SOC FORUM 2023

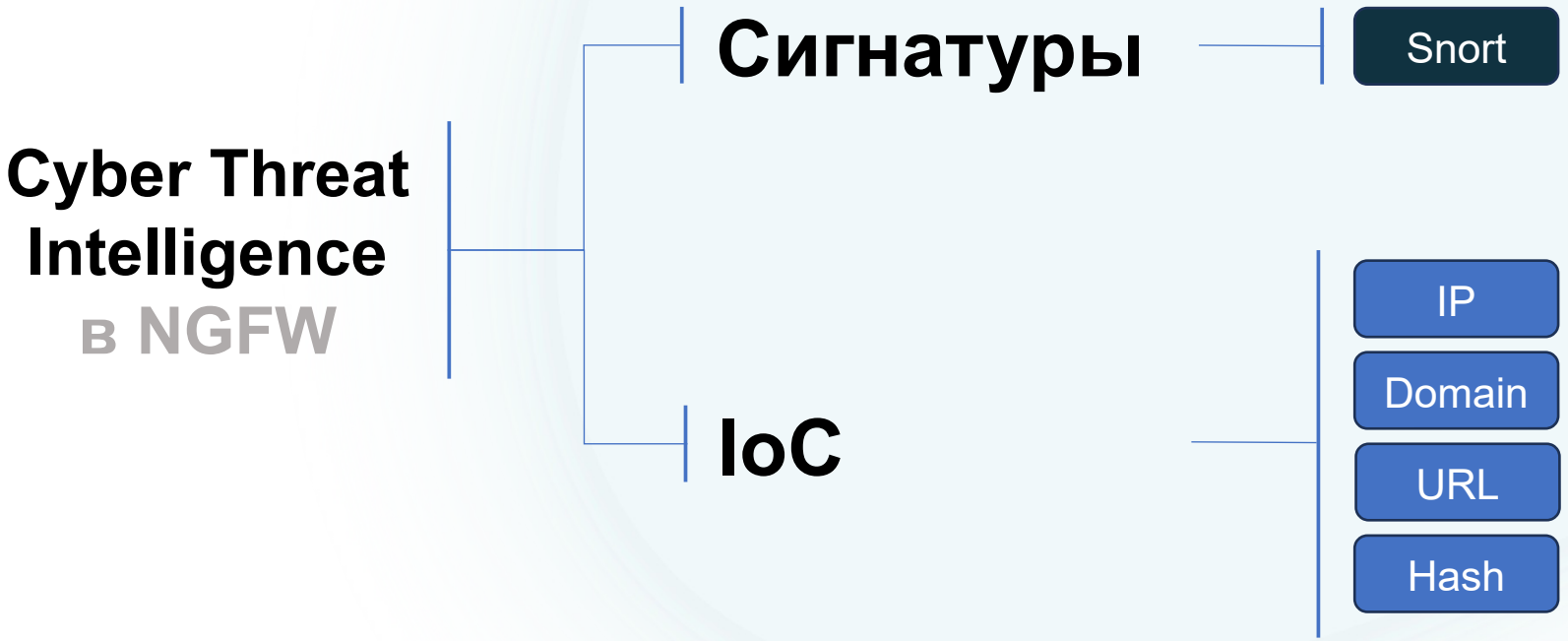
Плюсы и минусы заливки индикаторов компрометации на межсетевой экран

Николай Арефьев
Генеральный директор ООО "Технологии киберугроз" (бренд RST Cloud)

RST CLOUD
ТЕХНОЛОГИИ КИБЕРУГРОЗ

Виды CTI в NGFW

SOC FORUM 2023



Что поможет выявить CTI

SOC FORUM 2023

№	Тактика	Типы IoC	IoC в NGFW
TA0043	**Reconnaissance**	IP	• Сканирование портов • Поиск уязвимостей • Подбор паролей • Анонимайзеры
TA0042 TA0001	**Resource Development** **Initial Access**	IP Domain URL	• Фишинг • Ботнеты • Ресурсы с ВПО • Скомпрометированные ресурсы
		Hash	• ВПО • Хакерские утилиты
TA0008	**Lateral Movement**	Hash	• Хакерские утилиты
TA0011	**Command and Control**	IP Domain URL	• Управляющие сервера
TA0010	**Exfiltration**	IP Domain URL	• Ресурсы для выгрузки данных
TA0040	**Impact**	IP	• **DDoS** • **Ботнеты**

Что поможет выявить CTI

SOC FORUM 2023

№	Тактика	Сигнатуры в NGFW
TA0002	**Execution**	Правила для сигнатурного анализа (чаще всего в формате SNORT)
TA0003	**Persistence**	
TA0004	**Privilege Escalation**	
TA0005	**Defense Evasion**	
TA0006	**Credential Access**	
TA0007	**Discovery**	
TA0009	**Collection**	

Подход к работе с CTI в NGFW

SOC FORUM 2023

SOC FORUM 2023

Выводы

Польза

- **Позволяет блокировать угрозы на ранних и даже на финальных этапах.**
- Оперативное выявление новых угроз.

Сложности

- **Высокие требования к качеству CTI.**
- Нельзя использовать весь поток CTI от поставщика "как есть". Необходима предварительная подготовка, с учетом ограничений NGFW.
- Предварительную подготовку делает либо сам клиент, либо поставщик CTI.

SOC FORUM 2023

info@cyberthreattech.ru

RST CLOUD

ТЕХНОЛОГИИ КИБЕРУГРОЗ