ANALYTICAL OVERVIEW OF THE SOAR PLATFORMS

Gracheva Iu.V., Vayts V.L., Rudik K.P.

Previously, the authors have overviewed the global market of the SOAR systems. Modern automation systems for responding to information security incidents were analyzed. Also, the relevance of this class of solutions was shown and a large number of various products were presented. This document provides an analytical overview of well-known commercial solutions of the IRP/SOAR class from domestic and foreign vendors offering their products in Russia. The products were analyzed based on their general and technical features as well as functionalities. The great capabilities of ERP/SAP solutions for automating the processing of cyber incidents and performing related actions (analytics, correlation, visualization), including Machine Learning, Artificial Intelligence, and Big Data, are demonstrated. Conclusions are drawn for each section.

Comparison criteria	**IBM Security SOAR Version 40 (USA)**	**PaloAlto Cortex XSOAR Version 6.1 (USA)**	**Siemplify Version 5.5.3 (Israel)**	**R—Vision IRP Version 4.5 (Russia)**	**Security Vision IRP/SOAR Version 5.0.0 (Russia)**
1. Comparison of general and technical characteristics					
1.1. Software requirements					
Delivery option	Installation on-premise and in the cloud infrastructure (IBM Cloud OS 2 Type 2, compliance with ISO 27001, 27017, 27018).	Local installation on virtual and physical infrastructures, as well as using Docker. Installation on the Azure, AWS cloud.	Support for installation in cloud infrastructure, on-prem, on virtual infrastructure.	Software appliance, it is possible to deploy on physical servers. In case of low estimated loads, there is an option to place all components in the All-in-one mode (on one server).	Software appliance, it is possible to deploy on physical servers. In case of low estimated loads, there is an option to place all components in the All-in-one mode (on one server).
Virtualization environments	VMware 6.0 or later.	VMware.	VMware.	VMware, VirtualBox, Hyper-V, Xen, Parallels.	VMware, VirtualBox, Hyper-V, Xen, Parallels, KVM.
Solution components	DBMS server, web server.	Cortex XSOAR Server, Cortex XSOAR Engine.	DBMS server, web server.	Management server, DBMS server (can be combined with the management server), central collector, inventory collector.	Management server, DBMS server, connector services (connectors to data sources and response connectors),

					monitoring service (optional, for the High Availability mode).
OS	RHEL 7.4-7.7 or later.	Cortex XSOAR Server: CentOS (7.x and later), Ubuntu (16.04 and later), RHEL (7.x and later), Oracle Linux (7.x) Cortex XOR Engine Server: Windows, MacOS, Linux.	CentOS 7.8.	Management server, collectors: CentOS 7, RHEL 7, Astra Linux CE 2.12, AltLinux Alt 8 SP. DBMS Server: Ubuntu 14/16, CentOS 7, RHEL 7, Windows Server 2012/2016, FreeBSD 11.	Management server, connector services, monitoring service: Microsoft Windows Server 2012R2 and later, CentOS 7 and later, RHEL 7 and later, Ubuntu 14 and later, Astra Linux CE, AltLinux, Alt. DBMS Server: Microsoft Windows Server 2012R2 and later, CentOS 7 and later, RHEL 7 and later, Ubuntu 14 and later, FreeBSD 11 and later, Astra Linux CE, AltLinux, Alt.
DBMS	PostgreSQL.	Elasticsearch.	PostgreSQL, Elasticsearch.	PostgreSQL v10 and later.	MS SQL (SQL Server 2016 and later), PostgreSQL 9.5 and later.
Customer software	Web browser.	Web browser.	Web browser.	Web browser.	Web browser.
1.2. Customer hardware and infrastructure requirements					
CPU architecture	Any that supports the server OS.	Any that supports the server OS.	Any that supports the server OS.	Any that supports the server OS.	Any that supports the server OS.

Hardware	Platform: 4 CPU 16 GB RAM 100 GB disk subsystem.	Cortex XSOAR Server: 8 CPU 16 GB RAM 500 GB disk subsystem. Cortex XOR Engine Server: 8 CPU 16 GB RAM 20 GB disk subsystem.	12 CPU 32 GB RAM 800 GB disk subsystem.	Depending on the number of assets, response scripts, system users: Management server: 1–22 CPUs 8 – 32 GB RAM DBMS Server: 1 – 16 CPUs 8 – 24 GB RAM Collector (recommended parameters): 4 CPU 8 GB RAM	Depending on the number of incidents and response scripts. Management server: 1-12 CPUs 4-16 GB RAM DBMS Server: 1-16 CPUs 4-16 GB RAM Connector services, monitoring service: 1-2 CPUs 2-4 GB RAM
Support for geographically distributed placement	Yes.	Yes, with the help of agents.	Yes, with the help of agents.	Yes.	Yes.
The ability to install updates without access to the Internet	Yes.	No.	Yes.	Yes.	Yes.
Application architecture	Microservice.	Microservice.	Monolithic.	Monolithic.	Microservice.
1.3. Ease of use, administration					
Documentation	Provided on the website.	Provided on the website.	Provided on the website.	Provided as contextual HTML help and as a separate document.	Provided as contextual HTML help and as a separate document.
Documentation language	English.	English.	English.	Russian, English.	Russian, English.

Interface language	Multilingual support. Russian language support — interface, objects, incident fields.	English.	English.	Russian, English.	Russian, English, multilingual support (the ability to add any languages).
Design themes	It is possible to configure.	Light, dark.	Light, dark.	Light, dark.	Light, dark.
Granted access rights to the OS on which the solutions are deployed	Full access rights.	Full access rights.	Full access rights.	Full access rights.	Full access rights.
Solution user authentication methods	LDAP, SAML, two-factor authentication support (the Duo authentication provider).	LDAP, SAML, using the Duo, Okta, Microsoft Azure, Microsoft ADFS authentication providers.	LDAP (Active Directory), SAML, using the Okta and G-Suite authentication providers; support for connecting a custom authentication provider.	Domain authentication (NTLM, Kerberos), built-in authentication. Note: domain authentication requires preliminary configuration using the Linux terminal, since the management server is running Linux.	Domain authentication (NTLM, Kerberos and including SSO), Radius authentication, built-in authentication. Note: Support for assigning roles to system users based on group memberships in Active Directory.
Configuring networking	The final list of required protocols and ports.	The final list of required protocols and ports.	The final list of required protocols and ports.	The final list of required protocols and ports, iptables configuration is done using the Linux terminal.	The final list of required protocols and ports, the configuration of the Windows firewall is done using the GUI or command line. The iptables configuration

					is done using the Linux terminal.
Search for all objects from a single interface	Search in all objects, a filter by object type, using search string operators, support for Elasticsearch search queries (the product uses the Elasticsearch search and analytical engine).	Search for specific object types or all data in the system, including using the Regex expressions and Apache Lucene query syntax. Search by tags in the system.	Using filters in search; searching by cases, entities, exporting found information to CSV. The ability to tag events and cases and further search with tags.	Search for all elements, incl. linked.	Global search for all objects.
Personal API	RESTful API.	RESTful API.	HTTP Rest API.	REST API.	REST API.
1.4. Differentiation of access rights to the system					
Access control model	Role-based access control Creation of custom roles. API access rights are granted to authenticated entities (API key accounts) that have an active internal Resilient account and the required access rights.	Role-based access control Creation of custom roles.	Role-based access control Creation of custom roles. Setting access rights for users and API keys.	Role-based access control System roles: access to sections of the system for reading or changing, for example: Administrator, User, Risk Manager, etc. Special roles: access to individual elements of the system, for example: Asset owner, Security administrator, Security auditor, etc.	Role-based access control Customizable roles based on object attributes. Differentiation of access to all system objects and the assignment of rights to read, modify, create, perform group operations for a specific user / group. Differentiation of access to the content of cards (to any field)

					depending on the current state in the workflow. Permissions are built on the "Module – Access Object – Access Right – Policy" principle.
Granular access support	Yes.	Yes.	Yes.	The ability to create custom roles with permissions to perform certain actions with certain objects, group users, and assign them roles.	The ability to create custom roles with permissions to perform certain actions with certain objects, group users, and assign them roles. The "Workflow" functionality allows defining the order of interaction with any logical object (incident, asset, vulnerability, task, etc.) of various user groups, including those depending on the current state and values of the object's properties, taking into account the roles and rights of users.
1.5. Logging					

Log of user actions	The history of actions of users and administrators is logged.	The history of actions of users and administrators is logged.	The history of actions of users and administrators is logged.	The history of actions of users and administrators in all modules is logged, including the export of log data and sending it via syslog.	The history of user and administrator actions in all modules is logged, including sending activity information to email, syslog, and SNMP.
Logging actions with objects	Yes, user actions.	Yes, user actions.	Yes, user actions.	The history of changes to all elements is logged (changing the value of fields, actions with elements, adding objects).	The history of changes to all objects (changes to properties, workflow states, completed transactions) is logged while the old and new values of the changed property are preserved.
Monitoring solution performance	Logging by means of the system and OS.	Logging by means of the system and OS.	Logging by means of the system and OS.	Logging by means of OS (text files), logging by writing events to the database.	Logging by means of OS (Windows Application log, text files), logging by writing events to the database.
1.6. Security					
Secure communication between solution components	Use of the SSL/TLS protocols.	Use of the SSL/TLS protocols.	Use of the SSL/TLS protocols.	The use of the SSL/TLS protocols and ability to authenticate with certificates between all system components, the use of certificates issued by a Certificate	The use of the SSL/TLS protocols and ability to authenticate with certificates between all system components, the use of certificates issued by a Certificate

				Authority/ Certification authority (CA). Note: PKI is configured using the Linux console.	Authority/ Certification authority (CA).
Protecting user access to the web interface	Access to the web interface via HTTPS.	Access to the web interface via HTTPS.	Access to the web interface via HTTPS.	Access to the web interface via HTTP/HTTPS, using the TLS 1.2 protocol	Access to the web interface via HTTPS, using the TLS 1.2 protocol, the ability to restrict the IP addresses that are allowed access.
Setting the web session timeout	Yes.	Yes.	Yes.	Yes.	Yes.
Setting password complexity and expiration (when using built-in authentication)	Yes.	Yes.	Yes.	Yes.	Yes.
Account lockout in case of unsuccessful authentication attempts	Yes.	Yes.	Yes.	Yes.	Yes.
Two-factor user authentication	Yes, using authentication providers.	Yes, using authentication providers.	Yes, using authentication providers.	Yes, according to certificates.	Yes, according to certificates.
Restricting access to the solution at the network level	No, only using OS.	No, only using OS.	No, only using OS.	No, only using OS (via iptables manually via the Linux console).	Yes, via the web interface: permission to access the system only from certain IP

					addresses, IP address ranges, subnets.
1.7. Licensing					
License cost	Individual modules can be licensed additionally (MSSP add-on, Privacy add-on).	It depends on the functionality, type of subscription, number of users, operators, number of connectors, validity period and type of technical support purchased.	It depends on the functionality, type of subscription, number of users, operators, number of connectors, validity period and type of technical support purchased.	It depends on the functionality, total number of assets, number of users, number of connectors, customization of the solution for a specific Customer, and duration of the purchased technical support.	It depends on the list of selected modules and number of connectors, ability to use high availability/ multithreading, and the selected level of technical support.
License type	Subscriptions (for on-prem and cloud installations) and perpetual licenses (for on-prem installations).	Subscriptions and perpetual licenses.	Subscriptions and perpetual licenses.	Perpetual, MSSP.	Perpetual, MSSP.
Number of users	Limited. Users can be purchased.	Limited. Users can be purchased.	Limited. Users can be purchased.	Limited. Users can be purchased.	Not limited.
Number of assets (IT assets)	Not limited.	Not limited.	Not limited.	Limited. Assets can be purchased.	Not limited.
Number of connectors	Not limited.	Limited. Connectors can be purchased.	Limited. Connectors can be purchased.	Limited. Connectors can be purchased.	Not limited in the enterprise version. Limited boxed version
Technical support	Yes. Service language: English.	Yes. Service language: English.	Yes. Service language: English.	Yes. Service language: Russian, English.	Yes. Service language: Russian, English.

Extra		The choice of the license depends on the storage period of incident data, connected TI feeds, available automation, and reporting. There is a free Community Edition.	The retention period for storing data on closed cases depends on the license and can be additionally expanded.	The vendor offers separate expertise packages; sets of audit requirements are purchased.	The vendor offers a "boxed" and enterprise solution adapted to the Customer's settings. Both options include expertise packages.
1.8. Сертификаты					
FSTEC, FSB certificates	No.	No.	No.	The product is certified by the FSTEC of Russia and can be used to provide IS in significant objects of CII of the 1st category, in the GIS of the 1st security class, in the ISPD with the 1st level of personal data protection. The product is included in the Unified Register of Russian Programs for Electronic Computers and Databases.	The product is certified by the FSTEC of Russia for the 4th level of trust, can be used to provide information security in significant facilities of the 1st category of CII, in the GIS of the 1st security class, in the ISPD with the 1st level of personal data protection. The product is included in the Unified Register of Russian Programs for Electronic Computers and Databases.
1.9. Deployment (list of Customers according to open sources)					

Deployment	Barclays, Rosselkhozbank JSC, CAE, Pension Fund of the Russian Federation.	Comcast, Oracle, Unity Technologies, Magnit, AutoSpecCentre.	Horace Mann, Fedex, ExxonMobile, Atos.	VTB, MTS Bank, UniPro, Gazpromneft, FTS of Russia, Sibur.	Sberbank, Rostec, Otkritie, FSO of Russia, SDM Bank, Russian Post, Goznak.
1.10. Other					
Working in the multitenancy mode	Yes, support for MSP providers is implemented in MSSP add-on.	Extended Multitenancy support.	Advanced Multitenancy support for MSSP providers and commercial SOCs.	Yes, support for access control and role model for MSSP without physical data separation.	Yes, support for granular access control for MSSP, including the ability to physically separate data.
Fault tolerance	Yes.	Yes, the Live Backup mode for instant backup.	Yes.	Yes, in the Active-Passive, Active-Active modes.	Yes, in the Active-Passive, Active-Active modes.

This comparison of the analyzed general and technical features of the solutions shows that modern IRP/SOAR systems are generally characterized by the same architectural approaches: support for virtualization environments and Open Source platforms, widespread use of APIs, access to the product via a web interface with support for various authentication methods, flexible search and appearance customization options, support for multitenancy and fast scaling to meet the performance requirements of MSSP providers. At the same time, products from vendors of wide specialization (IBM, PaloAlto) are guaranteed to open their abilities when working together with related data systems of these developers, as well as the components and internal mechanisms of such products are also often "tied" to the use of a single technology stack of the vendor. On the other hand, vendor-independent products can boast of greater flexibility and breadth of integration capabilities.

Domestic solutions from R-Vision and Security Vision have certain competitive advantages compared to foreign products: they have certificates of the FSTEC of Russia; they are included in the Unified Register of Russian Programs for Electronic Computers and Databases; vendors can provide operational support on-site and in Russian, as well as they are familiar with the specifics of the market. Russian solutions support installation on domestic operating systems, which can also become a determining factor for a number of customers. Both players also offer something more than just IRP/SOAR systems: the integration of Information security management processes (using SGRC systems modules) and cyber incident response processes, which provides a deeper understanding of Information security events and incidents, data enrichment, and provides the necessary context for decision making when handling cyber incidents. However, Security Vision offers more attractive license terms (unlimited number of IT assets and users in the system, expert packages included in the price), more flexible installation options (support for Windows installations), physical isolation of tenant data (which may be critical for certain clients of MSSP providers).

It should be noted that a number of Western and Russian manufacturers have taken the path of microservice architecture, which, on the one hand, simplifies the delivery of more complex integrations, but on the other hand, leads to the need for additional qualifications of the employees responsible for product maintenance. The availability of certificates of Russian regulators and the ability to install on domestic operating systems can be important for a number of customers.

2. Comparison of functionality					
2.1. Automation and response scripts					
2.1.1. Working with scripts	The use of dynamic playbooks that implement the business logic of procedures for responding to cyber incidents of the company, as well as rules, conditions, actions, phases, tasks, scripts, workflows. The graphical editor of workflows for responding to cyber incidents allows setting the logic of repeatable business processes and response scripts with complex execution conditions and the setting of manual and automatically executed tasks. A small workflow can be part of a more complex workflow.	The solution receives messages about potential incidents from connected IT/ Information security systems (for example, from SIEM systems, e-mail systems), from CSV files, using the RESTful API; incidents can also be manually created in the system. Incident response procedures are presented in customizable playbooks (response scripts) written in YAML in accordance with the COPS standard. It supports the execution of scripts in Python and JavaScript, which are run when performing Tasks used in playbooks and when executing commands in the "War Room" (the incident handling workspace with all actions, artifacts, logging). Teams in	Input data comes from the SIEM systems. Next, the solution aggregates relevant events into cases using custom grouping rules, then a playbook is applied for this type of case, then the resulting case is assigned to a specific analyst. A playbook is a predefined set of actions used when executing triggers and logical conditions for each type of event in order to enrich event data from connected IT/IS systems, request information from users affected by the incident, as well as make decisions and perform automatic or automated actions on connected systems to counter the threat. The result of Actions is returned as	Input data comes from integrated systems, then processed by performing incident actions (depending on the type of incident) and response scripts (a sequence of actions performed when predefined boolean conditions are met). Actions and scripts are configured via the Playbook editor's graphical interface. Creation of a case manually from a vulnerability is supported.	Input data comes from integrated systems or related platform modules. Working with incidents is configured through the universal functionality of workflows that implement the tool for handling and life cycle of incidents, including enrichment from external systems and the execution of active actions. Graphical editor of response processes. Performing response actions depending on the fulfillment of boolean conditions.

		the "Command Center" can perform some actions in the XSOAR platform (for example, closing an incident), as well as perform actions in integrated systems (for example, checking the reputation of an IP address). Support for creating scheduled events using the functionality of Jobs, which are triggered either by a timer or by a certain incoming event.	messages, tables, links, files, and JSON objects. Next, the analyst can perform additional actions, run scripts and commands, and then decide to close or escalate the case.		
2.1.2 Support for complex logic in playbooks	The ability to implement complex case response logic is provided by creating Python scripts (Python 2.7 and 3.6 are supported) that allow accessing case data and performing complex actions. Scripts can be run by rules or workflows. Python scripts are denied access to the server file system and networking, and import of certain Python libraries is not supported. The list of Python	Support for the creation of YAML playbooks in accordance with the COPS standard. Creating elements (incidents, indicators) from the solution command line using proprietary syntax.	By editing Python scripts.	Graphic editor for playbooks (response scripts), manual and automatic launch of preset response scripts	The graphical interface of the playbook editor allows implementing both preset actions and the functionality of complex boolean operations: mathematical, boolean, textual, operations, as well as operations with arrays.

	modules available for import is also limited.				
2.1.3 Support for scheduled playbooks	No.	No.	Yes.	Limited. Scripts can be launched on a group of assets according to a schedule.	Yes.
2.1.4. Integrated development environment (IDE) for creating workflows	No.	No.	Yes, creating custom scripts in the Python 2.7 IDE.	No	No, using integration.
2.1.5. Pre-configured playbooks	Yes.	Yes.	Yes, more than 80 preset playbooks for the most common use-cases.	Yes, more than 30 preset playbooks.	Yes, more than 50 preset playbooks.
2.1.6. Access to playbooks from the community	No.	Access to playbooks from the community using the marketplace.	Access to response scripts and playbooks from the community using the Marketplace. The ability to share personal response scripts and playbooks for other users of the solution after verification and approval by the vendor.	No.	No.
2.1.7. Support for codeless playbook creation	Yes, codeless creation of playbooks in a graphical editor of workflows and response rules.	Yes, codeless creation of playbooks in a graphical playbook editor.	Yes, using a graphical playbook editor.	Yes, using a graphical playbook editor.	Yes, using a graphical playbook editor.

2.1.8. The ability to export / import playbooks	Yes, export and import rules, workflows, scripts, incident card fields, functions, phases, tasks to a JSON file.	Yes, export the playbook as PNG.	Yes, export playbooks as CSV, PDF. Export/import of playbooks (ZIP format) for transferring from one environment to another, copying, etc.	Yes, export system data as xlsx, docx, and pdf. Export elements to a graphic format (png,).	Import/export any data in machine-readable form. Import / export any objects as xlsx, csv, docx, pdf. Import/export of customized workflows in internal format. Export elements to a graphic format (png, jpeg).
2.1.9. Support for versioning playbooks, the ability to rollback to a previous version	No.	No.	Support for versioning of playbooks, viewing the history of playbook versions, the ability to rollback to any of the previous versions.	No.	No.
2.1.10. Support for simulating (testing) responses on playbooks before publishing them	The ability to create simulations of response to test incidents with the development of response actions (Simulations functionality). Two types of simulations are supported: scripts (practicing actions to respond to an incident) and risk assessment (modeling a personal data leak situation and providing recommendations, as well as indicating the	Testing scripts, commands, APIs in a dedicated test environment – Playground. Using product and test repositories to check the correctness of updates, scripts, playbooks.	The ability to create a test case manually, to simulate a case to test a new playbook on the events available in the system. The ability to test (by simulation) an existing IS event by cloning it. Launch of playbooks on a staging server and the ability to transfer to a production server.	No.	Yes.

	potential penalty for the leak). A special permission is required to create a simulation from the solution interface.				
2.2. Tools for interacting with integrated systems					
2.2.1 Interaction protocols with MS Windows systems	MS RPC, PS-Remoting (NTLM authentication). Executing the Windows Shell, PowerShell commands.	MS RPC, PS-Remoting (NTLM authentication). Executing the Windows Shell, PowerShell commands.	MS RPC (NTLM authentication). Executing the Windows Shell, PowerShell commands.	MS RPC (NTLM authentication). Executing the Windows Shell, PowerShell, and WMI commands.	MS RPC (NTLM, Kerberos authentication). Executing the Windows Shell, PowerShell, and WMI commands.
2.2.2 Interaction Protocols with Linux systems and software software-hardware systems	SSH, SNMP.	SSH, SNMP.	SSH, SNMP.	SSH, SNMP.	SSH, SNMP.
2.2.3 IT asset inventory module	No. By integrating with IBM QRadar.	No. By integrating with connected systems, incl. Asset Management.	No. By integrating with connected systems, incl. Asset Management.	Yes, based on the built-in nmap. Python-based windows connection module – the impacket module.	Yes, personal development.
2.2.4 Supported databases	MySQL/MariaDB, PostgreSQL, Microsoft SQL Server.	MySQL, PostgreSQL, Microsoft SQL Server, Oracle.	MS SQL, MySQL, PostgreSQL.	MS SQL, MySQL, PostgreSQL, Oracle.	MS SQL, MySQL, PostgreSQL, Oracle.
2.2.5 Web Request Support	REST, SOAP.	REST, SOAP.	REST, SOAP.	REST, SOAP.	REST, SOAP.

2.2.6 Event flow support	Syslog.	Syslog.	Syslog.	Syslog.	Syslog.
2.2.7 SIEM systems support	IBM Qradar, McAfee ESM, Micro Focus ArcSight, Splunk.	IBM Qradar, McAfee ESM, Micro Focus Arcsight, Splunk, FortiSIEM.	IBM Qradar, McAfee ESM, Micro Focus ArcSight, Splunk.	MP SIEM, IBM Qradar, McAfee ESM, Micro Focus ArcSight, FortiSIEM, RSA Netwitness SIEM, RuSIEM.	MP SIEM, IBM Qradar, McAfee ESM, Micro Focus Arcsight, Splunk, FortiSIEM, RSA Netwitness SIEM, RuSIEM. KAV KUMA, Comrad SIEM.
2.2.8 DLP systems support	Forcepoint, Symantec.	Forcepoint, Symantec.	Forcepoint, Symantec.	InfoWatch, Forcepoint.	InfoWatch, Searchinform, Falconegaze.
2.2.9 Support for message brokers	Kafka.	Kafka.	No.	No.	Kafka, IBM MQ.
2.2.10 Support for virtualization systems	VMware.	VMware.	VMware.	VMware.	VMware, Microsoft Hyper-V, OpenStack.
2.2.11 Support for Russian CERTs	No.	No.	No.	FinCERT, NCCCI.	FinCERT, NCCCI.
2.2.12 Support and interaction with Active Directory	LDAP. Interaction and unloading based on personal development.	LDAP. Interaction and unloading based on personal development.	LDAP. Interaction and unloading based on personal development.	LDAP. Interaction and unloading based on pyldap and ldapdomaindump.	LDAP, ADWS. Interaction and unloading based on personal development.
2.2.13 Support for E-mail services	Microsoft Exchange, Microsoft Exchange Online.	Microsoft Exchange Online.	Microsoft Exchange, IMAP\POP3, SNMP.	Microsoft Exchange, IMAP\POP3, SNMP.	Microsoft Exchange, IMAP\POP3, SNMP.

2.2.14 Support for endpoint security systems	Kaspersky, McAfee, Symantec, Carbon Black.	Microsoft Defender, McAfee, CrowdStrike, Carbon Black, Symantec.	Microsoft Defender ATP, McAfee, CrowdStrike, Carbon Black, Symantec.	Kaspersky, McAfee, Symantec.	Kaspersky, McAfee, Symantec, Security Code.
2.2.15 Support for Vulnerability Management Systems	IBM VM, Tenable, Qualys.	Tenable, Qualys, Nexpose.	Tenable, Qualys, beSecure.	Tenable, Qualys, RedCheck, MaxPatrol, Nexpose, SkyBox, OpenVAS.	Tenable, Qualys, RedCheck, MaxPatrol, Nexpose, SkyBox, OpenVAS.
2.2.16 Executing user scripts	Sending messages, running functions, performing actions on connected systems using Action Processors. Resilient App (extension/integration) – a set of playbook components (which includes rules, workflows, Python scripts, custom fields of an incident card, data tables, message destinations for internal information exchange) or executable code (for accessing and receiving data from external systems, integration and interaction with them). Resilient Apps can be either independent Kubernetes containers or software extensions that	Integration using RESTful API is supported. To run Python scripts and perform integrations, Docker containers are used. They contain all the necessary libraries and dependencies, which are programmatically isolated from the Cortex server to improve security. The ability to send notifications to administrators about an error when receiving data from integrations is supported.	The ability to transform data coming from sources (property values) into solution properties using transformation functions (Regex expressions), processing the results of actions (coming as JSON objects) using Pipe functions (processing arrays, filtering, sorting, normalization). Setting access rights for API keys.	Connectors allow interacting with different systems by using the following protocols and mechanisms: · SSH · SOAP · REST · LDAP · MySQL · PostgreSQL · Oracle · RPC · PowerShell · SNMP · R-Vision script. The results obtained can be converted based on regular expressions and stored in multiple incident fields.	Connectors allow interacting with different systems by using the following protocols and mechanisms: · Apache Kafka · DNS · HTTP · HTTPS · IBM MQ · IMAP · PowerShell · RPC · REST · SNMP · SOAP · LDAP · Microsoft SQL · MySQL · Oracle · PostgreSQL · SSH · CMD · TLS · WMI

	require server integration. As a result of Resilient App, the following actions are performed: sending data and interpreting the execution results, recording the execution results in the incident card, accessing the TI service, accessing a third-party system and two-way interaction with it via the RESTful API. Support for downloading the Resilient App from the IBM marketplace. Support for parsing email messages from a connected mailbox using Python scripts.				· Java · Javascript · PowerShell · Python. The results obtained can be processed as JSON, XML or Text, indicating the path to the desired element, as well as converted based on regular expressions and stored in multiple incident fields. Support for parsing emails from a connected mailbox. Generation of multi-stage commands of the format: authentication-data request-data retrieval is available.
2.2.17. Types of integrated systems	Integration with over 180 IT / Information security systems using Resilient App Host containerization technology (based on Kubernetes).	Over 500 integrations, full integration with PaloAlto products.	Over 230 integrations with IT / Information security systems.	Pre-configured integration with more than 50 IT / Information security systems of different classes.	Pre-configured integration with more than 100 IT / Information security systems of different classes.
2.2.18. Two-way interaction with integrated systems	Two-way interaction with connected systems using RESTful API, data transfer in JSON format, access to	Support for two-way integration with some IT / Information security systems with data	Depending on the integration.	Depending on the integration.	Yes, two-way interaction with connected systems.

	all the functionality of the solution, access to the interactive REST API browser to evaluate all the features.	synchronization (Mirroring).			
2.2.19. The ability to create user integrations	Yes, Resilient SDK for building Resilient Apps in the Kubernetes containers or plug-ins. The containers are running the Python 3.6.8 environment and the Resilient Circuits framework for implementing text messaging via the STOMP protocol and REST API interaction with the Resilient platform. Templates for creating a user application are provided. The tool for working with external IT / Information security systems is implemented using Functions, with which one can send data from the incident card (static or dynamically received) through the Message Destination to an external system and get	Yes, creating custom integrations using the BYOD (Bring Your Own Integration) functionality. Using the Cortex XSOAR IDE to develop automation scripts in Python (version 2.7 or 3.x).	Yes, creating user integrations and Actions via the built-in Python 2.7 IDE. View and edit the source code of commercial integrations and actions, as well as import, export, and manage them in the IDE. Python 2.7 syntax highlighting; the ability to add libraries with Python PIP. Version control, version history, the ability to rollback to a previous version.	No.	Yes. A universal mechanism for creating new connectors implemented according to the Low-code principle.

	the result of their processing as JSON, followed by changing the data in the incident card, attaching the attachment file, adding an entry to the data table, etc. There is a developer portal, a GitHub repository, and a community.				
2.2.20. Support for code-free integration with IT / Information security systems	Code-free integration with Resilient App Host.	No.	No.	No.	No.
2.2.21. Integration with Threat Intelligence systems	Yes, built-in integration with TI services (IBM X-Force Exchange, AlienVault, iSight Partners, SANS Internet Storm Center, VirusTotal); the ability to add additional TI feeds, connect your own TI service via the REST API. The ability to use GeoIP feeds.	Yes, support for creating custom fields in indicators and custom types of compromise indicators, configuring the display of the indicator card. Analysis of the reputation of indicators using the DBot functionality. TI data can be processed using the DBot functionality integrated with the Slack messenger. Getting indicators using integrations (TI-types and TI-data enrichment services), from Information security events (for example, from SIEM	Yes, the Siemplify ThreatFuse technology in partnership with cyber intelligence company Anomali to collect, analyze and manage TI data and indicators of compromise using Machine Learning methods Receiving data from TI feeds as part of customized integrations. The ability to create a custom indicator and enter data manually.	Using R-Vision Threat Intelligence Platform, a cyber intelligence data management solution.	Using Security Vision Threat Intelligence Platform, a cyber intelligence data management solution.

		systems), manually (uploading STIX files to the solution). The ability to export and import indicators (CSV, STIX). Accounting for the reliability of the TI data source. Accounting for the obsolescence of indicators. Launching playbooks when updates are received from TI-feeds. The ability to extract indicators from incoming Information security events and immediately use them as parameters in playbooks. Using fuzzy hashes (SSDeep hashes).			
2.2.22. Marketplace availability	Marketplace and GitHub repository.	Built-in marketplace with content packs (free and paid), including integrations, playbooks, dashboards, automation scripts, use cases, reports. Portal with applications from Palo Alto and partners.	Marketplace with playbook templates, use cases, integrations that can be downloaded by the vendor, third-party users (after vendor verification), as well as the end user of the system. The ability to download content updates offline (via ZIP archives).	No.	No.
2.2.23. Response agents	No.	Using D2 agents for Windows, Linux, and macOS to perform response actions (scripts,	Agent for performing response actions at remote sites using cross-platform (Windows, Linux) agents,	No.	No.

		commands) on remote devices, and to collect forensic data. Windows devices support remote execution of commands for obtaining a list of running processes, services, WMI requests, accessing the registry, file system, accounts, network configuration, and obtaining a RAM dump.	which are a Python application installed both on-prem and in the cloud (supporting the launch from a Docker container). The agent interacts with the proxy server (Publisher) using HTTPS to receive new commands and send the collected data.		Optionally, if necessary, it is implemented as a separate response service.
2.3. Internal cross-modular integration tools					
2.3.1. Interaction between solution modules	Native integration with the IBM QRadar SIEM system (incident data exchange, event request) and with the IBM X-Force Exchange cyber intelligence provider.	Using internal user lists with the storage of text data, JSON objects and files available for use in automations, playbooks, scripts, "Command Centers".	Manual task creation is supported.	Management and response to cyber incidents is based on a multifunctional solution that allows integrating data on incidents with vulnerabilities, assets, audits, tasks, and cyber risks. IRP, SGRC, SENSE, TDP, TIP, CII, GOSSOPKA are separate products.	The platform is designed for IS management and automation. The ICP/SOLAR/SDRH products and modules work on a single platform. Allows automating such IS processes as: incident management, asset and inventory management, vulnerability management, cybersecurity threat analysis (TI), interaction with NCCCI (GosSOPKA), FinCERT, cybersecurity risk management, compliance management,

					operational risk management. All functional modules can interact with each other both in terms of data exchange and enrichment, and implementation of the logic of the processing workflow.
2.3.2. Integration with the cyber risk management system	No.	No.	No.	Yes.	Yes.
2.4. Incident management (case management)					
2.4.1. Configuring an incident card	Configuring the display of the incident card (the Incident Layouts function). Data tables are used in the incident card to display information on the incident in a tabular form, to record data received from connected IT / Information security systems, and to use this data later in the product. Support for creating custom fields of the incident card. Support for execution timers for incident fields (in order to build response time	The creation of custom fields in the incident card is supported. The ability to view the running playbook in real time, the ability to assign tasks from the incident viewing interface (the Work Plan tab). Full customization of the properties and design of the incident card while considering user access rights. The ability to automate the creation and filling of incident card properties using scripts (Python, PowerShell, JavaScript).	Configuring how to display cases, filtering, sorting.	The ability to Configure the design of the incident card in a graphical editor, support for setting the view depending on the user's role. Configuring incident description fields that are displayed depending on the type of incident.	Flexible configuration of the incident card in a graphical or HTML editor. Arbitrary arrangement of fields on the card (without a preset "grid"). The ability to create tabs in the card. The ability to configure the composition of the displayed data of related objects (assets, vulnerabilities, etc.). The ability to customize the view depending on the user's role. Formatting, validation, and autofill of card fields depending on the field value and other fields.

	metrics, switch a workflow to an alternative route in case of a timeout). Support for adding HTML elements to the incident card.				
2.4.2. Model of access control to incident data	Granular access to objects based on the role model, which allows granting access to certain incidents with particular rights (create, view, edit, perform tasks, create reports, close or delete incidents), as well as to artifacts, simulations, tasks, incoming emails from a mailbox connected to Resilient. Creation of custom roles. The ability to display the value of an incident property only when certain boolean conditions are met. Setting access rights for API keys.	Creating custom roles, granular access rights (denial of access, read-only, read and change) to solution modules, the ability to grant a role for a period of time (for example, during an analyst's shift in SOC). Clear authentication of any domain user on the Self-Service portal with minimal read rights (creating an incident, viewing the status of personal application). Granting granular access rights (no access, read-only, read-write) to incidents and investigations using a role-based access model, as well as granting access to sensitive incidents only to certain Team Members.	Users are assigned to a specific "department" whose members will be involved in handling incidents. The role of an auditor is assigned who can view all incidents, close and reopen them. There is a role "Administrator" with full rights, a role with read-only rights, a role for standard users. Setting access rights for users and API keys. The ability to set restrictions on the use of certain Actions. The ability to create up to 20 custom roles.	Differentiation of access to incidents based on a role model. Including users in the incident workgroup automatically (using response scripts) or manually (in the incident properties).	Differentiation of access to incidents based on a role model. The ability to restrict access to incidents based on any properties of the incident. The ability to restrict access to viewing certain properties of specific objects (for example, certain properties of incidents containing confidential information).

2.4.3. TLP-Incident Privacy labels	Yes, using integration.	No.	No.	No.	Yes, in the card of the module for interaction with NCCCI. This type of label can be imported into any other incident card.
2.4.4. The ability to add attachments to the incident card	Yes, the ability to create custom attachments in the incident card.	Yes, the ability to create attachments ("evidence") to incidents.	Yes, adding attachments to the case is supported.	Yes, the ability to add evidences to the incident and the calculation of the checksum of the file.	Yes, the ability to add an unlimited number of "File" fields to the incident card (for example, "Explanatory", "Artifacts", "Analytical reports", etc.). The ability to exchange files in the chat of the incident card.
2.4.5. Creating custom incident types	Support for creating new types and subtypes of incidents with a hierarchical structure (parent / child types of incidents). Response rules are assigned to certain types of incidents to correctly handle certain situations.	It is possible to create custom types of incidents with custom fields of the incident card.	Creating custom case types	Creation of custom categories and types of incidents, levels of severity, methods of implementation, templates of incidents.	Creation of custom categories and types of incidents, levels of severity, methods of implementation, templates of incidents.
2.4.6. Incident prioritization	Incident prioritization based on the logic of rules and workflows.	Incident prioritization based on rules in playbooks and machine learning recommendations.	Setting priorities for sequential execution of playbooks (up to 3 playbooks) for one type of event.	Incident prioritization is performed using the settings of the incident handling workflow.	Automatic incident prioritization based on the workflow logic (including calculation based on user formulas using other platform data – assets, users, vulnerabilities, risks,

					etc.). Manual incident prioritization by users.
2.4.7. Filtering out false positive incidents	No.	Filtering out false positives based on machine learning data.	Using the Overflow Mechanism to filter out "noise" – false positives, minor warnings.	Yes, manual.	Yes, manual and automatic with a "learning" tool.
2.4.8. Correlation and deduplication of incidents	No.	Yes, manual deduplication, within the playbook (3 preset playbooks, including a machine learning playbook), using scripts, pre-processing rules and a table of Dropped Duplicate Incidents. Correlation of incidents by indicators, by types of incidents.	Yes, processing the incoming stream and mapping the properties of incoming events to the properties of the Simplify platform is done using the built-in Data Processing Engine (DPE). Correlation of Information security events is carried out using the Alert Grouping tool for combining Information security events entering the system into cases by analyzing the temporal characteristics and properties of events.	Yes, the ability to automatically extract incident property values based on tags (from incoming emails and API integrations) and regex expressions (from the output of automation scripts).	Yes, extensive possibilities for working with data obtained through integrations – parsing and normalization, cleaning and validation, filtering and deduplication, correlation. Grouping events into a single incident based on custom criteria. Creating incident links based on custom attributes.
2.4.9. Working with compromise indicators	Yes, an incident visualization graph showing the artifact and timeline links. Linking incidents that have the same artifact values of a	Yes, adding indicators of compromise from Information security events sent to the solution (for example, from the SIEM systems). Using integrations to enrich	Yes, building visual models (24 preset models) and links between event sources, entities (subjects and objects of the incident), indicators, events, incidents using the	Yes, the implementation of a full-fledged data processing for indicators of compromise – data acquisition, analysis and processing, checking for signs of compromise in the	Yes, the implementation of a full-fledged data processing for indicators of compromise – data acquisition, analysis and processing, checking for signs of compromise in the

	certain type. Create custom artifact types.	indicator data. Support for linking incidents based on matching indicators (for example, hash sum values). Graphical display of similar incidents, for example, those which have the same indicators of compromise.	Ontology mechanism. Visual representation of the development of the incident, incoming events, and links between the subjects and objects of the incident.	infrastructure, automatic addition to security tools, using it in incident response processes.	infrastructure, automatic addition to security tools, using it in incident response processes.
2.4.10. Building an incident timeline	Yes, building an incident timeline in the incident visualization graphs.	Yes, creating an incident timeline as records in the " Command Center" of the incident.	Yes, incident data is ordered chronologically in the "Command Center". The creation of visual timeline of Information security events related to the case is supported. The ability to graphically "reproduce" the sequence of events related to the case.	Yes.	Yes.
2.4.11. Incident collaboration options	Yes, dividing the product interface into Workspaces to provide sharing or isolation of displayed incidents for different departments of the company. Collaboration can be organized through the functionality of Tasks, in which, depending on the values of the properties of the incident card, a task is assigned to	Yes, collaboration in the virtual space of the "War Room" of the incident.	Yes, collaboration on incidents in a single interface of the "Command Center", which exchanges information between analysts and investigators, displays the current status of the incident and current tasks when processing, the time schedule representing the work with the case.	Yes, co-viewing and working with incidents in the "Incidents" tab.	Yes, co-viewing and working with analyst team incident cards. Additionally, the team chat is available in the card.

	analysts, and the process of its solution is controlled. Tasks can also be assigned depending on the incident phase.				
2.4.12. The ability to set manual response tasks (To Do Tasks)	Yes, assigning tasks to employees for manual execution using the Tasks functionality.	Yes, assigning Tasks to employees: manual (To Do Tasks) or as part of a playbook, with an indication of the expected completion time.	Yes, the ability to set manual actions that require the direct intervention of the employee (choice of option, answer to a question).	Yes, requesting information from the user (sending a request by email and receiving / parsing a response). Manual solution in the response scripts: user choice, no more than 3 response options.	Yes, assigning tasks to employees for manual execution by setting up a response workflow.
2.4.13. Notification functionality	Support for notification functionality through various communication channels by integrating with the Everbridge software and by installing the Slack Integration for Resilient software. Access to the Slack messenger on mobile devices.	Notifications via email, the Slack messenger, work via the Cortex XSOAR Enterprise mobile app (for iOS, Android) and abilities for incident management, viewing dashboards, processing attachments, receiving and sending messages.	Notifications on the web portal by sending email notifications, push notifications to users whose manual action is required in the playbook to continue responding. Sending notifications if the playbook is "frozen" with an execution error. Creating HTML templates for emails.	Support for custom messages using the following communication channels: · Event feed · E-mail · Telegram.	Support for custom messages using the following communication channels: · Sound, siren · Event Feed · E-mail · SMS · Telegram The ability to configure a new type of notification via the connector mechanism.
2.4.14. Implementation of the ChatOps concept	Implement the ChatOps concept by installing the Slack Integration for Resilient software.	The ChatOps concept is implemented by integrating the XSOAR solution with the Slack messenger using the DBot functionality, which allows	No.	No.	Partly using chats on requests.

		analyzing indicators and artifacts from a single interface available for various platforms, incl. mobile ones. Incident chats for analysts to collaborate in the "Command Center".			
2.4.15. Incident chats	Functionality for entering user data in the incident card when working with it.	Communication on incidents is implemented in the "Command Center" of the incident as a chat. Support for incident chats in the Slack messenger and in the Cortex XSOAR Enterprise mobile app (for iOS, Android).	The ability to "mention" a user or group in the case, as well as automatic notification sending. The ability to send a message to a team member from the case view interface. Informing response teams by posting Announcements that appear in the event feed of all users.	No.	Yes, a separate chat for each incident.
2.4.16. Support for creating an audit trail	No.	Logging all incident actions in the virtual "War Room" created for each incident. Logging actions performed by administrators in the XSOAR system, sending to an external syslog server.	Storing closed cases in accordance with the established retention period of data storage.	Yes, logging of all changes per incident.	Yes, logging of all changes per incident.
2.4.17. Support for MITER ATT & CK Matrix	No.	Yes, support for MITER ATT & CK matrix, linking indicators of compromise to TTPs.	No.	No.	Yes, support for MITER ATT & CK matrix in the Investigation module.

2.4.18. Maintaining a knowledge base of resolved incidents	The ability to specify instructions and recommendations in response tasks (in the Instructions property). Maintaining an internal Resilient Wiki indicating important information, instructions, reference information, with differentiation of access rights (view and create/change/delete) based on roles.	Analysis of resolved incidents based on machine learning methods to issue recommendations and classify new incidents.	Creating a knowledge base about events and cases in the system considering the links between event sources, entities (subjects and objects of the incident), indicators, events, incidents using the Ontology mechanism by building data models. The built data model allows automatically processing new input data and performing the corresponding automatic response actions.	Yes, by accumulating the history of incidents and their solutions based on manual search.	Yes, by using the "Knowledge / Solution Base" functionality, which accumulates and analyzes information on previously resolved incidents. The ability to search for the most suitable solution based on a neural network with dynamic weights and supervised learning (when used together with the BigData module).
2.5. Cyber incident response					
2.5.1. Performing types of response actions	Support for manual and automatic response actions as part of the workflow: manual actions (the Menu Item functionality) involve clicking a certain interactive button in a drop-down action menu; automatic actions are performed when certain conditions are met without user interaction.	Reacting in playbooks and tasks by performing manual and automatic actions (scripts).	Reacting in playbooks by performing automatic actions and manual operations.	Automating incident response by performing incident actions (depending on the type of incident) and response scripts (a sequence of actions performed when predefined boolean conditions are met). The ability to perform manual actions on integrated systems using remote device login (WMI, MS RPC for Windows systems; SSH/SNMP for Linux/ Unix systems, Cisco, Juniper, HP network equipment),	Automating incident response by executing scripts and incident actions that can be configured using the Workflow functionality. The ability to perform manual actions on integrated systems. The ability to perform actions through a react connector that supports the following protocols and tool: · Apache Kafka · DNS · HTTP · HTTPS

				running automation scripts on devices (PowerShell, cmd, Bash), executing proprietary R-Vision scripts on the collectors to automate response actions.	· IBM MQ · IMAP · POP3 · PowerShell · RPC · REST · SMTP · SNMP · SOAP · SSH · SSL · TLS · WMI · Microsoft SQL connection tool · MySQL connection tool · Oracle connection tool · PostgreSQL connection tool · Active Directory connection tool · Exchange connection tool.
2.5.2. Logic of response action execution	Support for executing actions when predefined boolean conditions are met. A condition can include a field, a mathematical expression, or a value calculated using Python scripts. Conditions can be combined using logical AND / OR. Actions can also be performed if	Responding when boolean conditions are met and considering a user request (including when filling out a questionnaire).	Reacting (triggering playbooks) by executing a predefined set of actions that are applied when triggers and boolean conditions are executed for each of the event types.	Running response scripts when boolean conditions are met (compare the value of the field, the associated asset), the ability to combine logical conditions (AND/OR).	Performing response actions as part of the response script, depending on meeting boolean conditions (matching the values of the incident fields to the specified criteria), and the ability to create complex conditions using the AND/OR operators. Performing actions initiated by the user. Starting actions

	certain data is received from the connected systems.				at a certain time, with a certain frequency.
2.5.3. Creating custom response actions	The ability to add personal response actions is provided by creating Python scripts (Python 2.7 and 3.6 are supported) that allow accessing incident data and performing complex actions on connected systems.	Creating automation scripts in JavaScript, Python, and PowerShell that are run when performing Tasks used in playbooks and when executing commands in "War Room". Scripts can access objects in the solution, use internal APIs, receive and process data. Protecting scripts with passwords is supported.	Performing custom actions when running Python scripts.	Performing response actions: · Email notification · Assignment of the responsible person · Changing incident properties · The script as Windows cmd, PowerShell, Linux Shell, Python, R-Vision.	The ability to perform the following types of actions: · Changing the attributes/ properties of the incident (including assigning a processing group and/or a responsible person) · Creating new system objects (processing tasks, additional actions, etc.) · Changing attributes of related objects (assets, vulnerabilities, tasks, etc.) · Email notification · Calling connector scripts on Windows cmd, Powershell, WMI, Linux Shell, Python, Java, JavaScript, Bash.
2.5.4. Tools for creating custom scripts	The Resilient Python SDK is provided (two libraries for Python versions 2.7 and 3.6), as well as the Resilient Circuits Integration framework, based on Python, for creating custom functions and actions.	No.	Creating Actions with the built-in Python 2.7 IDE. View and edit the source code of commercial actions, as well as import, export, and manage them in the IDE. Python 2.7 syntax highlighting; the ability to add libraries with Python PIP. Version control, version history,	No.	Graphical editor of workflows and connectors.

			the ability to rollback to a previous version.		
2.5.5. Access to isolated network segments	No.	Working with isolated network segments based on "engines" – servers on Linux / Windows with the Cortex XSOAR Engine installed, which receive information security events and execute integration commands in isolated segments, sending data to the central server of the solution.	Performing response actions at remote sites using cross-platform (Windows, Linux) agents, which are a Python application installed both on-prem and in the cloud (supporting the launch from a Docker container). The agent interacts with the proxy server (Publisher) using HTTPS to receive new commands and send the collected data.	Yes, by installing distributed components.	Yes, by installing distributed components.
2.6. Machine learning methods					
2.6.1. Application of machine learning	Yes, support for machine learning methods (by installing the application) and the choice of algorithms, tuning models to predict the values of the incident card fields, including recommendations for the assignment of the most appropriate analyst, categorization and	Yes, using machine learning methods to analyze resolved incidents and automatically classify new incidents, close false-positive incidents, and use a scoring model to assess the level of incident risk. Analysis of the reputation of indicators and artifacts using the DBot functionality that uses machine learning. Using a scoring model for assessing	No.	No.	Yes, support for decision-making on response based on a neural network with dynamic weight coefficients and supervised learning. A semantic incident analysis module that contains a machine learning model and is designed to automatically identify and execute cybersecurity incident response commands. The use of machine learning

	prioritization of incidents.	the hazard and reliability of an indicator based on machine learning data. Recommendations for assigning the most appropriate analyst to a particular incident.			algorithms for detecting anomalies provides automatic creation of incidents and the ability to automatically determine incident response teams.
2.6.2. The ability to load custom machine learning models	Yes, customization of downloadable models.	Yes, support for supervised learning, the ability to create custom ML models.	No.	No.	Yes.
2.7. Data visualization, incident reporting					
2.7.1. Incident data (News Feed) visualization	Activity Dashboards for all users with News Feed, a list of tasks assigned to the user. Analytics Dashboards with charts and graphs of incident data. Viewing data in tabular and graphical form. Export data to CSV, save charts as JPG, PNG, SVG. Creation of custom graphs and charts (bar, pie), display of arbitrary data in tables. Plotting time graphs of incident processing (displaying the time spent on processing each phase of the incident) with the Time Tracker function.	Data visualization in fully customizable dashboards and widgets, presentation of information and incidents as charts, graphs, tables, text. Visualization of SLA execution, a field in the card for accounting for SLA parameters and sending notifications in case of their violation, output of reports and SLA metrics as CSV. Creating custom dashboards and widgets, the ability to share dashboards based on the role model of access. Creating widgets using JSON files and scripts (JavaScript, Python,	Visualization of data on incidents in dashboards with the description of the incident, risks, expected damage, timestamps for response tasks, and a graph of changes in the level of danger of the incident. Dashboards are customizable to a limited extent – only some predefined elements can be added. In dashboards, one can place custom widgets (no more than 12) and display charts, graphs, tables. Sharing dashboards and saving dashboard data in a report are supported. Displaying statistics, work	Viewing an incident action diagram – a graphical display of the incident action tree with visualization of the action state. Viewing the progress of the incident handling process (as a percentage) in the incident properties. Chart types: · Incident management (more than 10 preset charts);· Asset management (more than 10 preset charts); · Risk management, including visualization of	Built-in designer of reports and dashboards for using any data and fine-tuning the displayed information. Export of graphics as pdf, jpg, png. Import of graphics from jpg, png formats. All graphical views provide object search, Drill-Down, and quick access to related objects (assets, incidents). Graphical views (widgets) with interaction support for creating dashboards of any composition and configuration.

		PowerShell) based on a search query to the list of incidents. Graphical visualization of incidents and indicators representing the links.	schedules, and performance metrics for each playbook using the dashboard or from the properties of the playbook.	damage from cyber incidents Map functionality: · Displaying incidents, assets, vulnerabilities, and groups of IT assets on geographical maps · Drill-Down functionality (switching from the map to incidents/assets with viewing detailed information) Functionality of diagrams: · Linking arbitrary types of incidents/assets with each other · Visualization of assets on the network diagram. Functionality of dashboard: · Charts and metrics displaying history, current statuses, events and statistics	Preset data display types for widgets: Line chart Bar chart Table Pie chart List Incident calendar Preset visualization panels: Operational dashboard (information on cyber incidents) Tactical dashboard (statistical information, visualization of the dynamics of incidents) General dashboard for risks (visualization of cyber risk dynamics, risk distribution, history) Advanced risk dashboard for information systems (risk distribution, history). Geographic map showing buildings, settlements, planets. Displaying features, links, interactions between objects, including assets and incidents; displaying the availability of devices and services.

2.7.2. Incident reporting	Exporting incident reports to Excel format; creating user report templates.	Exporting incident data to a CSV file; the ability to create a report from the incident viewing interface. Reporting and providing statistical information for a specific time period, exporting as PDF, DOC, and CSV. The ability to set the design of the report and the list of sections with data, add a widget to the report, schedule the release of the report, send it by email, and release the report from the incident card. Calculating and visualizing the ROI of XSOAR product based on data on the time of analysts saved by automation.	Support for exporting reports on incidents as DOC, exporting playbooks as CSV, PDF, graphics. Exporting reports on system operation (user actions, connection history) as CSV. Assigning time-based SLA metrics for cases that display response statistics. Generation of a report (as DOC) on ROI (Return on investment) for the solution. Generation of reports (as PDF, DOC) on the performance of the SOC Center, analysis of the work of employees, analysis of case processing metrics with the ability to schedule the release of reports and with the option of generating custom reports containing graphics.	Export of reports as docx, pdf. Generation of reports on schedule and manually, sending by email. Generation of custom reports. Preset reports.	Built-in designer of reports and dashboards for using any data and fine-tuning the displayed information. Generation of reports on arbitrary data obtained by creating SQL queries to the database. Full customization for the needs of the customer. Export of reports as xlsx, docx, pdf, xml, csv. Creation of reports on schedule and manually, delivery by email/to file/via API in xml, pdf, doc, xls, ppt. The ability to prepare a report based on a certain template from the incident card. The ability to generate summary reports on the parameters of lists, to use analytical and predictive tools for data analysis with function of graphical display, integration with external visualization systems. Preset reports.

2.7.3 Additional custom data analytics.	No, partly as part of search queries.	Yes, the use of search queries enables complex analytics and reuse of the received data in dashboards.	No, partly as part of search queries.	No, partly as part of search queries.	Yes, data manipulations, complex searches, groupings, and views are available in the Analytics module.
2.8. Lists, databases of normative acts					
2.8.1. Creating and using lists	Yes, ability to create user lists.	Yes, using user lists with the storage of text data, JSON objects and files available for use in automations, playbooks, scripts, "Command Centers".	Yes, maintaining Custom Lists by entering arbitrary text data into them and using records as triggers for playbooks.	Yes, ability to create custom lists for use in all modules of the solution, including incident management.	Yes, ability to create custom lists for use in all modules of the solution, including incident management.
2.8.2. Using a regulatory database (integrated SGRC/auto-SGRC abilities)	Partially. Compliance with legal requirements in case of personal data leakage is implemented in the Privacy add-on module. The regulatory database contains more than 170 international, state, and local regulatory requirements (GDPR, HIPAA, CCPA, etc.), including the regulations of all US states. The module specifies the jurisdiction of the company and the type of data that it processes; based on this, some actions prescribed	No.	No.	Partially. Preset regulations: 152-FZ, FSTEC of Russia (Orders №№17, 21, 31, 239), PCI DSS (3.1, 3.2), SWIFT's Customer Security Program, ISO 27001, GOST R ISO / IEC 27001-2006, 382-P, STO BR IBBS-1.0-2014, GOST R 57580.	Yes, preset regulations: 187-FZ, 152-FZ, GDPR, FSTEC of Russia (Orders No. 17, 21, 31, 235, 239), PCI DSS (3.1, 3.2), SWIFT's Customer Security Program, SWIFT CSCF 2020 , ISO 27001, GOST R ISO / IEC 27001-2006, 382-P, 672-P, 683-P, 684-P, 716-P, STO BR IBBS-1.0-2014, GOST R 57580. Automatic adjustment of settings for tools and systems using the Auto-SGRC mechanism: automatic change of OS/software/IS tools to comply with internal

	by law are automatically performed.				regulatory requirements/return to baseline settings.
2.9. Options for MSSP providers					
2.9.1. Support for MSSP providers	Yes, support for MSSP providers is implemented in the MSSP add-on module.	Yes, extended support for the Multitenancy mode.	Yes, advanced Multitenancy support for MSSP providers and commercial SOCs.	Yes.	Yes.
2.9.2. Data sharing for tenants	The division of response workflows for different clients is carried out by building a hierarchy of organizations with various independent playbooks. Creating global objects (dashboards, playbooks) to control customer infrastructures.	Complete data isolation between tenants. The ability to distribute centrally created playbooks, automation scripts, integrations, widgets, dashboards to tenants. The ability to exchange indicators of compromise between tenants. For each tenant, dedicated control of the SLA metrics, reporting, sending notifications, executing automation scripts in case of violation of the SLA metrics is supported.	Support for the multi-environments functionality to handle incidents of multiple clients/companies (“environments”) at the same time. Providing access to the "Command Center" only for certain "environments". Launching and providing access to solution elements (cases, dashboards, playbooks, events, entities, etc.) based on their belonging to a certain "environment". Providing a role-based model of differentiating access to "environments" for users and API keys. Setting the retention period for storing data on closed cases for "environments". Assigning personal SLA metrics for	Yes, support for access control and role model for MSSP without physical data separation.	Yes, support for granular access control for MSSP, including the ability to physically separate data.

			each of the "environments". Setting access rights for API keys for each of the "environments".		

Trends:

The functionality of the IRP/SOAR systems demonstrates the main modern trends in automating the processes of responding to cyber incidents: integration with a large number of heterogeneous systems for enriching and contextualizing incident data and automated elimination and localization of threats, presentating the logic of response processes as graphical playbooks. Also, the ability to create custom response scripts, provide tools for collaboration of Information security analysts (both as a single interface and implementation of the ChatOps concept), interact with cyber intelligence data management systems, build an incident history with documentation and collect forensic data, visualize processed data in dashboards, widgets, and reports. Machine Learning, Artificial Intelligence, and Big Data analysis systems are also being used: they provide IS analysts with tips on the most appropriate ways to respond, suggest options for further actions, analyze trends, and assign the most experienced employees to cases.

Integrations:

The main tool that no modern SOAR system can do without is the integration module. All the solutions have a fairly good number of ready-made connectors provided in "out-of-the-box". However, it is worth noting that some of the domestic and Western solutions have built-in tools for developing their own connectors according to the Low-code principle, which greatly simplifies the implementation of independent integrations with various external systems for end users. It is also important to be able to customize and have the flexibility to integrate IT/IS solutions into a complex architecture. Developers often change the interfaces of interaction, and the ability to make the necessary adjustments as soon as possible without waiting for a response from the SOAR vendor is also a key factor when choosing a solution.

Information systems are not always ready for external integrations which are "out-of-the-box". In some situations, data acquisition becomes a multi-iterative, time-separated process of generating an authentication token, requesting a receipt, waiting for the request to succeed, and finally obtaining the desired information. If the company implements such solutions as Privilege Access Management Vault, this feature becomes simply necessary. Of the analyzed products, long live containers from Palo Alto and Security Vision have such an opportunity and make it possible to create several interrelated steps and a toolkit for enriching the data obtained from the report "in an online fashion". Then each of the received report elements is supplied with additional data from an adjacent element.

Inventory of IT assets is an important feature integrated into Russian solutions as opposed to foreign ones. Foreign products solve inventory problems mainly by integrating with related solutions, including Asset Management. To download and work with Active Directory, most vendors use their own development and secure methods. At the same time, the use of third-party scripts for uploading data (such as pyldap and ldapdomaindump) and interacting with systems on the MS Windows platform (such as python impacket) are not the best practices in information security and pose threats to Customers who use the solution.

Working with incidents:

The speed of processing and, ultimately, its quality largely depend on how convenient, informative and intuitive the card of the incident or other object in the system will be created. Obviously, the card that registers a DDoS attack should be very different from the card that reports a potential compromise of the administrator account. Incident Layouts from IBM and View Editor from Security Vision enable the creation of custom incident templates to best manage the SOC analyst's attention.

Visualization and reporting:

SOAR is aimed to become a single showcase for the consolidation of data on the performance of SOC processes. The functionality of search, analytics, data presentation, and report preparation is of particular importance in this case. Thus, it is not only about the number of preset template views, the functionality of which is rapidly being “outgrown” by the current Information security department. The ability to replicate user analytic views on the platform is important. Otherwise, the performance metrics agreed with the management will have to be calculated by creating complex queries directly to the SOAR solution base, or, in the old fashioned way, in Excel. The R-Vision solution has pretty good preset reports and visualizations. At the same time, the analytical tools of the Palo Alto product and the Analytics module in Security Vision allow any calculation and presentation of data.

Specificity of the Russian market:

Foreign solutions are more open: there are marketplaces for downloading ready-made playbooks, plugins and integrations; there are portals for developers with technical documentation and the opportunity to share their best practices with the community; GitHub repositories are freely accessed by cybersecurity enthusiasts; free Community Editions of commercial products are provided. Domestic solutions have other obvious advantages: a knowledge base of Russian regulatory requirements; interaction with FinCERT and GosSOPKA; integration with domestic Information security solutions; broad expertise in ensuring compliance with legislation and countering specific cyber threats. The R-Vision solution interacts with TIP (cyber intelligence data management), SENSE (anomaly detection and analysis of the Information security state), TDP (decoy system for analyzing the actions of attackers), SGRC (company IS management). Modules /Products are purchased separately, and the R-Vision IRP solution looks less flexible when building workflows for responding to cyber incidents compared to the Security Vision SOAR system. In the Security Vision IRP/SOAR platform Machine Learning, Artificial Intelligence and BigData are widely used, for example, for suggesting the most appropriate response action, analyzing incidents and assigning the optimal response team and for automatical creation of incidents when anomalies are detected. The Security Vision modules can run on the same platform. The Security Vision solution uses the Auto-SGRC tool to automatically adjust the settings of IT / Information security systems to comply with internal regulatory requirements and return to the baseline settings.