



#### Aether Релиз XII Что нового

21.07.2021

www.pandasecurity.com www.cloudav.ru



#### Содержание

- 1. Обзор релиза
- 2. Индикаторы атаки
- 3. Настройки
- 4. Компьютеры
- 5. Мои оповещения
- 6. Задачи
- 7. Другие улучшения в Aether

# Обзор релиза

#### Обзор релиза

- Сервисы Threat Hunting позволяют администраторам обнаруживать скомпрометированные машины, ранние стадии атак и подозрительную активность
- Сервисы Threat Hunting помогают обнаруживать:
  - RDP-атаки на подключение к удаленному рабочему столу
  - Атаки без использования вредоносных программ
  - Скомпрометированные компьютеры
  - Хакеров и инсайдеров
- Новый релиз XII платформы Aether предоставляет администраторам доступ к инструментам сервиса Threat Hunting, включая индикаторы атак, расширенное расследование, графики и сопоставление с матрицей MITRE
- В новом релизе XII можно автоматически останавливать RDP-атаки



## Индикаторы атаки

#### Что такое индикатор атаки?

- Индикаторы атаки (IoA) это подтвержденные события, которые с высокой степенью вероятности говорят о наличии атаки
  - Наша команда ИБ подтверждает события, получаемые с конечных устройств, если они соответствуют созданным ею гипотезам
- Как правило, сведения об атаке можно получить на ее самые ранних стадиях, когда еще не используется какое-либо вредоносное ПО
- Мы настоятельно рекомендуем Вам сдерживать атаки и восстанавливать конечные устройства как можно быстрее

#### Панель индикаторов атаки

- В разделе Статус > Индикаторы атак Вы можете увидеть сводную информацию по обнаружениям сервиса Threat Hunting.
- Панель показывает информацию за период времени, выбранный в верхней части страницы
- Для получения более подробной информации необходимо нажать на соответствующие ссылки в панели



### Виджет Threat Hunting

- Виджет Threat Hunting показывает сводную информацию по событиям, индикаторам и индикаторам атак (IoA) для всех компьютеров и устройств в сети за выбранный период времени
  - События количество действий, выполненных программами, установленными на защищаемых компьютерах, и отслеживаемых решением Adaptive Defense 360 / Adaptive Defense
  - Индикаторы количество подозрительных событий, обнаруженных в потоке данных событий
  - Индикаторы атак количество индикаторов, которые с высокой степенью вероятности характеризуют наличие атаки
- Чтобы открыть статус защиты компьютеров и увидеть компьютеры, которые подверглись RDPатаке, необходимо нажать ссылку Смотреть все
- Локальный кеш невредоносных программ (goodware)

#### CEPBUC THREAT HUNTING



2 Компьютеров в режиме "Сдерживание RDP-атак". Смотреть все

#### Виджет Эволюция обнаружений

- Виджет Эволюция обнаружений гистограмму обнаружений индикаторов, ЮА в ожидании и архивных ЮА за определенный период времени
  - Индикаторы количество подозрительных элементов, обнаруженных в потоке данных событий
  - ЮА в ожидании количество подозрительных элементов, которые с высокой степенью вероятности являются индикаторами атак (IOA). При этом администратор еще не проанализировал их
  - Архивные ЮА количество подозрительных элементов, которые с высокой степенью вероятности являются индикаторами атак (ЮА). При этом администратор уже проанализировал их и решил связанные с ними вопросы
  - Левая ось У показывает количество ІОА (архивные и в ожидании)
  - Правая ось У показывает обнаруженные индикаторы
- Чтобы открыть список индикаторов атаки, необходимо нажать на виджете

#### ЭВОЛЮЦИЯ ОБНАРУЖЕНИЙ



### О матрице MITRE ATT&CK

- MITRE ATT&CK это стандарт в индустрии для классификации тактик и техник атак
- Охотники за угрозами (threat hunting) используют ее для оценки рисков организации



#### Индикаторы атак в соответствии с матрицей MITRE

- Данный виджет в панели индикаторов атак показывает количество индикаторов атак, обнаруженных за выбранный период времени, в соответствии с тактиками и техниками MITRE
- Чтобы посмотреть название и код техники или общее количество обнаружений, наведите мышку на столбец или блок
  - Заголовки столбцов это тактики
  - Техники показываются ниже тактики
  - Чтобы увидеть ЮА в ожидании, наведите мышку на число в красном кружке

#### ИНДИКАТОРЫ АТАК (ІОА) В СООТВЕТСТВИИ С МАТРИЦЕЙ МІТКЕ



#### Индикаторы атак в соответствии с матрицей MITRE

 Нажмите на тактику или технику, чтобы открыть список Индикаторы атак с выборкой по выбранной тактике или тактике и технике

ALL DUALATO DUE ATAIX	(TOAL D	CONTRETETRIAL	C LAATDIAL FLA AATTOF
	110 10 1 8	C D R D R F R D R R R R R	I MATRIATER MITRE
	ILON D	COULDELCIDNN	CIVICIT FILLEF WITTINE
	*		

Initial Access	Exe	ution	Persistence	Privile Escala	ge tion	Defense Evasion										
Valid	Com Line Inte	mand-	Accessibility	50 СТИ	лус	компьютерь	і настрой	ки вадачи		демо	D Bee	¢9	•	8 drussian_fo	aderation_c14 DEMO - Adapt	UV
0,	G	панел	И УПРАВЛЕНИЯ		<	Индикато	оры атак	(IOA)								I
• •		0 :	Sezonachocte		Иск	atu		Q	Фильтры 🔿							₿
		<u>ک</u> و	Зеб-доступ													
		8,	Индикаторы атак (ІОА)		Риск		~	Дойствие		Тактика	Eccolation /7	240004)	4	Latu:	e ă	
		88 F	Patch Management		Стату	IC.		Индикатор атак		Privilege	Escalation (1	A0004)		последние / дн		1
		@ =	Full Encryption		Bce		×	Bce	~	Bce			~			
		8 /	Тицензии												Q BNE	рать
					ПК	омпьютер	Fpynna	Индикатор атак		Инцид	енты Риск		Дейсте е	Статус	Дата 👃	
		моис	писки до	Барить	0	2 WIN_LAPTOP_ 1	Laptop	Повышение приви	легий в обход U/	lic.	1 Крити	лческий		в ожидании	25.07.2021 13:01:15	1

### Обнаруженные ЮА и компьютеры с ЮА

- Виджет Обнаруженные индикаторы атак показывает распределение по типу обнаруженных ЮА за выбранный период времени
  - Чем больше количество обнаруженных IOA определенного типа (относительно других типов), тем крупнее его квадратик
- Виджет Компьютеры с индикаторами атак показывает распределение обнаруженных ЮА по компьютерам в сети за выбранный период времени
- Нажмите на требуемый квадратик в виджетах, чтобы открыть список Индикаторы атак с выбранной информацией



ОБНАРУЖЕННЫЕ ИНДИКАТОРЫ АТАК (IOA)



КОМПЬЮТЕРЫ С ИНДИКАТОРАМИ АТАК (ІОА)

#### Список Индикаторы атак

- Список Индикаторы атак показывает сведения по IOA, обнаруженным решениями Adaptive Defense 360 или Adaptive Defense на рабочих станциях и серверах
- Чтобы открыть список, в панели Индикаторы атак необходимо нажать на количество IOA (виджет Сервис Threat Hunting) или на любые другие виджеты (и их элементы) в данной панели (в этом случае откроется отфильтрованный список)
- Чтобы добавить список в Мои списки:
  - В левом меню «Мои списки» нажмите ссылку Добавить
  - В секции Безопасность выберите Индикаторы атак (IOA)
  - При необходимости настройте фильтр и нажмите Сохранить

ПАНЕ	ЛИ УПРАВЛЕНИЯ	
$\mathbb{O}$	Безопасность	
<u>^-</u>	Веб-доступ	
2	Индикаторы атак	(IOA)
8	Patch Management	:
٢	Full Encryption	
R	Лицензии	
мои	списки	
	CHRICKR	Добавить
1	Незащищенные р	Добавить абочи
() ()	Незащищенные р Незащищенные с	добавить абочи
() ()	Незащищенные р Незащищенные се Оборудование	добавить абочи ерверы
	Незащищенные р Незащищенные с Оборудование ПО	добавить абочи ерверы

#### Список Индикаторы атак

- Для просмотра сведений по всем доступным ЮА, Вы можете экспортировать список в CSV-файл
- В списке индикаторов атак можно применить фильтр для более узкого поиска
- В контекстном меню у каждого индикатора атаки Вы можете отправить данный индикатор в архив, посмотреть IOA, обнаруженные на данном компьютере или посмотреть компьютеры, на которых обнаружен данный IOA

Adaptive Defense 360	статус компью	еры настр	РОЙКИ ЗАДАЧИ	ДЕМО	Bce	۞ 💫		ian_federation_c1 SIAN DEMO - Ada	4 ptiv
ПАНЕЛИ УПРАВЛЕНИЯ	< Индик	аторы ата	ак (ІОА)						:
🔘 Безопасность	Искать		Q Фильтры	~					B
🖅 Веб-доступ	Компьютер	Группа	Индикатор атак	Инцидент	Риск	Действие	Стату	/с Дата ↓	
<ul> <li>Индикаторы атак (IOA)</li> <li>Patch Management</li> </ul>	WIN_DES     OP_1	T 🗋 Workst ation	Скомпрометированные учетные данные после RDP-атаки типа «brute-force»	-	В архив				•
( Full Encryption	B WIN_SER	E 🗋 Server	Дамп учетных данных из процесса LSASS с использованием ProcDump	2	Смотреть IO	А, обнаружен	ные на этом і	компьютере	:
Я Лицензии		T 🗋 Workst ation	Загрузка файлов через процесс svchost.exe	Ţ	Смотреть ко	мпьютеры, на	а которых обн ожид	наружен этот IOA ании 13:55:15	`:
мои списки Добавит	ъ 💭 WIN_DES OP_3	T 🗋 Workst ation	Дамп учетных данных из процесса LSASS с использованием PowerShell	1	Критический	й	В ожид	25.07.202 ании 13:53:15	1 :

#### Сведения по индикатору атаки

- Для просмотра сведений по конкретному индикатору атаки, нажмите на нем в списке индикаторов атак
- Чтобы отправить индикатор атаки в архив или перевести в статус «В ожидании», нажмите синюю кнопку рядом с датой обнаружения
- Для просмотра описаний тактики и техники, используемых на пострадавшем компьютере, нажмите кнопку
   Расширенное исследование атаки
  - Включает рекомендации по смягчению последствий атаки и последовательность событий, приведших к появлению индикатора атаки

Adaptive Defense 360	СТАТУС	компьютеры	настройки	задачи	ДЕМО	D Bce	0	8 drussian_feder	ation_c14 MO - Adaptiv			
ПАНЕЛИ УПРАВЛЕНИЯ	<	Назад	Дамп уче	тных данных і	из процесса LSA	SS с исп	ользован	ием ProcDum	р			
Безопасность	д	ата обнаружения:	25	5.07.2021 14:03:15	Вархив							
🗠 Веб-доступ 📋 Индикаторы атак (IOA)	И	Індикатор атак (IO/	а): Д	амп учетных данных і	із процесса LSASS с испо	ользование	и ProcDump					
Patch Management	0	иск: Описание:	3/ 3/	овсокии Злоумышленник пытается украсть имена и пароли учетных записей для доступа к другим системам, извлекая информацию из процесса Isass.exe в Windows. Для этого злоумышленник делает дамп памяти								
Full Encryption           Я         Лицензии			n	роцесса LSASS, исполь	зуя утилиту ProcDump.	~						
мои списки Добави	ть р	екомендации:		роверьте, является ли	асследование атаки это вторжением, закон	ными дейст	виями или тес	рафикатаки 🖸				
<u> </u>			Ed	ли это вторжение, ре	комендуется:	H						

### График атаки ЮА

- Для просмотра графического представления дерева выполнения атаки, по которому появился данный индикатор атаки, на странице со сведениями ЮА нажмите на кнопку Смотреть график атаки
  - Узлы это элементы, которые участвуют в операции (например, процессы, файлы, и т.д.)
  - Стрелки показывают направление операции
- График помогает идентифицировать причину атаки



#### Подробности индикатора атаки

- Секция Подробности индикатора атаки (IOA) показывает пострадавший компьютер, количество обнаруженных инцидентов, а также дату и время последнего события
- Блок Другие подробности предоставляет пример JSON с полями, соответствующими событию, которое привело к появлению данного индикатора атаки

Подробности инди	катора атак (IOA)
Компьютер:	WIN_SERVER_2
Обнаруженные инциденты:	1
Последнее событие:	25.07.2021 0:16:26
Другие подробности:	[ { "ChildPath": "PROFILE \\Downloads\\Procdump\\procdump.exe", "CommandLine": "\"C:\\Users\\CLEBER\\Downloads\\Procdump\\procdump.exe\" -accepteula - ma lsass.exe mydump.dmp", "ParentPath": "SYSTEM \\WindowsPowerShell\\v1.0\\powershell.exe", "ChildMd5": "D3763FFBFAF30BCFD866B8ED0324E7A3", "extendedInfo": "", "ParentPID": "8117", "ChildFileName": "procdump.exe", "ParentFileName": "powershell.exe", "LoggedUser": "WIN_SERVER_2\\CLEBER",

### Подробности MITRE

- Секция MITRE показывает тактику и технику, а также подробное описание техники
- Нажмите на тактику или технику, чтобы увидеть их описания на веб-сайте MITRE

#### 🗇 MITRE

Тактика:	Credential Access (TA0006)
Техника:	Credential Dumping (T1003)
Платформа:	Windows, Linux, macOS
Необходимые разрешения:	Administrator, SYSTEM, root
Описание:	Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.
	Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
	### Windows
	#### SAM (Security Accounts Manager)

#### Список Статус защиты компьютеров

- В панели Индикаторы атаки виджет Сервис Threat Hunting показывает количество компьютеров в режиме сдерживания RDP-атак
- Режим сдерживания RDP-атак защищает от тех сценариев, когда хакер проникает в ИТ-сеть через уязвимый компьютер, затем осуществляет горизонтальные перемещения на другие незащищенные устройства, и использует RDP для перехода с одного устройства на другое
- Нажмите на ссылку Смотреть все, чтобы открыть список Статус защищенных компьютеров с выборкой по компьютерам с включенным режимом сдерживания RDP-атак

#### CEPBUC THREAT HUNTING



2 Компьютеров в режиме "Сдерживание RDP-атак". Смотреть все

# Изменения в списке Статус защищенных компьютеров

- Список Статус защищенных компьютеров включает новую иконку RDP для отображения того, что данный компьютер работает с включенным режимом сдерживания RDP-атак
- Новый столбец Подключение к Знаниям показывает, может ли установленный агент подключаться к серверам знаний и обновлять сигнатурные файлы

0	Adaptive Defense 360	CTATYC	компьютеры	настройки	задачи			] Bce (	🤊 📀 2	drussian_federation_c14 DRUSSIAN DEMO - Adapti	v
ПАНЕ	ЛИ УПРАВЛЕНИЯ	<	Статус защи	иты компь	ютеров						:
$\mathbb{O}$	Безопасность	N.	скать		Q	Фильтры 👻					B
<u>^-</u>	Веб-доступ		Компьютер	Группа	Расширенна защита	ая Антивиру с	Обновленная защита	а Знания	Подключение к Знаниям	Последнее соединение ↓	
8	Индикаторы атак (IOA)	Π	U WIN_LAPTOP_	🛛 👱 🗋 Laptop	8	$\odot$	9	Ø	$\odot$	25.07.2021 16:48:13	:
88	Patch Management		UWIN_DESKTOP_1	🙁 🗋 Workst	atio 🕝	Ø	$\bigcirc$	0	Ø	25.07.2021 16:48:12	:
٢	Full Encryption			n							
R	Лицензии										

#### Режим сдерживания RDP-атак

- Новый релиз XII платформы Aether отслеживает попытки подключения к компьютеру в сети через службу RDP
- Если свыше 50 неудачных попыток подключения были с одного и того же IP-адреса, то включается режим Сдерживание RDP-атак
  - Запрещаются все IP-адреса, которые имеют свыше 23 подключений
  - Если злоумышленник способен удачно подключиться с правами администратора, то идентифицируются все коммуникации с внешних IP-адресов за последние 24 часа с более одной ошибкой, при этом эти внешние IP-адреса запрещаются
  - Если свыше 50 неудачных попыток подключения были с одного и того же IP-адреса, то включается режим Сдерживание RDP-атак
- Вы можете добавить разрешенные IP-адреса в разрешенный список, чтобы подключения с этих IP-адресов не блокировались

#### Страница со сведениями по компьютеру

- В списке выберите требуемый компьютер, чтобы перейти на страницу со сведениями о данном компьютере
- В блоке с уведомлениями показывается предупреждение о том, что у компьютера включен режим сдерживания RDP-атак
- Чтобы отключить данный режим, нажмите на кнопку Отключить режим «Сдерживания RDP-атак»



# Настройки

#### Права в ролях пользователей

- Вам необходимо настроить новые права безопасности для той роли пользователей, которые смогут настраивать параметры индикаторов атак
- В разделе Настройки > Пользователи на закладке Роли у требуемой роли необходимо включить разрешение Настроить индикаторы атак (IOA)

Adaptive Defense 360	статус компьютеры	НАСТРОЙКИ	задачи	демо	🛅 Bce	( <mark>2</mark> )	چ د	drussian_federation_c14 DRUSSIAN DEMO - Adaptiv					
основное	Отменить			Изменить роль	5			Сохранить					
В Пользователи	Перезапускать и восс	lepeзапускать и восстанавливать компьютеры											
🖧 Настройки компьютеров	Изолировать компью	золировать компьютеры											
	БЕЗОПАСНОСТЬ	ЗОПАСНОСТЬ											
Сетевые настройки	Настраивать безопас	ность для рабочі	их станций и сервери	ов									
📒 Сетевые службы	Настраивать безопас	ность для устрой	іств с Android										
VDI-среды	Использовать защиту	/ Анти-вор для ус	стройств Android (обн	наружение, очистка, блок	ировка и т.д	.)							
<u>۸</u>	Смотреть обнаружен	ия и угрозы											
//>// Мои оповещения	Смотреть доступ к ве	б-страницам											
	Запускать проверки	Запускать проверки											
БЕЗОПАСНОСТЬ	Временно исключать	угрозы (Вредон	осное ПО, ПНП и Заб	локированные объекты)									
📃 Рабочие станции и серверы	Настраивать управле	ние патчами											
	Установить, удалить і	и исключить пат	чи										
	Настроить блокировк	у программ											
Блокировка программ	Настраивать разреше	енное ПО											
🕗 Разрешенное ПО	Настроить индикатор	ы атак (IOA)											
Verooverna Android	ЗАЩИТА ДАННЫХ												
. Scipoversa Android	Настраивать шифров	ание компьютер	008										

#### Настройки безопасности – Индикаторы атак

- В разделе Настройки > Индикаторы атак (IOA)
   Вы можете включить защиту от RDP-атак и других индикаторов атак
- Чтобы посмотреть описание индикатора атаки, нажмите на иконку с восклицательным знаком у требуемого индикатора в списке
- Вы можете отключить индикаторы атак для ложных срабатываний и применить профиль с настройками безопасности для группы компьютеров, конкретных компьютеров или для всей организации

Adaptive Defense 360 CT/	АТУС КОМПЬЮТЕРЫ НАСТРОЙКИ	<b>задачи</b> ден	10 🗖 Bce	۞ 🔇	8 drussian_federa	tion_c14 O - Adaptiv
основное	Отменить	Добавить нас	тройки			Сохранить
🖉 Пользователи	Имя: Настройки нового индикатора а	так (ІОА)				
🔗 Настройки компьютеров	Описание: Описание					
💮 Сетевые настройки	Получатели: Получатели пока не выб	раны				
😸 Сетевые службы	Индикаторы атак и поведе	ение				
🐼 VDI-среды	RDP-атаки			Расш	иренные настройки $\smallsetminus$	
🖄 Мои оповещения	<ul> <li>Атака типа Brute-force против RDI</li> <li>Скомпрометированные учетные,</li> </ul>	э (]) данные после RDP-атаки типа «brute-fo	rce» (])			
БЕЗОПАСНОСТЬ	PowerShell.exe переименован 🛛 💭					
	Выполнение в памяти удаленного скр	ипта 💭				
(0)	Выполнение запутанных параметров	командной строки с использованием с	md.exe 💭			
о индикаторы атак (10А)	Выполнение скрипта в памяти с помо	цью PowerShell 🕕				
Блокировка программ	Дамп учетных данных из процесса LSA	SS с использованием PowerShell 🕕				
Разрешенное ПО	Дамп учетных данных из процесса LSA	SS с использованием ProcDump				
<ul> <li>Устройства Android</li> <li>Patch management</li> </ul>	Деинсталляция решения Panda для за	щиты конечного устройства 🛛 💭				

### Расширенные настройки для RDP-атак

- Когда Вы включаете опцию RDP-атаки, Вы можете настройки Расширенные настройки
  - Автоматическая реакция в этой секции Вы можете выбрать, какие действия будут применяться автоматически отдельно для рабочих станций и серверов (Только сообщить или Сообщить и заблокировать RDP-атаки)
  - Надежные IP в этой секции Вы можете указать IP-адреса и диапазоны IP-адресов в качестве исключений. О них будет сообщаться, но они не будут блокироваться

Adaptive Defense 360	статус компьютеры	настройки	задачи Демо	D Bce	Ç <mark>2</mark>	<del>ن</del> ک	drussian_federation_c14 DRUSSIAN DEMO - Adaptiv						
основное	Отменить		Добавить наст	ройки			Сохранить						
😤 Пользователи	Индикаторы ат	Индикаторы атак и поведение											
🔗 Настройки компьютеров	RDP-атаки • Атака типа Brute	-force против RD	P (I)		F	Расширен	ные настройки 🔨 💼						
Сетевые настройки	• Скомпрометиро	<ul> <li>Атака типа вrute-тогсе против КDP (С)</li> <li>Скомпрометированные учетные данные после RDP-атаки типа «brute-force» (С)</li> </ul>											
🚪 Сетевые службы	Автоматиче	ская реакц	ция										
🐼 VDI-среды	Реакция на рабочих	станциях	Сообщить и заблокировать RDP-атаки	~									
\land Мои оповещения	Реакция на серверах	( I	Сообщить и заблокировать RDP-атаки	~									
<b>БЕЗОПАСНОСТЬ</b>	Надежные IF	<b>b</b>											
Рабочие станции и серверы	RDP-атаки, исходящі	ие с этих IP-адрес	сов, не будут заблокированы, но о них буд	ет сообщено:									
Индикаторы атак (IOA)	Добавить IP-адрес												
Блокировка программ	Вы можете ввести не	есколько адресов	з (192.168.1.1) и диапазонов (192.168.1.1-19	2.168.1.254), раз,	деленных	запятой.							

# Компьютеры

### Закладка Обнаружения

- На странице со сведениями по компьютеру новая закладка Обнаружения показывает количество обнаруженных на нем вредоносных программ, ПНП, эксплойтов, уязвимостей и индикаторов атак, отфильтрованных по дате
- Закладка также показывает угрозы, обнаруженные антивирусом, а если у клиента имеются лицензии на модуль Patch Management, то еще и доступные патчи и программы на стадии End-of-Life
- Нажмите на элементы виджетов, связанных с индикаторами атак, чтобы открыть список
   Индикаторы атак, отфильтрованный по данному компьютеру



# Мои оповещения

#### Настройки оповещений

- На странице Настройки > Мои оповещения Вы можете включить опцию Индикаторы атак (IOA) для получения почтовых уведомлений при появлении индикатора атаки
- Получатель почтового оповещения сможет нажать на ссылку в письме, чтобы перейти на страницу со сведениями о данном индикаторе атаки в веб-консоли

0	Adaptive Defense 360	татус	компьютеры	настройки	задачи	демо	Bce
осно	овное				Почтовые оп	овещения	
8	Пользователи	Отп	равлять оповещен	ия в следующи	к случаях:		
~	Настройки компьютеров		13 I.C		12		
۲	Сетевые настройки	Обн Обн	аружения вредонос аружения эксплойт	сного ПО ов			
	Сетевые службы	Обн	аружения ПНП				
Ś	VDI-среды	Прог	грамма, ожидающа	я классификации,	заблокирована		
⊿	Мои оповещения	Про Фай,	граммы, заблокиро n, разрешенный ад	ванные админист министратором, с	гратором окончательно классифициро	ван	
		3a67	юкирован вредоно	сный URL			
6E3O	ПАСНОСТЬ	Обн	аружения фишинга				
Ţ	Рабочие станции и серверы	3a67	юкирована попытк	а вторжения			
ര	14	Забл	окированные устр	ойства			
۵	индикаторы атак (IOA)	Инд	икаторы атак (IOA)				
	Блокировка программ	Ком	пьютеры с ошибкая	ии защиты			
$\odot$	Разрешенное ПО	Ком	пьютеры без лицен	зии			
÷	Устройства Android	0ши	ібки установки		101		
88	Patch management	OOH	аруление неуправл	INCINCIO KOMILEIOTI	=ha		



#### Управление задачами

- В разделе Задачи теперь можно выбрать все задачи, чтобы затем отменить их или удалить
  - Вы должны сперва отменить задачу, чтобы потом можно было ее удалить

0	Adaptive Defense	360 СТАТУС	компьютеры	НАСТРОЙКИ	задачи	ДЕМО	🛅 Bce	Ç <b>9</b> {	3	8 drussian_feder	ration_c14 MO - Adaptiv
2	<u>च</u> Удалить 🛞	Отменить									4 выбрано 🗙
	Uninstall Interr           25.07.2021 в 17:0           Отменить	net Explorer 11 pat ОО Смотреть резул	ch from 6 computers Iьтаты	i						В ПРОЦЕССЕ	
	Install Google C           25.07.2021 в 17:0           Отменить	Chrome 39 patch or ОО Смотреть резул	n 6 computers Іьтаты							В ПРОЦЕССЕ	
	New task (Insta 25.07.2021 в 17:0           Отменить	all patches): Install 00 Смотреть резул	patches with the fo	llowing criticality	y					В ПРОЦЕССЕ	Ō
	Q New task: Scher 25.07.2021 в 17:0 Отменить	duled scan DD Смотреть резул	іьтаты							В ПРОЦЕССЕ	Ċ

#### Периодичность выполнения задачи

 Теперь при создании задачи по запланированной проверке или установке патчей Вы можете настроить выполнение задачи на определенный день недели или месяца

Adaptive Defense 36	О СТАТУС	компьютер	чы настройки	задачи		демо	Bce	Ç2	٩	8	drussian_federation_c14 DRUSSIAN DEMO - Adaptiv
Отменить				Новая	задача						Сохранить
Имя: Новая задача проверк	и										
Описание: Описание											
Получатели: Получатели по	ка не выбраны										
Запуск:	С Как можно ( 26.07.2021	быстрее	13:30 🗸 🔽 Локаль	ное время ко	мпьютера						
	Если компьюте	ер будет выклю	чен в запланирован	ный день/вре	мя, запустите задач	у как можно	быстрее в те	ечение:			
Максимальное время запуска: Периодичность	Нет предела Ежемесячно	~		•							
	● B 26	день каждого	) месяца								
	🔘 В 🛛 первый	й 🗸 Пон	едельник 🗸 кажд	ого месяца							

# Аругие улучшения в Aether

#### Подробные отчеты

- Теперь можно отправлять полный подробный отчет об активности ПО или вредоносного ПО
- Получатель почтового оповещения сможет нажать на ссылку в письме, чтобы перейти на страницу со сведениями о данном индикаторе атаки в веб-консоли

Max	Her				
VIM9:	HOE	ыи запланирован	ный отчет		
Отправлять	автоматиче	ески			
Каждый ме	сяц 🗸	День 1	~	в 11:00	~
Следующая	информаци	я			
Тип отчета:	Акти	вность вредонос	ного ПО		
	0				
	🥑 Св	одный отчет			
	• св О по	одный отчет лный отчет			
До:	● Св О По Добавить а	одный отчет лный отчет адрес эл. почты			
До: CC:	• Св по Добавить а Добавить а	одный отчет лный отчет адрес эл. почты адрес эл. почты			
До: СС: ВСС:	<ul> <li>Св</li> <li>По</li> <li>Добавить а</li> <li>Добавить а</li> </ul>	одный отчет лный отчет адрес эл. почты адрес эл. почты			
До: СС: ВСС: Тема:	● Св О по Добавить а Добавить а Добавить а Тема	одный отчет лный отчет адрес эл. почты адрес эл. почты			

#### Поиск в Моя организация

 В разделе Компьютеры в блоке Моя организация теперь можно осуществлять поиск по группам в дереве



#### Блокировка эксплойтов по умолчанию

- Теперь у новых клиентов, если в разделе Настройки > Рабочие станции и серверы включена Расширенная защита, то режим работы Анти-эксплойта по умолчанию устанавливается в Блокировка
- Также у опции Обнаруживать вредоносную активность (только для Linux) по умолчанию теперь устанавливается режим Блокировка

Отменить	Изменить настройки	Сохранит
Анти-эксплойт		
ATTI-SKCIDIOUT		
Антиэксплойтная защита не позво	оляет вредоносным программам использовать известные и неизвестные (ну ютерам в корпоративной сети	левого дня) уязвимости в
приложениях для доступа к компа	ютерам в корпоративной сети.	
-		
Анти-эксплойт 🧰		
Анти-эксплойт <b>сер</b> Режим работы (только для Windov	vs)	
Анти-эксплойт Режим работы (только для Windov Блокировка	vs)	
Анти-эксплойт Режим работы (только для Windov Блокировка Блокирует эксплойты. Иногда мож	vs) хет потребоваться завершение скомпрометированного процесса или переза	грузка компьютера.
Анти-эксплойт Режим работы (только для Window Блокировка Блокирует эксплойты. Иногда мож	vs) хет потребоваться завершение скомпрометированного процесса или переза	грузка компьютера.
Анти-эксплойт Режим работы (только для Window Блокировка Блокирует эксплойты. Иногда мож Сообщать пользователю компьют	vs) хет потребоваться завершение скомпрометированного процесса или переза тера о блокировке	грузка компьютера.
Анти-эксплойт Режим работы (только для Window Блокировка Блокирует эксплойты. Иногда мож Сообщать пользователю компьют Запросить у пользователя разреш	vs) сет потребоваться завершение скомпрометированного процесса или переза гера о блокировке вение на завершение скомпрометированного процесса (в некоторых случая	агрузка компьютера. х это может привести

#### Уведомления в веб-консоли

- В веб-консоли теперь могут публиковаться уведомления Panda Security, предназначенные для выборочных групп клиентов или пользователей определенных продуктов.
- Иконка уведомлений в виде звоночка показывается в панели инструментов в правом верхнем углу веб-консоли. В красном кружочке у этой иконке показывается количество новых уведомлений. При нажатии на иконку открывается окно со списком уведомлений



#### Уведомления

#### ×

#### What's New at WatchGuard

2021 Cybersecurity Predictions

Hello World!In 2021, how might hackers use automation, smart devices, Cloud computing, and more, to find a path to your data? In this year's cybersecurity predictions, we discuss how hackers might exploit vulnerabilities found in the gaps between people, their devices, and the corporate network.

#### ×

You have not yet updated your clients to Aether? Aether is a new platform of management that comes loaded with improvements and new modules that you can offer to your customers. Click here to know the advantages of Aether. Little by little we will update all our clients to this platform, through a update process automatic and very simple. Remember that you can control the process and update your clients from your Partner Center console, and offer them the new modules available on this platform, such as Patch Management, Panda Full Encryption and much more.

#### Уведомления по апгрейду продукта

- Когда доступна новая версия продукта, то в списке уведомлений показывается отдельное уведомление по апгрейду продукта.
  - Если пользователь веб-консоли обновит свою версию Aether, то все другие пользователи этого аккаунта (клиента) будут отключены от веб-консоли на период выполнения апгрейда

	Notifications ×
	×
	What's New at WatchGuard
-	2021 Cybersecurity Predictions
	Hello World In 2021, how might backers use automation, smart devices. Cloud
	computing, and more, to find a path to your data? In this year's cybersecurity
	predictions, we discuss how hackers might exploit vulnerabilities found in the gaps between people, their devices, and the corporate network.
	×
•	You have not yet updated your clients to Aether? Aether is a new platform of
	management that comes loaded with improvements and new modules that you can
	offer to your customers. Click here to know the advantages of Aether. Little by little we
	will update all our clients to this platform, through a <b>update process</b> automatic and very simple. Remember that <b>you can control the process and update your clients from your</b> <b>Partner Center console,</b> and offer them the new modules available on this platform, such as Patch Management, Panda Full Encryption and much more.
•	You can now request the update to the new version of Aether Platform. You can see the

### Заблокированные программы

- Если у Вас есть заблокированные программы, ожидающие классификации, то Вы можете удалить их из списка заблокированных программ в веб-консоли
  - Новый столбец Статус показывает файлы, которые не могут быть получены для классификации, и которые могут быть удалены из списка
  - Когда Вы удаляете программу из списка, это не влияет на уровень защиты
- Если программа запущена повторно, то она снова будет заблокирована
  - Когда файл поступит в Panda Security, он будет классифицирован сервисом Zero-Trust Application
- Список История заблокированных программ показывает также, какие программы были удалены из списка

#### ЗАБЛОКИРОВАННЫЕ ПРОГРАММЫ, ОЖИДАЮЩИЕ КЛАССИФИКАЦИИ



### Удаление заблокированной программы из списка

- Чтобы удалить заблокированную программу из списка:
- В разделе Статус > Безопасность нажлите на виджете Заблокированные программы, ожидающие классификации
- 2. В появившемся списке выберите программу, которую Вы хотите удалить
- 3. Нажмите кнопку **Удалить из списка** или в контекстном меню у данной программы выберите пункт **Удалить из списка**

<	Заблоки	ированные программы	, ожи	даюц	цие класс	ификации			:
Ī	У <mark>д</mark> алить из сп	иска						1 выбрано	×
	Компьютер	Путь	۸	۲	Режим защиты	Вероятность вредоносности	Статус	Дата 👃	
	WIN_DESKTOP _10	SYSTEM   \WinSxS\SOS.dll	0	•	Lock	Очень высокий	Невозможно получить файл	24.07.2021 21:20:00	
	WIN_LAPTOP_1	PROGRAM_FILES \WinRAR\Formats \7zxa.dll	•	0	Lock	Высокий	н п 🔟 Удали	іть из списка	•
	WIN_DESKTOP _3	DESKTOPDIRECTORY \worm.EXE	٠	0	Hardening	Высокий	Получение программы	24.07.2021 14:15:38	- 1
	WIN_SERVER_5	SYSTEM \spool\prtprocs\w32x86\T PWinPrn.dll	0	0	Lock	Высокий	Классификация	24.07.2021 13:13:52	:

### Интеграция Windows 10 AMSI

- Новый релиз XII платформы Aether включает более глубокую интеграцию с Windows 10 AMSI (Antimalware Scan Interface)
- AMSI предоставляет:
  - Телеметрию и дополнительную информацию о выполнении скриптов и макросов
  - Больше контекстных сведений для повышения уровня защиты

### Исключение модуля защиты Exchange

- Защита серверов Exchange перешла в режим End of Life, и теперь этот модуль исключен в аккаунтах новых клиентов
  - Обновленные аккаунты существующих клиентов пока еще видят модуль защиты Exchange и связанные с ним виджеты
  - Клиенты, у которых были настроены опции защиты Exchange до июля 2021, смогут ими пользоваться дальше до июня 2024 года

### Спасибо!