



Securaa Integrations

Securaa is a Comprehensive SOC automation product suite. Securaa is built entirely on No-Code and bring down dramatically time required to implement, configure and customize. Securaa suite includes a SOAR, TIP and Cyber Asset Management.

Securaa is a versatile and user-friendly security management platform that simplifies threat monitoring and incident response for SOC teams. Securaa supports unlimited integrations and has unlimited integrations support, 1000+ Automated tasks and playbooks. With Securaa, businesses can effectively manage their security applications, resources, and operations without the need for scripting or complex operations. The platform offers a visual interface that enables easy control and management, making it accessible even to low-skilled resources. Implementation and management of Securaa are straightforward compared to other platforms, streamlining the hectic and tedious processes of security management. Securaa provides a unified solution that empowers businesses to identify and respond to threats promptly, reducing the mean time to respond and enhancing overall security.

S.No	Category	Product	Tasks
1.	SIEM	IBM QRadar On Cloud (QROC) v7.4.1	Get Offenses Get Offenses Closing Reason Get Offense By ID Get Search Get Search Results Get Asset By ID Get Assets Close Offense Update Offense Create Offense Note Get Offense Note Qradar Run Query Create Reference Get Reference Get Reference By Name Delete Reference Set Delete Reference Set By Name Delete Reference Set Value Get Events Create Securaa Case From Qradar Offence Update Offence to Securaa Update Events Data to Securaa Case Update Events Data To Securaa Case With Query Get Raw Logs

2.		RSA NetWitness V11	Get Incident Details Get Incident Alert Delete Incident Update Incident Get Incident Time Range
3.		Wazuh	Fetch Alerts
4.		LogRhythm	Fetch Alerts
5.		RSA Platform V11.3.2.0	List Auto Provision Get Advanced Threat Protection List JIT List Storage List JIT by Location Update Advance Threat Protection Update Auto Provision Get Auto Provision Setting Get Alerts Get Alert by Category Update Alert
6.		Azure Sentinel V1.0	Get Alerts Alert By Get Alerts Category Update Alert
7.		Splunk V9.0.3	Get All Index Splunk Search Create Search Job ID
8.		HP Arcsight ESM V7.0	Get All Query Viewers Get All Cases Get Single Case Create a Case Delete a Case Get Query Viewer Result Get Case Event IDs Get Security Events Get Entries Clear Entries Add Entries Update Case
9.		Securonix V6.3.1	Check Entity in Watchlist Create Watchlist Get Default Assignee for Workflow Get Incident Get Incident Available Actions Get Incident Status Get Incident Workflow Get Watchlist

			List Activity data List Incidents List Policies List Threat Actions List Resource Group List Users List Violation Data List Watchlist List Workflows Perform Action on Incident Add Comment to Incident Create Incident
10.		Google Chronical V1.0	Get Domain Reputation Get IP Reputation Get List IOC's Get IOC Details Get List Assets Get List Alerts Get List Events
11.		Elastic Search SIEM V7.6.0	Get Single Case Get Case Activity Get Case Status Get All Cases Create Case Add Comment Update Comment Update Case
12.		Azure Security Center Version: 1.0	List Auto Provision Get Advanced Threat Protection List JIT List Storage List JIT by Location Update Advance Threat Protection Update Auto Provision Get Auto Provision Setting Get Alerts Get Alert by Category Update Alert
13.		BluSapphire Version: 1.1.18	Get All Alerts Get Particular Alert
14.		IBM QRadar Security Intelligence v7.3.1	Get Offenses Get Offense by ID Get Search Get Search Results

			Get Assets Get Asset by ID Close Offense Update Offense Get Note Create Reference Get Reference Get Reference by Name Delete Reference Update Reference Qradar Run Query Get Event Get Offense Closing Reason Get Offense Correlations Get Username from Correlation Log Check Asset Status Get Asset Information Add Location List Location Block Location Verify Location
15.		DNIF	Search Alerts
16.		CrowdStrike Nextgen	
17.		Graylog	Get List of Investigation Get Detail of Investigation Create Investigation
18.		Rapid7 SIEM	Get Investigation Assign User to Investigation Get Investigation Alerts Create Investigation Update Investigation
19.		Sumologic	Get All Insight Status Get Single Insight Status Get Single Insight Resolutions Get All Insight Resolutions Get All Custom Insight Get Single Custom Insight Get Single Insight
20.	Vulnerability Scanner	Nessus V7.1.0	Nessus Scan Nessus Host VA Details Get Nessus Scan Status Get Scan List Create Scan Get Scan Details

21.		Rapid7 Nexpose V1	Get All Sites Get Particular Asset Get Particular Scan Stop Particular Scan Start Particular Asset Scan Get Particular Site Scan Get Asset Vulnerability
22.		Qualys V1.0	Scan Asset Get Scan Report
23.	IT Services	Amazon AWS S3	Get S3 Bucket List Delete Bucket
24.		AWS DynamoDB	Create Table Update Table Delete Table
25.		AWS EC2 Instance	Get EC2 Instance Information Start EC2 Instance Information Stop EC2 Instance Information
26.		AWS Route53 V1.1	Create Record Delete Record List Zones
27.		AWS WAF V1.0	Create IP Set Update IP Set Get IP Set
28.		AWS ACM V1.1.18	Get Certificate List Certificate
29.		AWS CLOUD Trail V1.0.7	Create Trail Delete Trail Update Trail
30.		AWS CloudWatchLogs V1.0	Create Log Group Delete Log Group
31.		AWS SQS V1.0	Create Queue Delete Queue Get Queue URL
32.		AWS Lambda V1.0	Get Account Settings List Aliases
33.		Azure Compute V1.0	Get Instances Get Resources Start Instance Stop Instance
34.		Google Calendar	Get Event Create Event List All Event
35.		Google Docs	Get Document Create Document

36.		Google Translate	Get Supported Languages Detect Language Translate Text
37.		Microsoft Azure Active Directory V1.0	Get User Info
38.		Microsoft Graph Calendar V1.0	Get Event Create Event List All Event
39.		Microsoft Graph Group V1.0	Create Groups List Groups Get Groups
40.		Microsoft Shift	Create Shift Get Shift
41.	ITSM(Ticketing Service&Issue Tracking)	Service Now	Create Service Now Ticket Get Service Now Ticket Status Delete Service Now Ticket Update Service Now Ticket Check Service Now Ticket Status for Attacker IP Get Device Info Get Service Now Query Ticket Get Service Now Query Table Get Service Now Query Computers Get Service Now Query Groups Get Service Now Query Users Get Tickets Get Securaa Service Now Incidents
42.		Microfocus SMAX	Get All Incidents Get Single Incident Create Incident Create Request Update Incident Update Request Get Single Request
43.		Zoho	Get All Reports Add Record Get All Records Get a Specific Record Update Records Update Specific Record
44.		Jira Software	Get Issue Create Issue

			Edit Issue
45.		Jira Generic	Delete Issue Edit Issue Get Issue Create Issue Add Attachment
46.		Jira Service Management V1.0	Create Jira Ticket Get Jira Ticket Status
47.		Symphony V3.0	Get Incident Details Log Incident Update Incident Reopen Incident
48.		Codesk V1.0	Create Service Request
49.		SysAid V1.0	Create Service Request
50.		Jira	Delete Issue Get Issue Comments Get Issue Get the ID Offset Search Jira Issue Add Comments to Issue Add Links to Issue Create Issue Edit Issue
51.		Fresh Service	View Ticket View Ticket Activity View Task Create Task Update Task Create Ticket Update Ticket List All Agents List All Groups View All Tasks

			Create A Note List All Conversations of a Ticket
52.	Directory Systems	Active Directory	User Info User's Manager Info Change User Password Authenticate User Disable User Enable User
53.		Azure AD	Get All Users Info Get Group Name Add User to Group Remove User from Group Create AD User Delete User Disable User Account Enable User Account Update User Get Particular User Info Get Manager Info
54.		OpenLdap V2.4.53	User Info Users Manager Info Authentication User Change User Password
55.	Antivirus and (EPP)	Symantec Protection Endpoint	Get Device Info Quarantine Host Scan Host UnQuarantine Host Get Computer Info for a Specific Domain Get Latest Antivirus Info Get Finger Print List Add Blacklist as File Finger Print Send Command to Update Content Get List of Accessible Domain Get Critical Info List Get Group Data Get Domain Name for Specified SEP Get Command Status Quarantine File
56.		Check Point EDR	Create IOC Create Multiple IOCs Delete IOCs

			Edit IOC Get IOCs by Filter Get all IOCs
57.		Trend Micro Deep Security Manager	Get Computer List Get Policy List Generate Report Run Open Port Scan on All Computers Run Open Port Scan on Single Computer Run Malware Scan On All Computers Run Malware in Single Computer Delete Task
58.		Trend Micro Control Manager	Get Product Agent List Get Specific Product Agent Get Product Server List Isolate Product Agent Restore Product gent Relocate Product Agent Uninstall Product Agent
59.		Cisco AMP	Isolate computer Remove Isolation
60.		Crowd Strike Falcon	Contain Host Lift Containment Update Detection Behavior Details Search Detection Search Device Device Exist Get Host Get Host Information
61.		Sophos	Create Policy Delete Policy
62.		SentinelOne	List Agents List Exclusions Create Exclusions List Blacklist Items Create Blacklist Item Initiate Scan Abort Scan Get Agent Details Create Multiple IOC Get IOC Create IOC

63.	Firewalls	Palo Alto	Block IP Unblock IP Block URL Unblock URL Block Application Unblock Application Commit Changes List of Predefined Applications List of All Rules Move Rule Top Move Rule After Move Rule Before Delete Rule Details of Particular Rule Check If IP is Blocked
64.		F5 ASM (WAF)	F5 ASM Create Policy F5 ASM Apply Policy F5 ASM Delete Policy F5 ASM List Policy Ips F5 ASM Delete Policy Ip F5 ASM Add Policy Ip F5 ASM Update Policy Ip F5 ASM List Policy Urls F5 ASM Add Policy Url F5 ASM Update Policy Url F5 ASM Delete Policy Url F5 ASM Get Policy F5 ASM Get All Policy
65.		Cisco ASA	ASA Create Rule ASA Update Rule
66.		Checkpoint	Block IP Rule Show Access Rule base Show Hosts Add Host Delete Access Rule Show Hosts
67.		Fortinet	Fortinet Block IP Fortinet Unblock IP Get All Policy Get Particular Policy Delete Policy Move Policy Before Move Policy After

68.		FortiNet V2	FortiGate Get Policy FortiGate Delete Policy FortiGate Move Policy Before FortiGate Move Policy After FortiGate Create Policy FortiGate Update Policy FortiGate Ban IP FortiGate Unban IP FortiGate Get Banned IP's FortiGate Get Address FortiGate Delete Address FortiGate Create Address FortiGate Get Address Group FortiGate Delete Address Group FortiGate Create Address Group FortiGate Update Address Group
69.		Azure Firewall	Create Policy Update Policy
70.		Sonic Wall	Login Add Address Object Get Address Objects Create Policy Get Policy Update Policy Delete Policy
71.		Zscaler	Block IP Unblock IP Unblock URL Block URL
72.		AWS Network Firewall	Create IP Set Update IP Set Get IP Set
73.		Cisco Firepower	Create Access Policy Update Access Policy Get Access Policy Delete Access Policy Create Access Rule Update Access Rule Get Access Rule Delete Access Rule
74.		Cisco ISE	Create Policy Assign Policy
75.		Sophos firewall	Create Firewall Delete Firewall

76.		F5 Firewall	F5 Create Policy F5 Delete Policy F5 Create Rule F5 Delete Rule F5 Modify Rule F5 List Rule
77.	Mail/Email Services	Microsoft Outlook/Exchange	Show Mail Folders Extract Attachment Read Message Get Email by Address in To Get Email by Address in CC Get Email by Address in BCC
78.		Gmail	Get Msg
79.	Collaboration	Google Drive	List Files Get File
80.		Google Sheet	Create sheet Get sheet
81.		Microsoft Team	Create team Get Team Delete Team
82.		Microsoft Team Management	Add member Get member Delete Member
83.	Threat Intelligence	Recorded Future	Get Domain Reputation Get File Reputation Get IP Reputation Get Vulnerability Details Search Malware By ID Download Domain Risk List Download IP Risk List Download Hash Risk List Download Vulnerability Risk List Get Malwares Download URL Risk List Get URL Reputation Get Multiple Indicator reputation
84.		AWS GuardDuty	Archive Findings Create Detector Create Sample Findings Create ThreatIntel Set Delete Detector Delete IP Set Create IP Set Delete ThreatIntel Set

			Get Detector Get Findings Get IP Set Get ThreatIntel Set List Findings List IP Sets List ThreatIntel sets Unarchive Findings List Detectors Update Detectors Update Findings Feedback Update IP Set Update ThreatIntel Set
85.		Check Phish	CheckPhish Url Get CheckPhish Urls
86.		Cisco Umbrella	Umbrella Domain Repotation Umbrella Domain Security
87.		MineMeld v0.9.70	Get All Miners Get Indicators List for a Miner Get Indicator from Miner Search IP Indicator Search Domain indicator Search URL Indicator Add Indicator to Miner
88.		MISP	Add Sighting Add Attribute Add Tag Add Event Add IP Object Add URL Object Add Domain Object Add Email Object Delete Event Get All Feeds Perform Feed Action Search IP Search URL Search File Get Search
89.		WHOIS	Domain Enrichment
90.		Phistank	Get Phishing URL Information
91.		URLScan.io	Hunt IP Hunt Domain Get Report

92.		Alexa Ranking	Get Rank
93.		Abuse IPDB	Report IP Check IP
94.		Farsight DNSDB	DNS Lookup IP Lookup IP Prefix DNS Lookup Domain
95.		Cyble Vision	Get IOC Filters Fetch IOCs Fetch IOCs by CSV File
96.		IBM XForce	CVE Details Domain Reputation WHOIS IP File Reputation WHOIS Domain IP Reputation URL Reputation
97.		Threat Miner	Get IP Address Data Get File Data Get Domain/URL data
98.		Google safe Browsing	Safe Browsing Lookup URL
99.		Stackip info	Get IP Information Get Requester IP Information
100.		Have I been pwned	Breach Domain
101.		What is my browser	User Agent
102.		URL void	Get URL Reputation
103.		IP void	IP Reputation
104.		Malshare	List Sources Get File Info List Hashes
105.		Phishing Initiative	Get Phishing URL Information
106.		Passive Total	WHOIS IP IP Detail WHOIS Domain Domain Detail
107.		PIPL	Get User
108.		IP info	Get IP Info
109.		Alien Vault	Get Pulse Details Get IP Details Get Domain Info Get File Hash

			Query Host Get URL Details
110.		MX Toolbox	Lookup IP Lookup URL
111.		Shodan	Get IP Details Lookup URL/Domain
112.		OPSWAT Metadefender	Defender Lookup IP Defender Lookup Domain Defender Lookup Hash
113.		CVE Search (CIRCL)	CVE Information by ID Get CVE List
114.		Neutrino	Get Blocked IP Information
115.		Virus Total	IP Reputation URL Reputation Domain Reputation File Reputation
116.		Threat Connect	IP Reputation Domain Reputation File Reputation URL Reputation
117.		Axonius	Get Devices Get Users Get Instances
118.	Sandbox	Hybrid Analysis	Get Report Detonate URL Scan Hash
119.	Database	MySql	MySQL Query
120.		Postgre Sql	PostgreSQL Query
121.		MongoDB	MongoDB Query
122.		Elastic Search V7.6.0	Get All Index Get Particular Index with Query Get Particular Index ID
123.	Authentication	Okta	Create User Get User Get Group Members Get zone List zona Delete User Deactivate User Unlock User Get Failed Logins

			Get Logs Add User To Group Set Password Get Groups Search User List Of Groups Suspend User UnSuspend User Clear User Sessions Get User Factor Get Application Assignments Get Group Assignments Active User Remove From Group Get Application Authentication Update User Reset Factor
124.		SAML V2.0	Enable/Disable
125.		HardwareSecurity Module(HSM)	
126.	File	Microsoft Graph File	Delete File List of Drive Contents List of SharePoint Sites Replace Existing File Content Download File Content List Drives in Site Create New Folder Upload New File
127.	Messaging	Zoom V4.1.281	Create Meeting Create User Delete User Fetch Recording List Users
128.		Slack v1.0	Get Slack User List Get Slack Channel List Send Message Create New Channel Invite User Delete Channel
129.		OpenAI ChatGPT	Prompt GPT
130.		Webex Teams	Create Room Create Message
131.		Zendesk V2.0	Get Ticket Data Get Ticket Count Update Ticket

			List Ticket
132.		Zoom IAM V4.1.281	Zoom Disable User
133.		Slack IAM	Get all members User look up by email
134.		Manage Engine Service Desk	
135.	Logs	Syslog	
136.	Identity and Access Management / User Management	Service Now IAM v7.3.0	Service Now Get User Service Now Create User Service Now Update User
137.		ATLASSIAN CONFLUENCE	List Space Create Space
138.		Atlassian Confluence Server	Get User Get Space Create Space Delete Space Update Space
139.		Arcon PAM	Set Service User Mapping Set Service User Un-Mapping Disable User Delete User Get Service Password Change Set User Details
140.		AWS IAM	Create AWS IAM Role Create AWS IAM User Delete AWS IAM User Delete AWS IAM Role Get AWS IAM User
141.		Jira IAM	Get Jira User Create Jira User
142.		AWS IAM(UserLifeCycleManagement)	Create AWS IAM User

			Get AWS IAM User Create AWS IAM Group Delete AWS IAM Group
143.	Collaborative Version Control	GitHub	List All Repository Create Repository
144.		GitHub IAM	Get Own Information Get GitHub User Info
145.		GitLab	Get a repository Delete Repository Create Repository
146.		BitBucket	Get Projects Get Repository Get Commits Create Repository Create Project
147.	Map	Google map	Get Location
148.	Misc	Rss Feeds	
149.	Network Network Security /	Bind DNS	Get Record Create Record Delete Record Update Record Get All Records
150.		Cisco CloudLock	Get Users Get User Activities
151.		Cisco IronPort	IronPort Report
152.		Cisco IronPort Email Api	IronPort Quarantine Release Email IronPort Spam Release Email
153.		Cisco Secure Cloud Analytics(Stealthwatch Cloud)	Add Domin or IP in Blacklist SW List Alerts
154.		Cisco Umbrella Cloud Security	Get Record Create Record Delete Record

			Update Record Get All Records
155.		Cisco Umbrella Enforcement	Umbrella Add Domain Umbrella Delete Domain
156.		Azure Key Vault	List Key Vault Get Key Vault Create Or Update Key Vault
157.	TI Feeds	7777 Botnet-ms	
158.		ADEO	
159.		Adaway-ah	
160.		Akamai-rm	
161.		AlienVault	
162.		Ares RAT C2-ms	
163.		AsyncRAT-ms	
164.		Azure Sentinel	
165.		Bambenek	
166.		Binary Defense	
167.		BitRAT-ms	
168.		Browser Exploitation Framework-ms	
169.		Brute Ratel C4-ms	
170.		BurpSuite-ms	
171.		C2 Address	
172.		CERT-PL	
173.		CINS Score	
174.		CISA	
175.		Caldera C2-ms	
176.		Cobalt Strike C2-ms	
177.		Collector Stealer-ms	
178.		Covenant C2-ms	
179.		Cybel	
180.		DShield	

181.		Dan-Pollock-ah	
182.		DarkComet Trojan-ms	
183.		Data plane	
184.		DcRAT-ms	
185.		Deimos C2-ms	
186.		ELLIO	
187.		FireHOL	
188.		Gh0st RAT Trojan-ms	
189.		GoPhish-ms	
190.		Gozi Trojan-ms	
191.		Granicus	
192.		GreenSnow	
193.		Hachcat-ms	
194.		Hacked_Malware	
195.		Hak5 Cloud C2-ms	
196.		Havoc C2-ms	
197.		Hookbot-ms	
198.		IPSum	
199.		Kadhosts-ah	
200.		LOLBAS	
201.		MD5 Hashes	
202.		MalShare	
203.		MalSilo	
204.		MalwareBazaar	
205.		Metasploit Framework C2-ms	
206.		Mirai	
207.		MobSF-ms	
208.		Multiproxy Anonymous Proxy List	
209.		Myip.ms	
210.		Mythic C2-ms	

211.		NCSC	
212.		NanoCore RAT Trojan-ms	
213.		NetBus Trojan-ms	
214.		NimPlant C2-ms	
215.		Nocoin-ah	
216.		Notrack malware blocklist	
217.		Oyster C2-ms	
218.		Palo Alto Networks - Unit 42	
219.		Patriot Stealer IPs-ms	
220.		Phishing-domains-ACTIVE-mk	
221.		Phishing-mk	
222.		Poseidon C2-ms	
223.		Posh C2-ms	
224.		Projecthoneypot.org-aa -rm	
225.		Pupy RAT-ms	
226.		Quasar RAT-ms	
227.		RedGuard C2-ms	
228.		Remcos Pro RAT Trojan-ms	
229.		Reputation IP Feed	
230.		SANS Malware Blocklist	
231.		SHA1 Hashes	
232.		SOC Prime	
233.		Securaa	
234.		Sekio-rm	
235.		ShadowPad-ms	
236.		Sinkhole	
237.		Sliver C2-ms	
238.		Sophos	
239.		SpamDomain-ts	
240.		Spamhaus DROP	
241.		Spamhaus DROPv6	

242.		SpiceRAT-ms	
243.		SpyAgent-ms	
244.		Stamparm-rm	
245.		Supershell-ms	
246.		Talos	
247.		Targeted Threats Feed	
248.		ThreatView	
249.		Tor	
250.		URL Abuse	
251.		UnamWebPanel-ms	
252.		VNC/RFB	
253.		VX Vault	
254.		VenomRAT-ms	
255.		Villain C2-ms	
256.		Viper C2 -ms	
257.		Vshell-ms	
258.		XMRig Monero Cryptominer-ms	
259.		XtremeRAT Trojan-ms	
260.		ZeroAccess Trojan-ms	
261.		Zerodot1's Mining	
262.		abuse.ch SSL Blacklist	
263.		abuse.ch URL Haus	
264.		blocklist.de ApacheIPs	
265.		blocklist.de BotIPs	
266.		blocklist.de BruteforceIPs	
267.		blocklist.de FTPIPs	
268.		blocklist.de IMAPIPs	
269.		blocklist.de MailIPs	
270.		blocklist.de SIPIPs	
271.		blocklist.de SSHIPs	
272.		blocklist.de StrongIPs	

273.		blocklist.de ssh attacks	
274.		bogons	
275.		danger.rulez.sk	
276.		emergingthreats	
277.		firebog	
278.		ktsaou	
279.		misp	
280.		njRAT Trojan-ms	
281.		openphish	
282.		osint.digitalside.it	
283.		ph00lt0 - Blocklist	
284.		phishing.army	
285.		pop3 Gropers	
286.		proxyscan ips	
287.		sblam	
288.		viriback	
289.		7777 Botnet-ms	
290.		Zero Hack	
291.	Malware Analysis	Symantec Blue Coat Content and Malware Analysis	Detonate URL Detonate File
292.		Haltdos Antiddos	Haltdos Get All Feeds Haltdos Get Specific Feed Haltdos Create Feed haltdos Update Feed
293.	Utilities	Cisco WSA	WSA Get Access Policies WSA Modify Access Policies
294.	Servers	Webhook	