекты

03

Дополнительные компоненты
(EDR, SYSMON и т.п.)

K2 кибер безопасность

Типовые проблемы при проведении расширенного аудита

Запуск службы

Права на чтение журнала

Какие сложности возникают с SACL

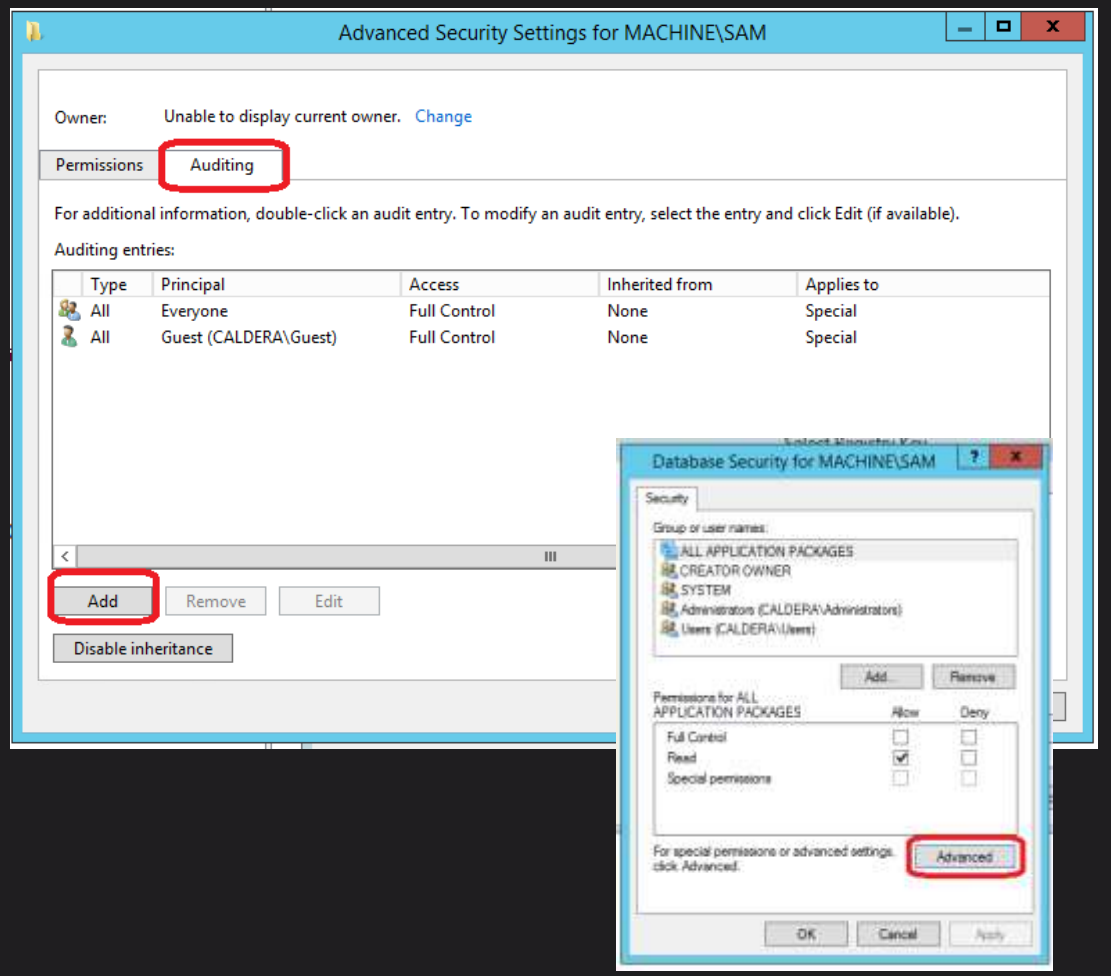
Штатная установка SACL

Отсутствие возможности редактирования

Потенциальная возможность затронуть DACL

Сложности с раскаткой на уникальные и персональные ветви

Проблемы на этапе проверки

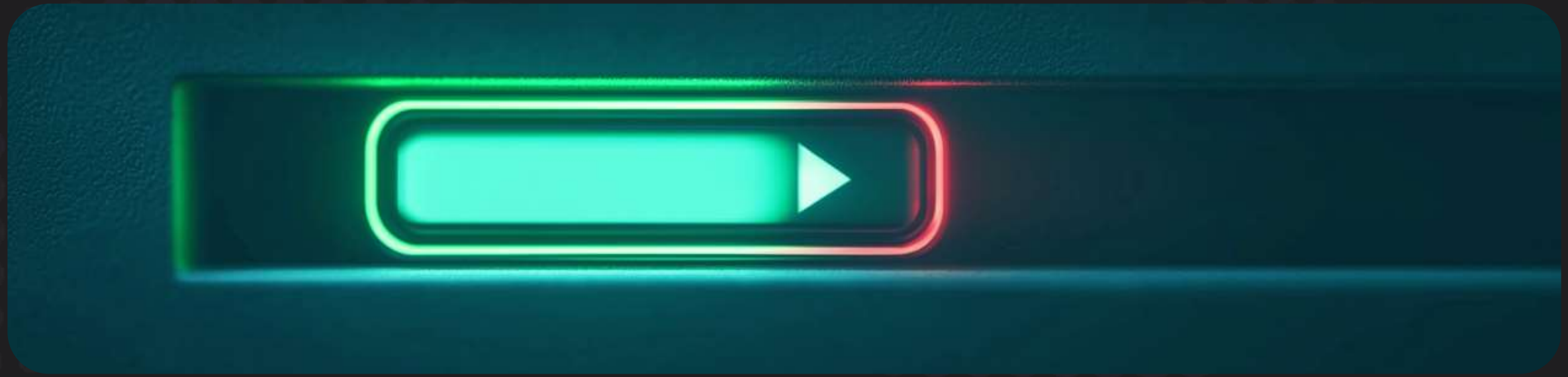


Проблема установки дополнительных компонентов

Права доступа

Сложность раскатки

Необходимость редактирования прав в журналах



Как решить проблемы с установкой средств

SCCM

- ⊕ Удобное управление
- ⊕ Можно использовать для всех типов устройств
- ⊕ Автоматическое распространение
- ⊖ Требует недешевой лицензии

Schedule/ GPO

- ⊕ Распространение на все типы устройств
- ⊕ Гибкое управление триггерами
- ⊖ Конфликты аудитов
- ⊖ Не всегда хватает прав
- ⊖ Нет обратной связи

Ansible

- ⊕ Условно бесплатное решение
- ⊕ Кросс-платформенность
- ⊖ Нужен пользователь с широкими правами
- ⊖ Требует плоских сетей
- ⊖ Хорошо работает на серверах, но не пользователях

Какие решить проблемы с SACL

```
New-PSDrive -name HKU -PSProvider Registry -Scope Global -Root HKEY_USERS


if (Test-Path -path $sysvol_path\$assign_list_fname) {
        Copy-Item -Path "$sysvol_path\$assign_list_fname" -Destination $sacl_path -Force
        foreach ($line in Get-Content $sacl_path\$assign_list_fname) {
                $Acl = Get-Acl -Path $line -audit
                $Acl.SetAuditRule($Audit)
                $Acl | Set-Acl -Path $line
        }
}
```

Какие решить проблемы с SACL. Распространение

Несколько но:

01

Персональные ветви
не появляются сразу

02

HKU\.Default — не то, чем кажется

Обратная связь

Скрипты проверок

Запись в windows event log

```
If
([System.Diagnostics.EventLog]::SourceExists
(‘SetAudit’) -eq $False) {

New-EventLog -LogName "SYSTEM" -Source
"SetAudit"}

...

Write-EventLog -LogName "SYSTEM" -Source
"SetAudit" -EventID 12001 -EntryType
Information -Message $auditmsg
```

Отправка сообщения напрямую в syslog collector:

```
$client = new-object
net.sockets.udpclient($port)

$client.connect($siemip,$port)

$client.send($send, $send.length)
```

Обратная связь

Контроль конфигураций

Расчет хеш-сумм от конфигураций

```
$hash_sddl = (Get-FileHash
"$curentPath\$ssdlfile" -Algorithm SHA256).hash
```

Профилирование конфигураций

Обратная связь

Контроль аудитов

```
foreach ($line in Get-Content $path\$filename)
{
    $rez = ($line.split(","))[1]
    $sf =@{}
    if ($rez.Contains("успех")){$sf["sucess"] = 1}
    else {$sf["sucess"] = 0}

    if ($rez.Contains("сбой")) {$sf["failure"] = 1}
    else {$sf["failure"] = 0 }
    $test.add(($line.split(","))[0],$sf)
}
```

```
foreach ($line in (auditpol /get /category:* /r))
{
    $guidindex = $line.IndexOf('{')
    if ($guidindex -gt 0)
    {
    $guid=$line.Substring($guidindex+1,37-1)
    if ($test.ContainsKey($guid) -eq $True)
        {
        testaudit($guid,$test)
        }
    }
}
```

Обратная связь

Контроль SACL

```
foreach ($line in Get-Content $curentPath\$assign_list_fname) {
            echo $line
            $Acl =$line +" : "+ (Get-Acl -Path $line -audit).Sddl
            $send = [text.encoding]::ascii.getbytes($Acl)
            $client.send($send, $send.length) #, $siem, $port)
            $result = $result+"`n"+$Acl
      }
```

Обратная связь

Контроль SIEM

```
logsource:
    category: SetAudit
detection:
    selection:
            action: failure
condition: selection
falsepositives:
    - unknown
level: low
```

```
logsource:
  category: SetAudit
detection:
  selection:
    action: Success
  timeframe: 600s
  condition: selection | count(category) by
src_host > <count_settings>
fields:
  - src_ip
falsepositives:
    - network error
level: low
```

Обратная связь

Контроль SIEM

```
logsource:
    category: SetAudit
detection:
    test: 'SACL'
    Hash|any:
            - <list of Hash>
condition: test and not Hash
falsepositives:
    - New config
level: high
```

А что с Linux?

Изменение аудита
во времени

Обратная связь аудита

Дальнейшее развитие

01

Автоматическая конфигурация аудит-контроля

02

Интеграция с SMDB/Zabbix

03

Контроль развертывания аудита новых хостов

K2 кибер безопасность

Спасибо за внимание

Контакты для связи

Кирилл Рупасов

Руководитель группы
инженеров SOC

Telegram — *@rupas_k*

salesinfosec@k2.tech

K2 кибер безопасность