Инструмент поддерживает API различных платформ, что упрощает интеграцию в существующие системы безопасности.

Исследователи в области кибербезопасности представили новый инструмент под названием Pythia, предназначенный для поиска и обнаружения вредоносной инфраструктуры. Pythia предлагает стандартизированный формат запросов, который легко конвертируется для использования на различных платформах поиска инфраструктуры.

Основная цель Pythia – помочь специалистам по безопасности в поиске потенциально вредоносных активов до того, как они будут использованы злоумышленниками. Это особенно актуально в современных условиях, когда срок жизни традиционных индикаторов компрометации (IoC) сокращается, а киберпреступники все чаще используют автоматизированное развертывание множества инфраструктур.

Pythia позволяет исследователям создавать запросы в едином формате, а затем легко конвертировать их для использования на таких платформах, как Shodan, Censys, FOFA, BinaryEdge, ZoomEye и Hunter. Это значительно упрощает процесс валидации и обогащения результатов поиска.

Ключевые особенности Pythia:

Формат запросов Pythia включает такие поля, как заголовок, уникальный идентификатор, статус, описание, ссылки, теги, автор и дата создания. Сам запрос состоит из параметров (поле-значение) и условий, объединяющих параметры логическими операторами.

Разработчики Pythia подчеркивают, что инструмент находится на стадии бета-тестирования и приглашают сообщество к участию в его развитии. В будущем планируется расширение поддерживаемых платформ и пополнение базы запросов.

Pythia может стать важным дополнением к существующим инструментам кибербезопасности, таким как Snort для сетевого трафика, YARA для файлов и Sigma для лог-файлов. Использование Pythia позволит исследователям более эффективно выявлять потенциальные угрозы и предотвращать атаки на ранних стадиях.

Для начала работы с Pythia достаточно клонировать репозиторий с GitHub, установить зависимости и запустить инструмент с помощью командной строки. Разработчики также предоставляют подробную документацию по созданию запросов и

использованию различных функций Pythia.