АРПП
Отечественный софт

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

05.06.2024 г. № АИ-1410/06-24

Директору
ФСТЭК России

В.В. СЕЛИНУ

О разработке требований

Уважаемый Владимир Викторович!

К 2024 году СЗИ типа средств управления киберинцидентами, средств анализа киберугроз, средств управления процессами кибербезопасности заняли свое место в общей системе кибербезопасности. Сформировались как отдельные классы систем. Однако отдельных требований по безопасности к системам данного класса пока нет.

Перечисленные средства защиты позволяют решать следующие задачи:

1) Средства управления киберинцидентами (международная классификация: SOAR - Security Orchestration, Automation and Response, IRP - Incident Response Platform) предназначены для централизованной координации и управления (оркестровки) средствами защиты информации, автоматизации всех этапов реагирования на инциденты ИБ (выявление, анализ, локализация, устранение инцидента, восстановление после инцидента, выполнение пост-инцидентных действий), роботизации действий специалистов по реагированию, управления событиями / инцидентами ИБ, активами и уязвимостями, автоматизации обмена информацией с регуляторами (НКЦКИ, ФинЦЕРТ).

2) Средства анализа киберугроз (международная классификация: TIP - Threat Intelligence Platform, UEBA - User and Entity Behavior Analytics) предназначены для сбора и обработки аналитических данных о киберугрозах (кибербразведка), обнаружения киберугроз с применением технологий поведенческого анализа, выявления аномалий и машинного обучения.

3) Средства управления процессами кибербезопасности (международная классификация: SGRC - Security Governance, Risk Management and Compliance; GRC - Governance, Risk Management and Compliance) предназначены для автоматизации управления кибербезопасностью (AM, CMDB, VM, VS, BCP, Audit, Report), киберрисками (RM, ORM, включая операционные риски по 716-П ЦБ РФ) и соответствием законодательству (требованиям НПА, включая 187-ФЗ, приказы ФСТЭК России и др.) и стандартам (СМ, ISO, NIST, ГОСТ и др.).

Основными производителями подобных решений являются:

- Security Vision: продукты Security Vision IRP | SOAR | NG-SOAR, Security Vision GRC | SGRC | Auto-SGRC | Auto-Compliance, Security Vision TIP | UEBA | AD+ML;

- Kaspersky: продукт Kaspersky CyberTrace (TIP);
- Positive Technologies: продукт PT Cybersecurity Intelligence (TIP);
- ePlat4m: ePlat4m SGRC;
- R-Vision: продукты R-Vision IRP | SOAR | SGRC | TIP;
- UserGate: продукт UserGate LogAnalyzer (IRP);
- InfoWatch ARMA.

Перечисленными продуктами пользуются крупнейшие государственные учреждения (министерства, ведомства, силовые структуры), банки, организации промышленности и здравоохранения, образовательные учреждения, ритейл, телекоммуникационные компании - в целом, более половины компаний из перечня крупнейших компаний России. Большинство данных решений входят в Единый реестр российских программ для электронных вычислительных машин и баз данных Минцифры России. Некоторые из данных решений также сертифицированы ФСТЭК России по различным уровням доверия в соответствии с документом "Требования по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий", утвержденным приказом ФСТЭК России №76 от 02.06.2020 г.

На основе этого документа **сейчас выпускаются требования по безопасности информации для других типов СЗИ**, например, "Требования по безопасности информации к средствам контейнеризации" (утверждены приказом ФСТЭК России от 04.07.2022 г. № 118), "Требования по безопасности информации к средствам виртуализации" (утверждены приказом ФСТЭК России от 27.10.2022 г. № 187), "Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети" (утверждены приказом ФСТЭК России от 07.03.2023 г. № 44), "Требования по безопасности информации к системам управления базами данных" (утверждены приказом ФСТЭК России от 14.04.2023 г. № 64).

В данных документах вводятся классы защиты соответствующих СЗИ, устанавливается соответствие классов защиты уровням доверия, обозначаются требования к реализуемым СЗИ функциям безопасности, а также устанавливаются требования по применению СЗИ определенных классов защиты для обеспечения кибербезопасности объектов различных категорий значимости / классов защищенности / уровней защищенности ПДн для КИИ, ГИС, АСУТП, ИСПДн. Таким образом, у производителей других типов СЗИ появился четкий перечень требований, которые надо реализовать для соответствия их продукта тому или иному классу защиты и для последующей сертификации в системе ФСТЭК России, а у потребителей

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

появились более понятные критерии для выбора СЗИ в зависимости от типа и уровня критичности защищаемого объекта и обрабатываемой информации.

АРПП «Отечественный софт» обращается к Вам с просьбой обеспечить разработку аналогичных требований по безопасности информации для:

1. Средств управления киберинцидентами: IRP | SOAR | NG SOAR;
2. Средств анализа киберугроз: TIP | UEBA | AD+ML;
3. Средств управления процессами кибербезопасности: GRC | SGRC | Auto-SGRC | Auto-Compliance.

Со своей стороны, готовы присоединиться к разработке соответствующих документов и участвовать в формировании перечня реализуемых данными средствами функций безопасности. Данные документы, при их разработке, обеспечат систематизацию и упорядочивание требований для соответствующих типов СЗИ и их функций безопасности, необходимых для обеспечения защиты объектов КИИ, ГИС, АСУТП, ИСПДн.

СПРАВОЧНО:

АРПП «Отечественный софт» учреждена в 2009 году крупнейшими российскими разработчиками тиражируемого программного обеспечения. В настоящее время в Ассоциацию входит более 280 ИТ-компаний с совокупным оборотом свыше 270 млрд рублей. Приоритетными направлениями работы Ассоциации являются формирование предложений для создания благоприятных условий развития отечественной ИТ-отрасли, импортозамещение и поддержка экспорта отечественного ПО, а также разработка совместных отечественных решений и их дальнейшее продвижение.

В составе Ассоциации образованы и на регулярной основе действуют 13-ть комитетов: Комитет по интеграции российского ПО; Комитет по экспорту российского ПО; Комитет по информатизации образования; Комитет по развитию финансирования ИТ-отрасли; **Комитет по информационной безопасности;** Комитет по цифровой трансформации; Комитет по искусственному интеллекту; Комитет по телекоммуникациям; Комитет по информационному моделированию градостроительной деятельности; Комитет по информатизации здравоохранения; Промышленной автоматизации; Правовой комитет и Комитет по развитию экосистемы российских мобильных продуктов.

С уважением,

Исполнительный директор
АРПП «Отечественный софт» Лашин Р.Л.