Информационная безопасность предприятия

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

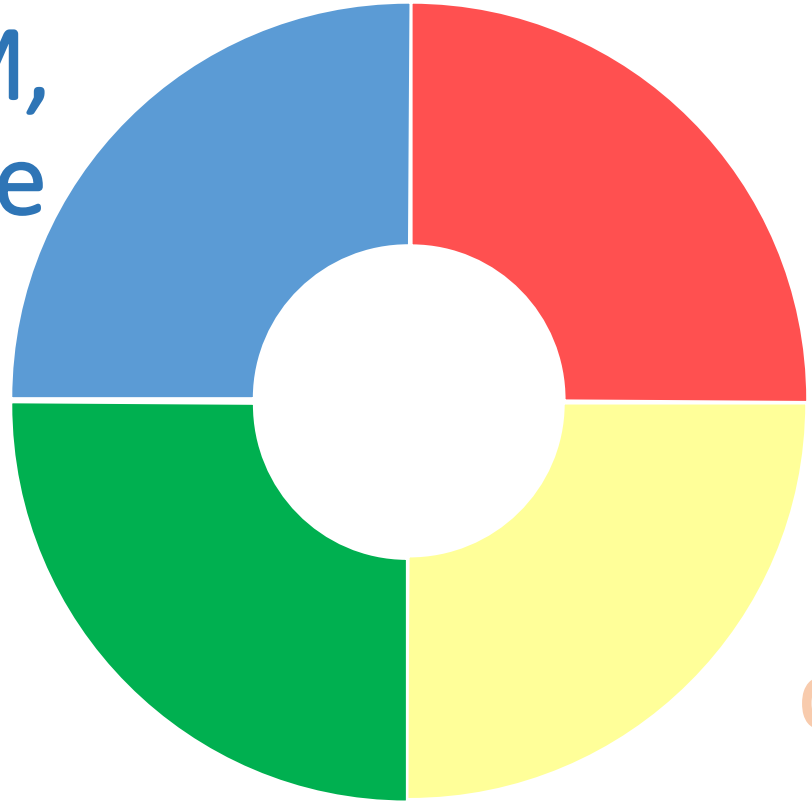
Современная модель угроз ИБ:

Угрозы	Пути проникновения	Методы борьбы	Раннее обнаружение
Кража, раскрытие данных	ОС, браузер, приложения	Шифрование данных, антивирус, Web-фильтры, фильтры приложений	Мониторинг, Анализ журналов, Управление закрытием уязвимостей, Тестирование
DDoS-атаки	Маршрутизаторы, Web-серверы, Коммутаторы, браузеры. Приложения, ОС	Устройства IPS, Web-фильтры	
Ботнеты	ОС, браузер, приложения, межсетевые экраны, приложения на клиентских устройствах	Защита DNS, фильтры приложений, антивирус, анти-ransomware	
Фишинг	ОС, браузер, приложения, межсетевые экраны, приложения на клиентских устройствах	Защита DNS, фильтры приложений, фильтры репутации	

Современная модель защиты:

Защита UTM, шифрование

Мониторинг модели безопасности

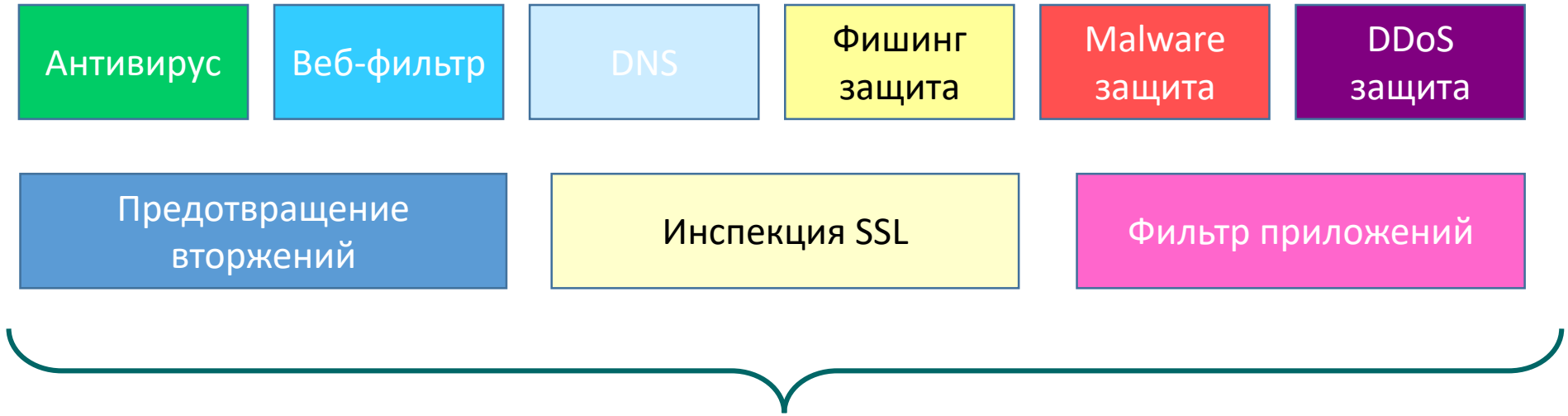


Поддержание актуальности модели безопасности

Контроль соответствия

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Unified Threat Management (UTM)



- ✓ Защита встроена в ASIC (реальный масштаб времени)
- ✓ Параллельная обработка данных

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

UTM: Антивирус

Ключевые особенности:

- ✓ Потоковый характер
- ✓ Фильтрация контента (DLP)
- ✓ Сервис репутации IP
- ✓ Вирусы, сетевые черви, трояны (включая архивы)
- ✓ Внешняя песочница (Sandbox)

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

UTM: Контроль приложений

Ключевые особенности:

- ✓ Блокировать отдельные службы (чат вконтакте)
- ✓ Сервис репутации IP
- ✓ Подключение внешней песочницы (Sandbox)

UTM: Предотвращение вторжений (IPS)

Ключевые особенности:

- ✓ Атаки нулевого дня
- ✓ Обнаружение вредоносного трафика и аномалий
- ✓ До 200 Гбит/с

UTM: Веб-фильтрация

Ключевые особенности:

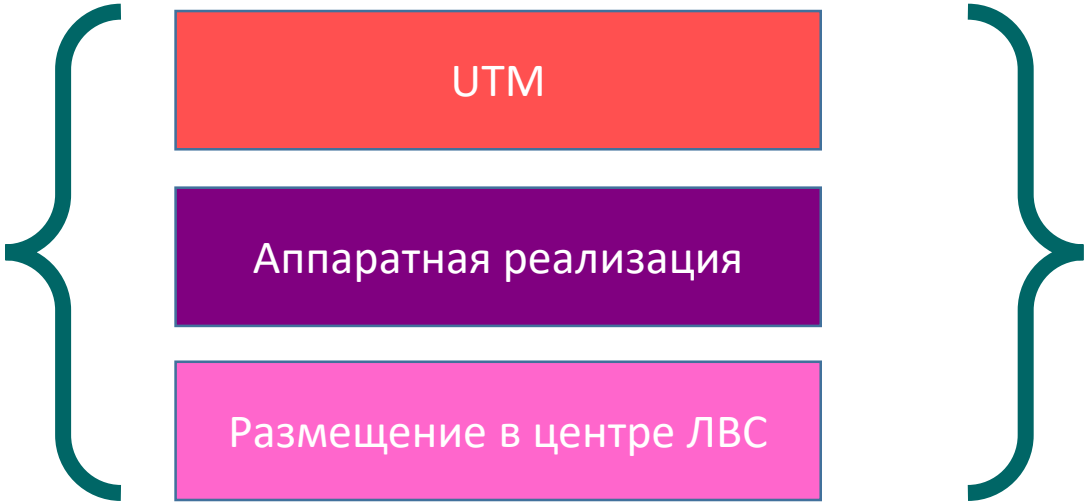
- ✓ Фильтрация по URL
- ✓ Фильтрация по содержимому
- ✓ Запрет использования анонимайзеров

UTM: Проверка SSL

Ключевые особенности:

- ✓ Инспекция дешифрованного трафика
- ✓ Возможность выбирать сайты для проверки

Межсетевой экран нового поколения (NGFW)



- ✓ Защита встроена в ASIC (реальный масштаб времени)
- ✓ Параллельная обработка данных

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Центр управления безопасностью

- ✓ Проверка клиентских устройств
- ✓ Управление уязвимостями
- ✓ Карантин, блокировка
- ✓ Анализ журналов
- ✓ Анализ характера и векторов атаки

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Проверка клиентских устройств (Endpoint Compliance)

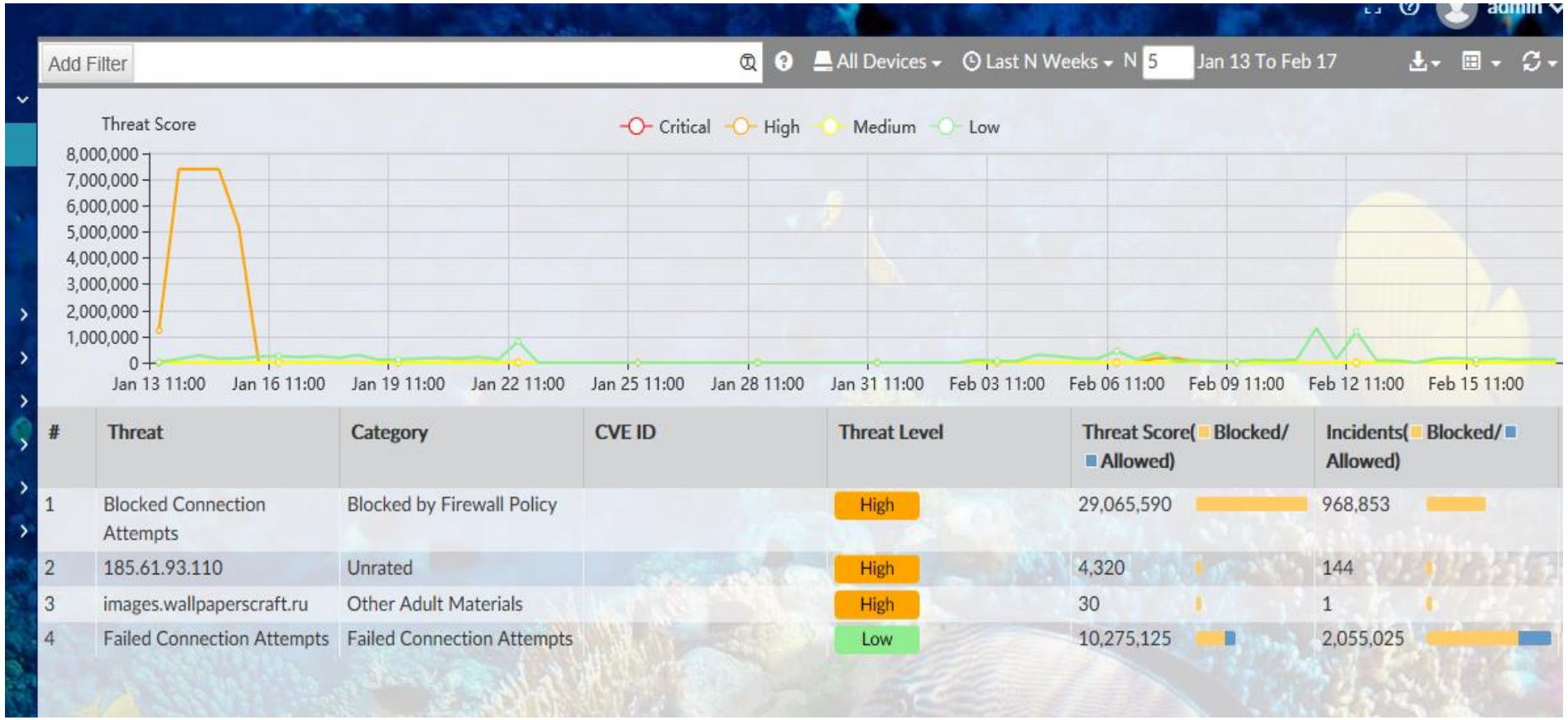
- ✓ Соответствие корпоративной политике безопасности
- ✓ Удаленное сканирование устройства
- ✓ Работает на Windows, IoS, Android, ARM

Мониторинг ИБ: FortiAnalyzer

- ✓ Сбор трафика и журналов
- ✓ Сбор информации с Forticlient
- ✓ Мониторинг угроз и уязвимостей
- ✓ Создание отчетов по безопасности

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

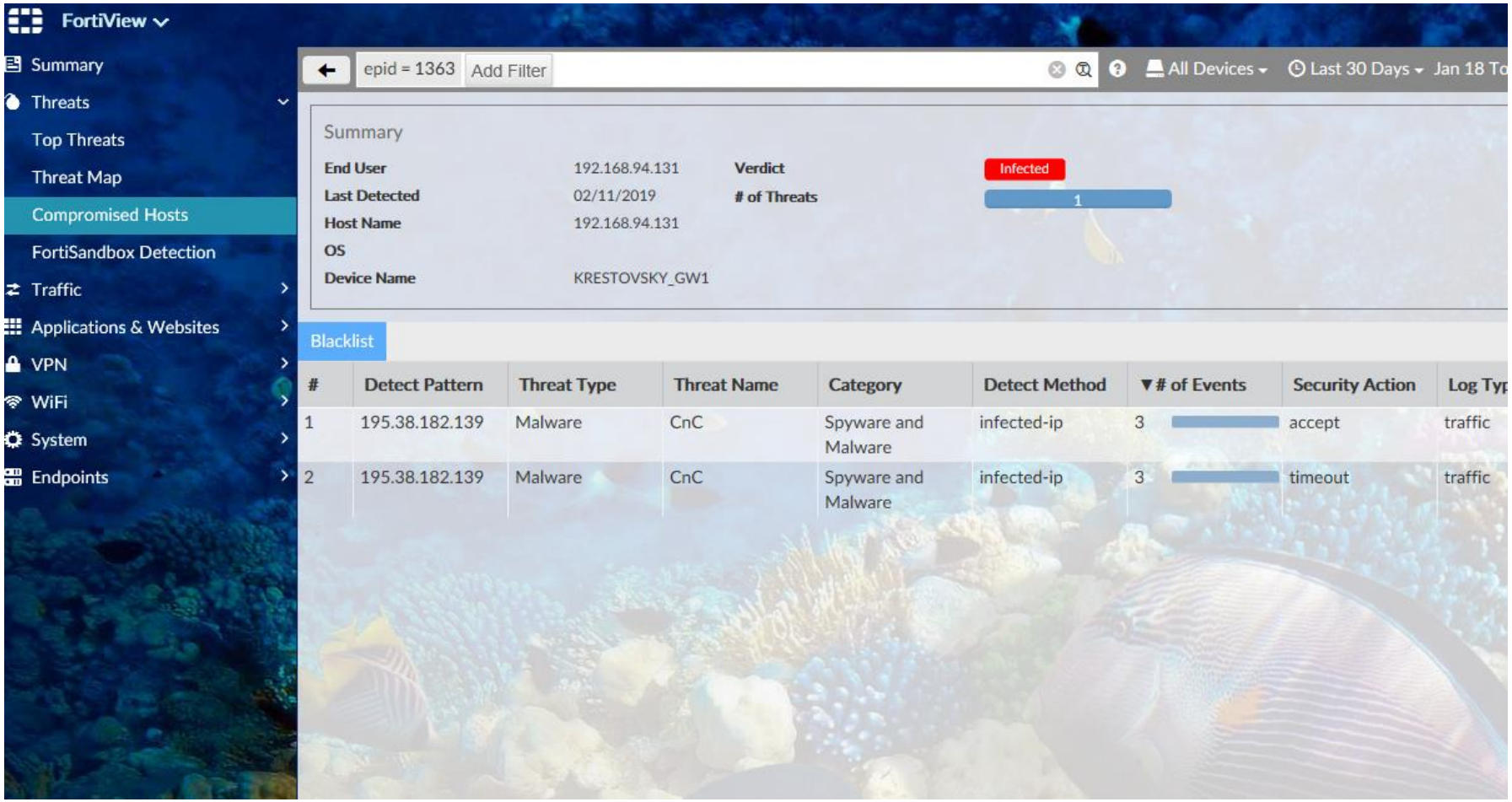
FortiAnalyzer: угрозы



#	Threat	Category	CVE ID	Threat Level	Threat Score(Blocked/ Allowed)	Incidents(Blocked/ Allowed)
1	Blocked Connection Attempts	Blocked by Firewall Policy		High	29,065,590	968,853
2	185.61.93.110	Unrated		High	4,320	144
3	images.wallpaperscraft.ru	Other Adult Materials		High	30	1
4	Failed Connection Attempts	Failed Connection Attempts		Low	10,275,125	2,055,025

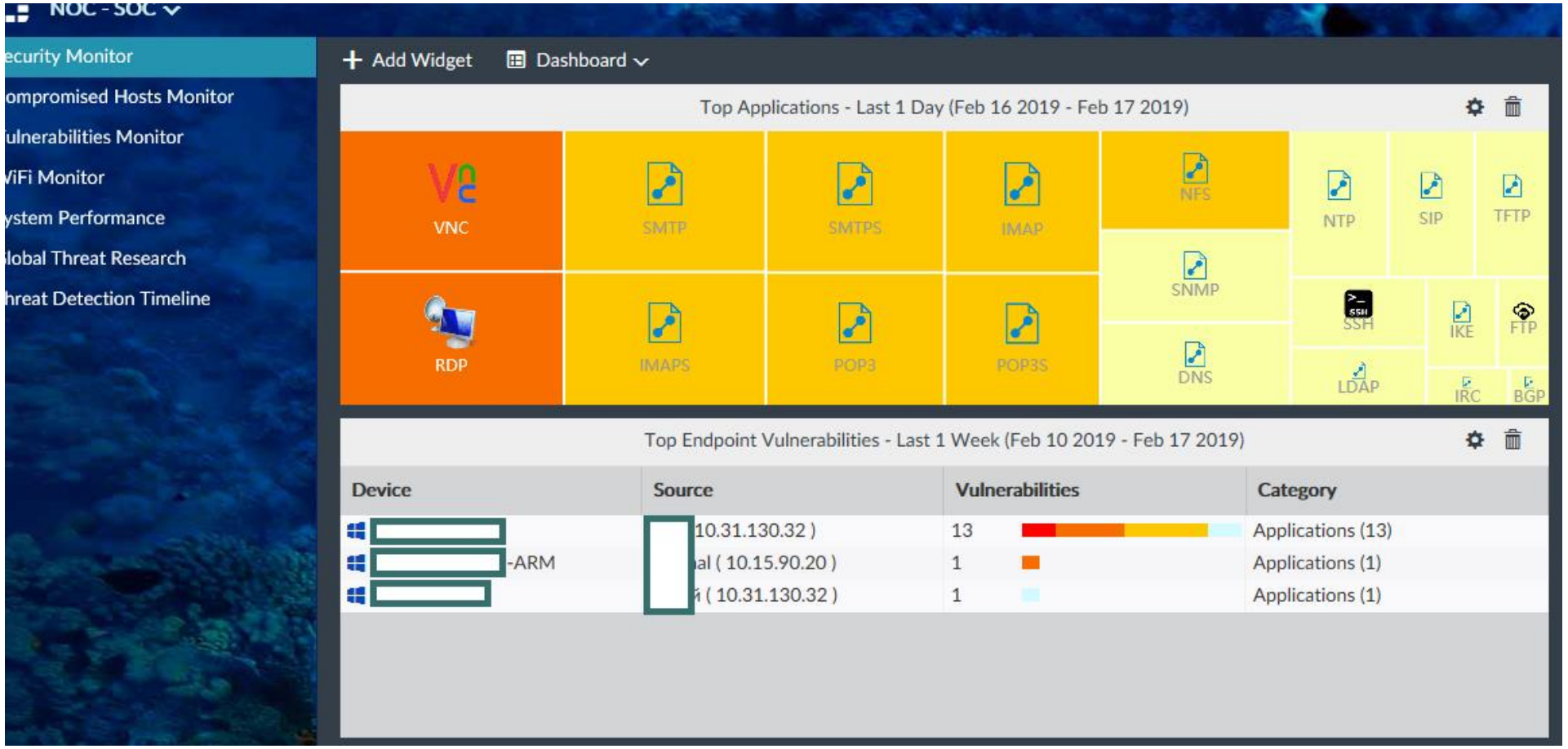
ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

FortiAnalyzer: инфицированные хосты



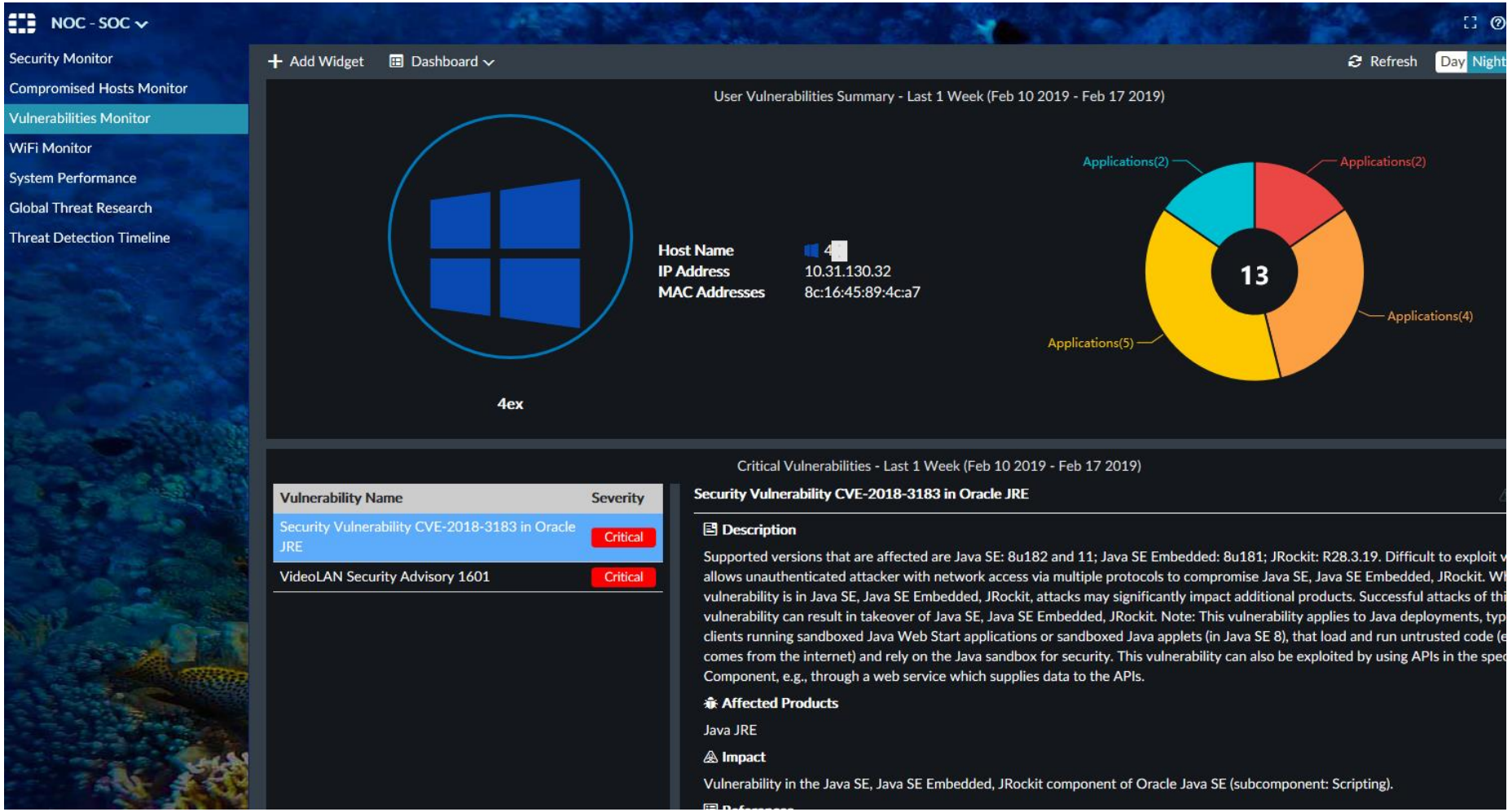
ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

FortiAnalyzer: инфицированные хосты



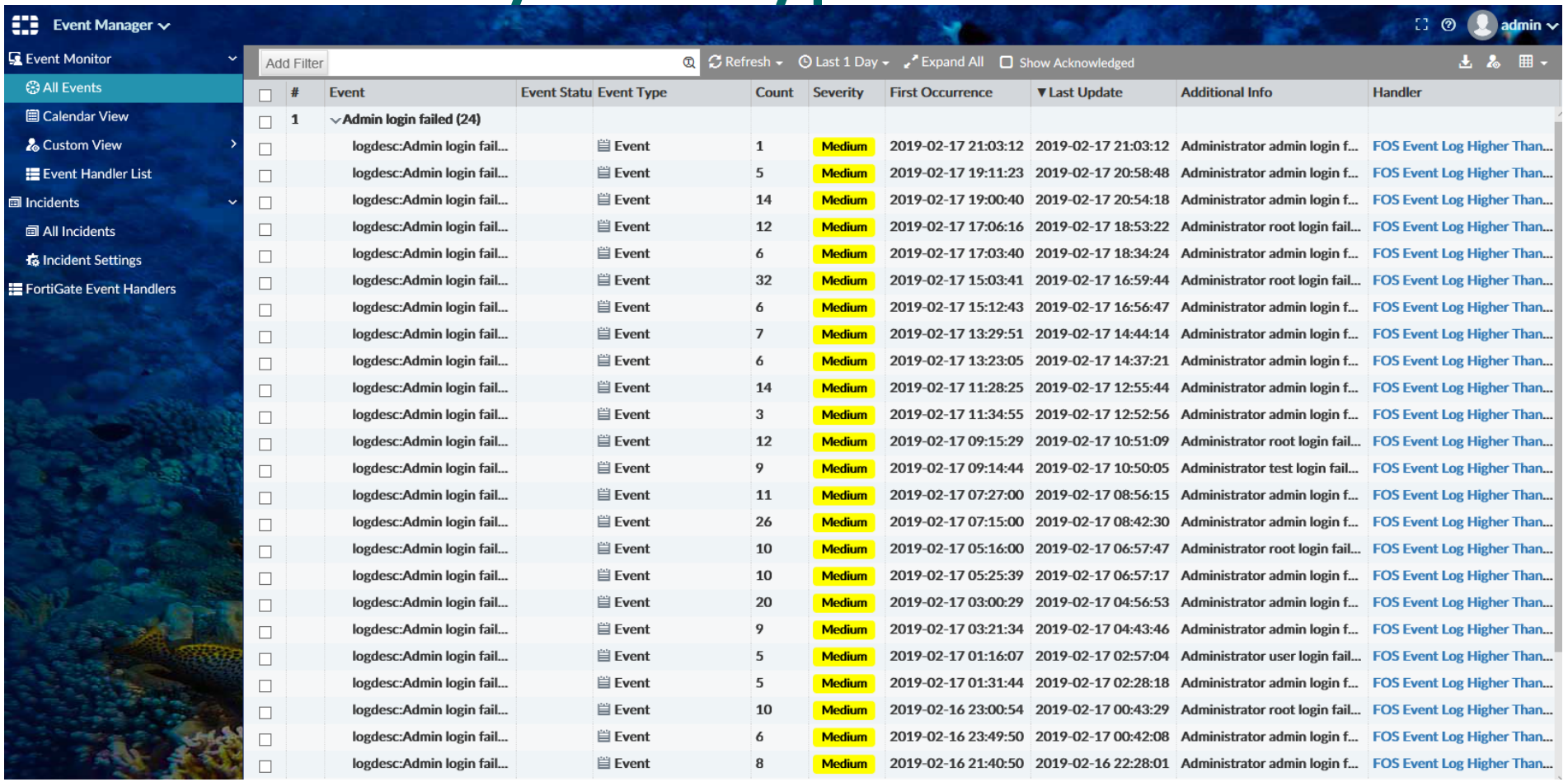
ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

FortiAnalyzer: уязвимости хостов



ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

FortiAnalyzer: журналы событий



#	Event	Event Statu	Event Type	Count	Severity	First Occurrence	▼Last Update	Additional Info	Handler
1	Admin login failed (24)								
	logdesc:Admin login fail...		Event	1	Medium	2019-02-17 21:03:12	2019-02-17 21:03:12	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	5	Medium	2019-02-17 19:11:23	2019-02-17 20:58:48	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	14	Medium	2019-02-17 19:00:40	2019-02-17 20:54:18	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	12	Medium	2019-02-17 17:06:16	2019-02-17 18:53:22	Administrator root login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	6	Medium	2019-02-17 17:03:40	2019-02-17 18:34:24	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	32	Medium	2019-02-17 15:03:41	2019-02-17 16:59:44	Administrator root login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	6	Medium	2019-02-17 15:12:43	2019-02-17 16:56:47	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	7	Medium	2019-02-17 13:29:51	2019-02-17 14:44:14	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	6	Medium	2019-02-17 13:23:05	2019-02-17 14:37:21	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	14	Medium	2019-02-17 11:28:25	2019-02-17 12:55:44	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	3	Medium	2019-02-17 11:34:55	2019-02-17 12:52:56	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	12	Medium	2019-02-17 09:15:29	2019-02-17 10:51:09	Administrator root login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	9	Medium	2019-02-17 09:14:44	2019-02-17 10:50:05	Administrator test login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	11	Medium	2019-02-17 07:27:00	2019-02-17 08:56:15	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	26	Medium	2019-02-17 07:15:00	2019-02-17 08:42:30	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	10	Medium	2019-02-17 05:16:00	2019-02-17 06:57:47	Administrator root login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	10	Medium	2019-02-17 05:25:39	2019-02-17 06:57:17	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	20	Medium	2019-02-17 03:00:29	2019-02-17 04:56:53	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	9	Medium	2019-02-17 03:21:34	2019-02-17 04:43:46	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	5	Medium	2019-02-17 01:16:07	2019-02-17 02:57:04	Administrator user login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	5	Medium	2019-02-17 01:31:44	2019-02-17 02:28:18	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	10	Medium	2019-02-16 23:00:54	2019-02-17 00:43:29	Administrator root login fail...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	6	Medium	2019-02-16 23:49:50	2019-02-17 00:42:08	Administrator admin login f...	FOS Event Log Higher Than...
	logdesc:Admin login fail...		Event	8	Medium	2019-02-16 21:40:50	2019-02-16 22:28:01	Administrator admin login f...	FOS Event Log Higher Than...

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

FortiAnalyzer: настраиваемые отчеты

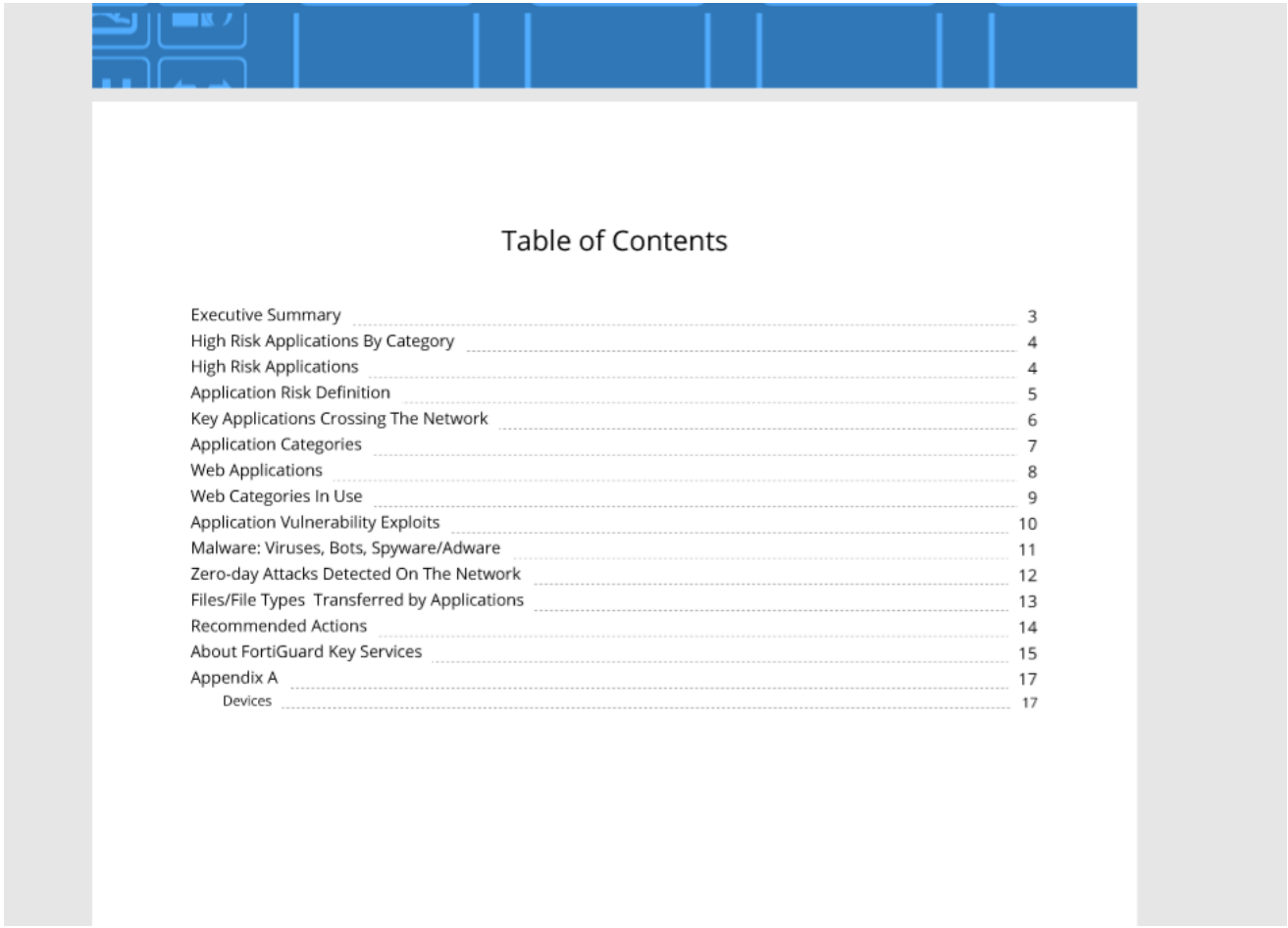


Table of Contents

FortiAnalyzer: Соответствие политике безопасности

Функция Compliance – проверка правил работы в сети:

- ✓ Правильные версии ПО и обновления
- ✓ Веб-фильтрация трафика
- ✓ Фильтрация UTM
- ✓ Встроенный клиент VPN
- ✓ Защита от эксплойтов


ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

ООО «Оптимал Системс»

Ключевые особенности:

- ✓ Концентрация на высокотехнологичных проектах
- ✓ Оптимизация расходов заказчика
- ✓ Быстрота реагирования
- ✓ Клиентоориентированность

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Деятельность

- ✓Строительство информационных систем:
  - ✓Проектирование
  - ✓Монтаж
  - ✓Поддержка
  - ✓Генподряд

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Системы

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Работа с лидерами рынка

Gartner MQ’18 – межсетевые экраны нового поколения (NGFW)

- ✓ Fortinet
- ✓ Cisco
- ✓ Check Point

Gartner MQ’18 – Защита оконечных устройств

- ✓ Palo Alto
- ✓ Fortinet
- ✓ Cisco
- ✓ Check Point

ООО Оптимал Системс ОГРН 1167746349088 ИНН 9701037157 / КПП 774301001. 125212, Россия, Москва, Кронштадтский бульвар, д. 7А, офис 511. Тел. +79096914151 +7915-OPTIMAL. Web: http://optimal.systems. Web: http://optimal-systems.ru. E-mail: info@optimal.systems.

Контакты

- ✓+7 909 691 41 51
- ✓+7 915 OPTIMAL
- ✓info@optimal.systems
- ✓Web: https://optimal.systems
- ✓Facebook: https://www.facebook.com/optimal.systems.moscow/