

A hand in a suit is holding a large, metallic gear. Overlaid on the gear and the background is a complex network diagram consisting of various nodes, lines, and smaller gears, representing a technical or security system. The background is a blurred office setting with a person in a suit.

## **ViPNet IDS HS -**

новая сертифицированная система  
обнаружения вторжений уровня узла  
от компании Инфотекс

Иван Кадыков

# Для чего нужны NIDS?

- Определять атаки, которые “не видит” NIDS;
- Обнаружение атаки после расшифровки входящего трафика;
- Обнаруживать подозрительную активность внутри ОС (файловая активность, изменения в реестре и процессах).



# ViPNet IDS HS

ViPNet IDS HS - система обнаружения вторжений, осуществляющее мониторинг и обработку событий внутри хоста, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры .



# Ключевая функциональность – выявление IoC

Анализ системных журналов и логов ОС и приложений

Мониторинг файловой активности и реестра

## Источники событий

Результаты выполнения команд или изменений результатов команд

Анализ трафика проходящего через хост

# Возможности IDS HS



Различные методы определения атак

- Сигнатурный метод
- Метод аномалий



Базы правил разрабатываются при участии  
ЗАО «Перспективный мониторинг»



4 уровня критичности событий

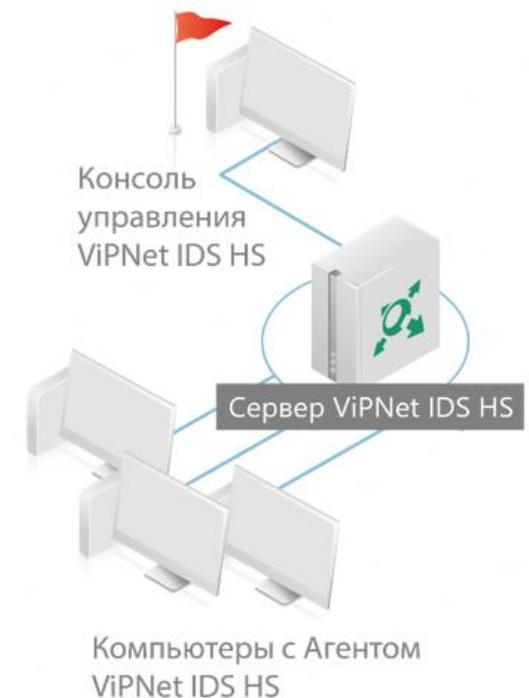


Уведомление администратора по e-mail



# Архитектура

- Агент — собирает необходимую информацию о функционировании хостов и выполняет первичный анализ данных
- Сервер — получает, хранит и анализирует информацию от Агентов, хранит правила, команды и параметры, и передаёт их на Агенты.
- Консоль управления — предоставляет графический интерфейс для управления Агентами и мониторинга их состояния



# Поддерживаемые ОС

- Microsoft Windows 10 (32/64-бит);
- Microsoft Windows 8.1 (32/64-бит);
- Microsoft Windows 8 (32/64-бит);
- Microsoft Windows 7 SP1 (32/64-бит);
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2008 R2 SP1;
- Microsoft Windows Server 2008 SP2 (32/64-бит);



# Сертификат

- Сертификат ФСТЭК России по требованиям к системам обнаружения вторжения уровня узла 4 класса.
- Список мер из приказов №21 и №17:
  - ИАФ.1, ИАФ.5
  - УПД.4
  - РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7
  - **СОВ.1, СОВ.2**
  - АНЗ.3
  - ОЦЛ.1, ОЦЛ.3
  - ИНЦ.2, ИНЦ.3, ИНЦ.4.



# Схема лицензирования

Совокупная стоимость продукта складывается из стоимости серверной лицензии (количество подключений агентов), права на подписку БРП на 1 год, сертификата на ТП и установочного комплекта.



# Внешний вид интерфейса

The screenshot displays the VIPNet IDS HS interface. The main window is titled "VIPNet IDS HS" and shows a list of "События и атаки" (Events and Attacks). A search bar and filter icons are visible above the table. The table lists various system events, including registry changes, file system modifications, and login attempts. One event is highlighted in blue, indicating it is the selected item.

Дата, время	Событие	Попытки	SIG	Устройство	Группа
02.03.17 11:03:09	Изменение реестра	2	100000		
02.03.17 11:03:09	Изменение реестра	2	100000		
02.03.17 11:02:51	Установлена задача планировщика	2	402000		
02.03.17 11:02:51	Попытка сброса пароля учетной записи.	1	600004		
02.03.17 11:02:51	Изменение учетной записи.	1	600002		
02.03.17 11:02:51	Изменение реестра	51	100000		
02.03.17 11:02:35	Изменение файловой системы	1	200000		
02.03.17 11:02:31	Интерактивный вход в систему.	4	500001		
02.03.17 11:02:31	Успешный вход с привилегированной учетной...	2	500004		
02.03.17 11:02:31	Изменение реестра	1	100000		
02.03.17 11:02:13	Изменение файловой системы	6	200000		
02.03.17 11:02:13	Изменение реестра	2	100000		
02.03.17 11:01:59	Изменения процессов	3	100400		
02.03.17 11:01:58	Изменение реестра	50	100000		
02.03.17 11:01:58	Создание процесса	2	300001		
02.03.17 11:01:58	Изменение файловой системы	2	200000		

The detailed view on the right shows the event "Успешный вход с привилегированной..." (Successful login with privileged account...). It includes a "Сработавшее правило" (Triggered rule) and "Логи события" (Event logs). The event description states: "Успешный вход с привилегированной учетной записью." (Successful login with privileged account). The category is "Подозрительная, потенциально опасная активность" (Suspicious, potentially dangerous activity). Recommendations include: "Рекомендуемые действия: провести корреляцию с другими событиями ИБ." (Recommended actions: conduct correlation with other security events).

Опасное событие

Подробная информация о событии

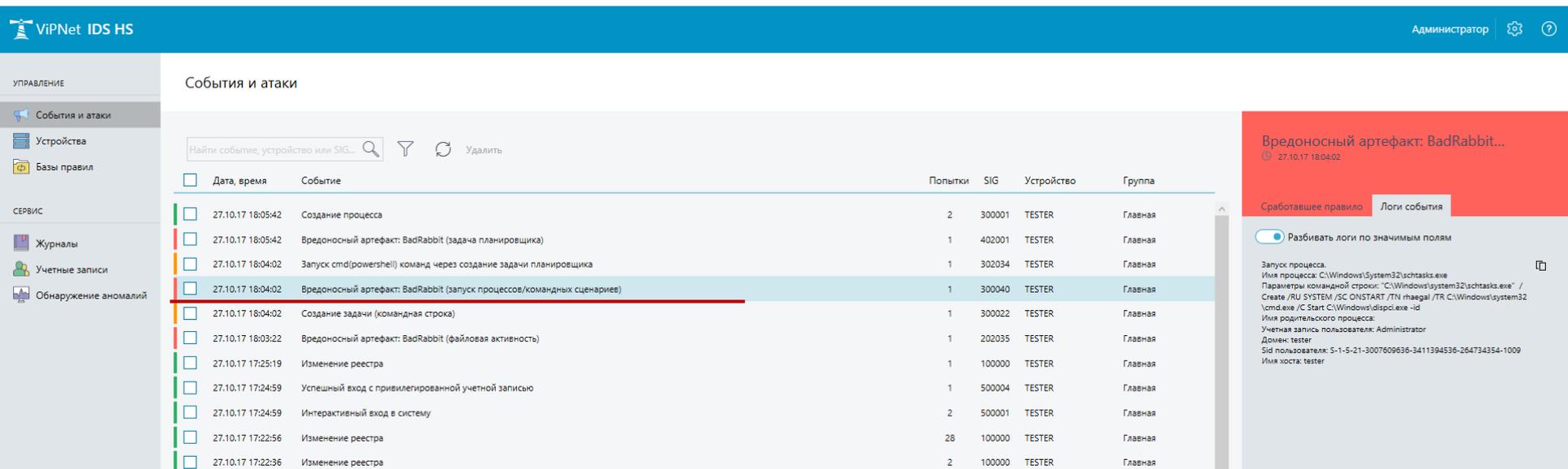
Рекомендации по дальнейшим действиям

**CONFIDENTIAL**

# BadRabbit - detected

24.10.2017 в пик активности шифровальщика BadRabbit произошли срабатывания сигнатур на ViPNet IDS HS:

- Запуск потенциально опасного ПО: mimikatz (sid: 121003)
- Вредоносный артефакт: mimikatz components (sid: 121117)
- mimikatz activity: попытка извлечения данных учетных записей (sid: 180000)
- mimikatz activity: попытка проведения pass-the-hash атаки (sid: 180001)
- mimikatz activity: попытка повышения привилегий (sid: 180002)



The screenshot shows the ViPNet IDS HS interface. On the left is a navigation menu with options like 'События и атаки', 'Устройства', 'Базы правил', 'СЕРВИС', 'Журналы', 'Учетные записи', and 'Обнаружение аномалий'. The main area displays a table of events under the heading 'События и атаки'. The table has columns for 'Дата, время', 'Событие', 'Попытки', 'SIG', 'Устройство', and 'Группа'. One event is highlighted in red: '27.10.17 18:04:02 Вредоносный артефакт: BadRabbit (запуск процессов/командных сценариев)'. To the right, a detailed view of this artifact is shown, including the command string: 'C:\Windows\system32\schtasks.exe / Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR C:\Windows\system32\cmd.exe /C Start C:\Windows\idsplci.exe -id'. Below this, it shows the user 'tester' and their SID.

Дата, время	Событие	Попытки	SIG	Устройство	Группа
27.10.17 18:05:42	Создание процесса	2	300001	TESTER	Главная
27.10.17 18:05:42	Вредоносный артефакт: BadRabbit (задача планировщика)	1	402001	TESTER	Главная
27.10.17 18:04:02	Запуск cmd(powershell) команд через создание задачи планировщика	1	302034	TESTER	Главная
27.10.17 18:04:02	Вредоносный артефакт: BadRabbit (запуск процессов/командных сценариев)	1	300040	TESTER	Главная
27.10.17 18:04:02	Создание задачи (командная строка)	1	300022	TESTER	Главная
27.10.17 18:03:22	Вредоносный артефакт: BadRabbit (файловая активность)	1	202035	TESTER	Главная
27.10.17 17:25:19	Изменение реестра	1	100000	TESTER	Главная
27.10.17 17:24:59	Успешный вход с привилегированной учетной записью	1	500004	TESTER	Главная
27.10.17 17:24:59	Интерактивный вход в систему	2	500001	TESTER	Главная
27.10.17 17:22:56	Изменение реестра	28	100000	TESTER	Главная
27.10.17 17:22:36	Изменение реестра	2	100000	TESTER	Главная

**Вредоносный артефакт: BadRabbit...**  
27.10.17 18:04:02

Срабатывающее правило: **Логи события**

Разбивать логи по значимым полям

Запуск процесса.  
Имя процесса: C:\Windows\system32\schtasks.exe  
Параметры командной строки: "C:\Windows\system32\schtasks.exe" / Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR C:\Windows\system32\cmd.exe /C Start C:\Windows\idsplci.exe -id  
Имя родительского процесса:  
Учетная запись пользователя: Administrator  
Домен: tester  
Sid пользователя: S-1-5-21-3007609636-3411394536-264734354-1009  
Имя хоста: tester

# Перспективы развития

- 09.11.2017 вышла версия 1.2:
  - Интеграция с Active Directory и ViPNet-сетями
  - Поддержка syslog (формат CEF) и snmp
  - Интеграция с ViPNet TIAS
  - Возможность управления продуктом из консоли ViPNet IDS MC
  - Детализация событий и рекомендации
  - Поддержка AstraLinux 1.5 и Debian
- Версия будет передана на инспекционный контроль. (при купленной первой версии – обновление будет бесплатным)



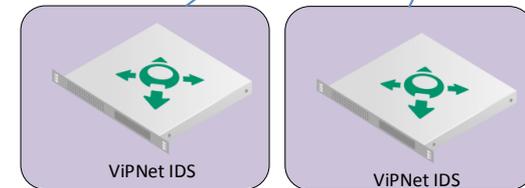
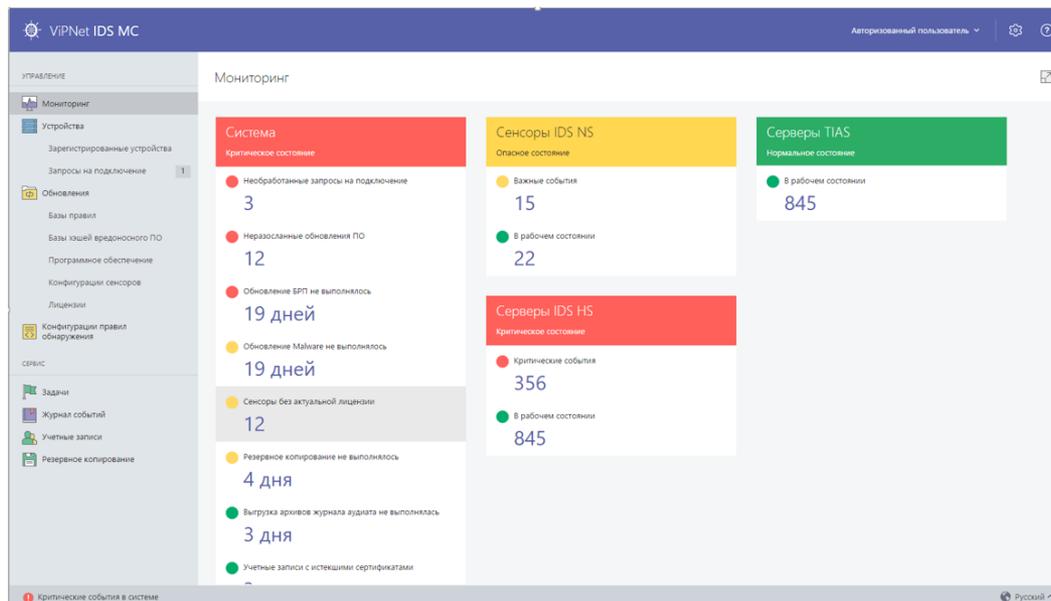
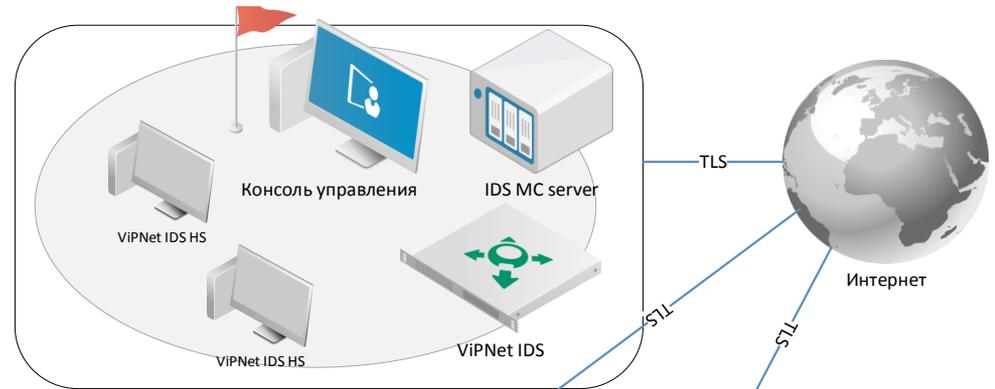
A person in a dark suit and blue patterned tie is holding a large, silver, 3D-rendered gear. In the background, a complex, multi-layered gear mechanism is visible, suggesting a complex system or process. The overall image has a blue and grey color palette with a semi-transparent white text box.

Комплексное решение  
компании ИнфоТеКС для  
обнаружения и устранения  
угроз и вторжений.

# Интеграция с IDS MC

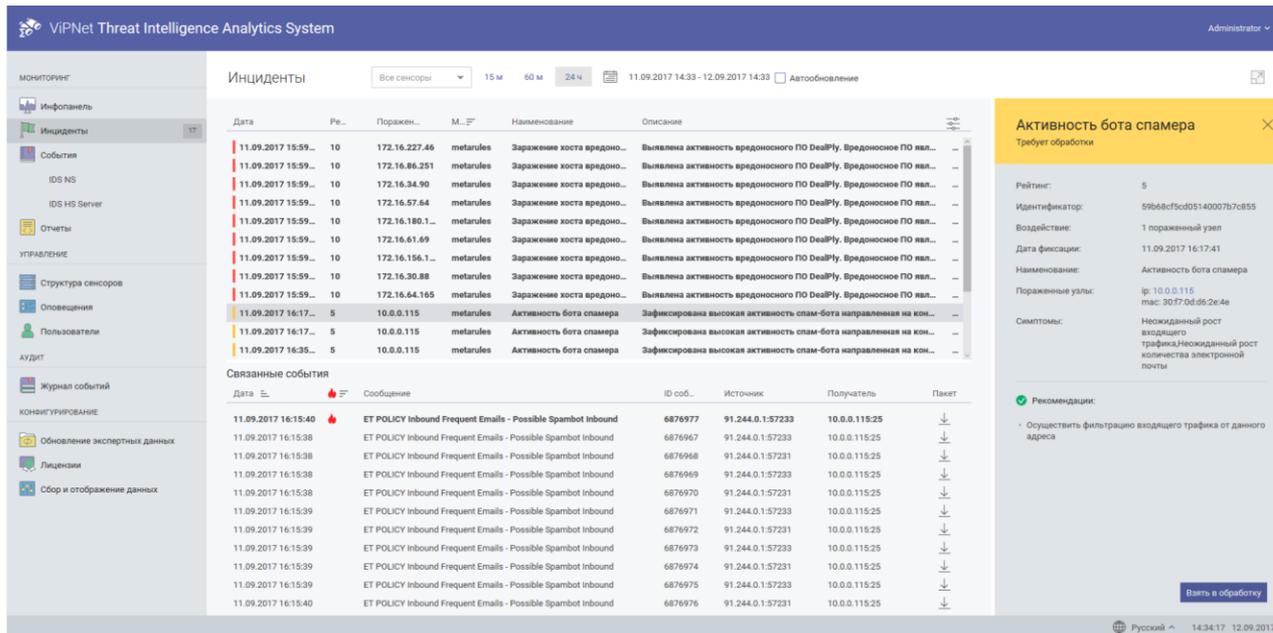
Единая консоль управления системами обнаружения вторжений:

- ViPNet IDS NS
- ViPNet IDS HS



# Интеграция с TIAS

- Возможность передачи событий от IDS HS в TIAS для выявления инцидентов и построения цепочек событий безопасности, которые привели к инциденту



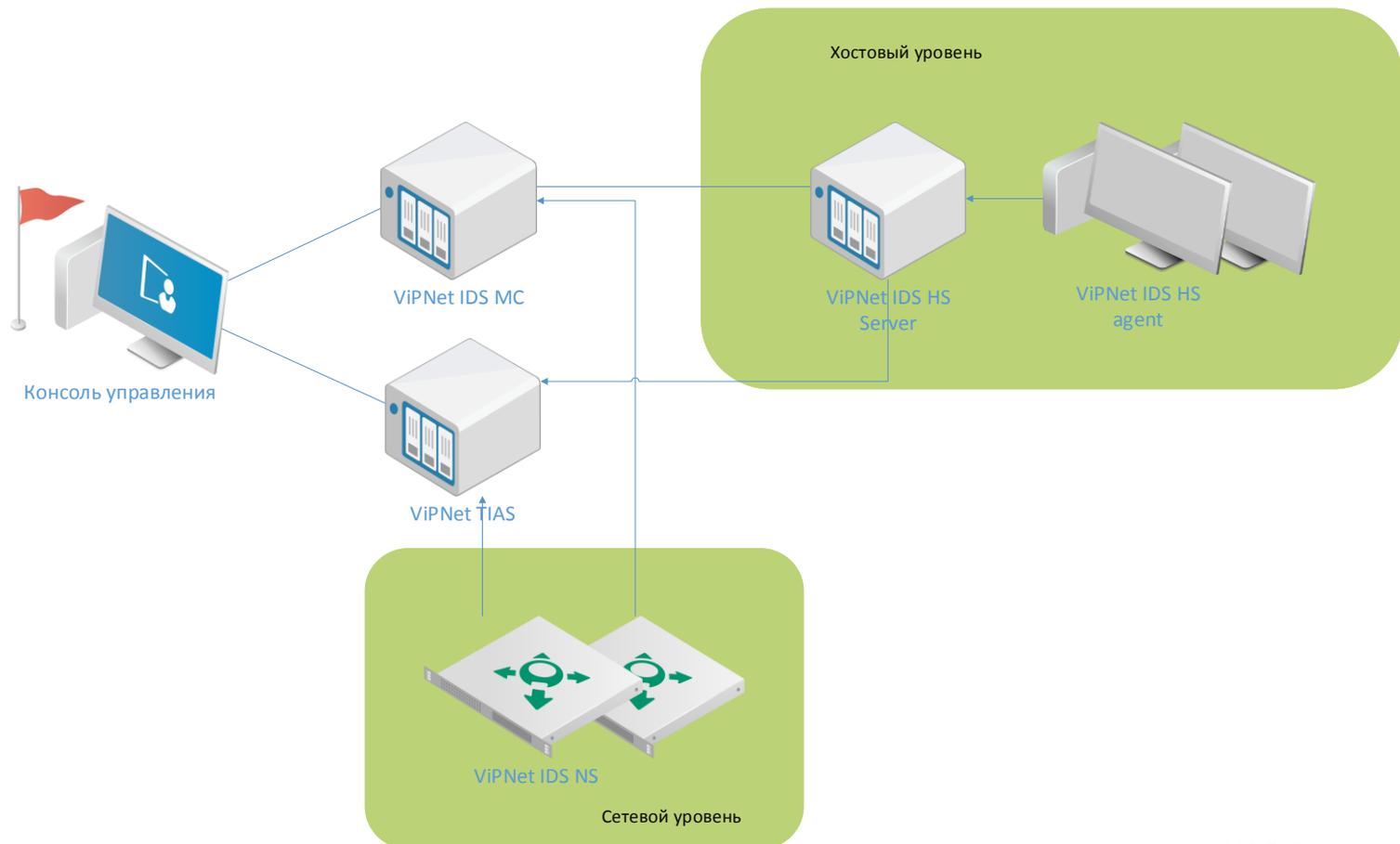
The screenshot displays the ViPNet Threat Intelligence Analytics System interface. The main window shows a list of incidents with columns for Date, Severity (Re...), Count (Поражен...), Malware (M...), Name (Наименование), and Description (Описание). A specific incident is highlighted, showing a bot spammer activity detected on 11.09.2017 at 16:17:05. A detailed view of this incident is shown on the right, titled 'Активность бота спамера' (Bot spammer activity), which includes details such as Rating (5), Identifier (59b68cf5cd05140007b7c855), and a recommendation to filter incoming traffic.

Дата	Re...	Поражен...	M...	Наименование	Описание
11.09.2017 15:59...	10	172.16.227.46	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.86.251	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.34.90	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.57.64	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.180.1...	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.61.69	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.156.1...	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.30.88	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 15:59...	10	172.16.64.165	metarules	Заражение хоста вредоно...	Выявлена активность вредоносного ПО DealPhy. Вредоносное ПО явл...
11.09.2017 16:17...	5	10.0.0.115	metarules	Активность бота спамера	Зафиксирована высокая активность спам-бота направленная на кон...
11.09.2017 16:17...	5	10.0.0.115	metarules	Активность бота спамера	Зафиксирована высокая активность спам-бота направленная на кон...
11.09.2017 16:35...	5	10.0.0.115	metarules	Активность бота спамера	Зафиксирована высокая активность спам-бота направленная на кон...

Дата	Сообщение	ID соб...	Источник	Получатель	Пакет
11.09.2017 16:15:40	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876977	91.244.0.1:57233	10.0.0.115:25	↓
11.09.2017 16:15:38	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876967	91.244.0.1:57233	10.0.0.115:25	↓
11.09.2017 16:15:38	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876968	91.244.0.1:57231	10.0.0.115:25	↓
11.09.2017 16:15:38	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876969	91.244.0.1:57233	10.0.0.115:25	↓
11.09.2017 16:15:38	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876970	91.244.0.1:57231	10.0.0.115:25	↓
11.09.2017 16:15:39	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876971	91.244.0.1:57233	10.0.0.115:25	↓
11.09.2017 16:15:39	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876972	91.244.0.1:57231	10.0.0.115:25	↓
11.09.2017 16:15:39	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876973	91.244.0.1:57233	10.0.0.115:25	↓
11.09.2017 16:15:39	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876974	91.244.0.1:57231	10.0.0.115:25	↓
11.09.2017 16:15:39	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876975	91.244.0.1:57233	10.0.0.115:25	↓
11.09.2017 16:15:40	ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	6876976	91.244.0.1:57231	10.0.0.115:25	↓

# ITDP: Intrusion&Threats – Detection&Prevention



A sunset scene with wind turbines and power lines. The sky is filled with orange and yellow clouds, and the sun is low on the horizon. In the foreground, several wind turbines are silhouetted against the bright sky. In the background, a series of high-voltage power lines stretch across the landscape. The overall mood is warm and serene.

**Спасибо!**