Securaa Playbooks

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.

Sl No.	Playbook
1	Multiple Logins Detected from VPN
2	Remote Logins from Unauthorized locations in VPN
3	AD_Block_User
4	ARVT
5	Account_Login_Failure V2
6	AssignCaseToUser
7	Block Account - Generic
8	Block Account - Generic V2
9	Block IP - Checkpoint
10	Block IP - Checkpoint V2
11	Block IP - Fortinet
12	Block IP - Fortinet V2
13	Block IP - Generic
14	Block IP - Generic V2
15	Block IP - PaloAlto
16	Block IP - PaloAlto V2
17	Block Indicator - IP
18	C&C Communication V2
19	C2C_Validation
20	C2_Validation_NO_UserIntervention_Paloalto V2
21	Check File Reputation V2
22	Check IP and URL Reputation V2

23	CnC Communication
24	Create Phishing SN Ticket
25	Custom App Playbook
26	Excessive firewall denies from remote host
27	Generic Enrichment - SYMC_CS_Nexpose_Qradar
28	Get Score For Indicator
29	Horizontal Port Scan
30	Investigate Offense – Qradar
31	IP Enrichment - Nexpose
32	IP Enrichment - CS
33	IP Enrichment - External
34	IP Enrichment - External V2
35	IP Enrichment - Internal
36	IP Enrichment - Internal V2
37	IP Enrichment-QRadar
38	IP Enrichment-SYMC
39	IPS high Severity Event
40	IPS Signature Detected
41	Instance Disable and Instance Not Present
42	Get_Jira_tickets
43	Multiple Logins Detected from VPN1
44	Multiple Signature Detected from Same Source on WAF
45	Network Endpoint TI Integrated Block Action - IBM_CP_CS
46	Network Endpoint TI Integrated Block Action - IBM_CP_SYMC
47	Network Endpoint TI Integrated Block Action - IBM_HP_CS
48	Network Endpoint TI Integrated Block Action - IBM_HP_SYMC
49	Network Endpoint TI Integrated Block Action - IBM_HP_TMCM
50	Network Endpoint TI Integrated Block Action - IBM_PA_CS
51	Network Endpoint TI Integrated Block Action - IBM_PA_SYMC
52	Network Endpoint TI Integrated Block Action - IBM_PA_SYMC V2
53	Network Endpoint TI Integrated Block Action - IBM_PA_TMCM
54	Network Endpoint TI Integrated Block Action - IBM_PA_TMCM V2
55	Network Endpoint TI Integrated Block Action - RF_CP_CS
56	Network Endpoint TI Integrated Block Action - RF_CP_SYMC
57	Network Endpoint TI Integrated Block Action - RF_CP_TMCM
58	Network Endpoint TI Integrated Block Action - RF_HP_CS

59	Network Endpoint TI Integrated Block Action - RF_HP_SYMC
60	Network Endpoint TI Integrated Block Action - RF_HP_TMCM
61	Network Endpoint TI Integrated Block Action - RF_PA_CS
62	Network Endpoint TI Integrated Block Action - RF_PA_SYMC
63	Network Endpoint TI Integrated Block Action - RF_PA_TMCM
64	Network Endpoint TI Integrated Block Action - Sec_CP_SYMC
65	Network Endpoint TI Integrated Block Action - Sec_CP_SYMC V2
66	Network Endpoint TI Integrated Block Action - Sec_CP_TMCM
67	Network Endpoint TI Integrated Block Action - Sec_HP_SYMC
68	Network Endpoint TI Integrated Block Action - Sec_HP_SYMC V2
69	Network Endpoint TI Integrated Block Action - Sec_HP_TMCM
70	Network Endpoint TI Integrated Block Action - Sec_HP_TMCM V2
71	Network Endpoint TI Integrated Block Action - Sec_PA_SYMC
72	Network Endpoint TI Integrated Block Action - Sec_PA_TMCM
73	Network Endpoint TI Integrated Block Action - Securaa_CP_CS
74	Network Endpoint TI Integrated Block Action - Securaa_HP_CS
75	Network Endpoint TI Integrated Block Action - Securaa_PA_CS
76	Network Endpoint TI Integrated Block Action - TMCM_CP_IBM
77	Notification Mail
78	Phishing Incident Response
79	Possible communication to Blacklisted IP
80	Quarantined Malware
81	Ransomware
82	Remote Logins from Unauthorized locations in VPN1
83	Remote Access Exploit Detected
84	SQL Injection on Web Application
85	Search Indicator in Securaa DB
86	Search Indicator in the Historical Alert data
87	Suspicious IP
88	TI Firewall Integrated Block Action - IBM_Checkpoint
89	TI Firewall Integrated Block Action - IBM_HP
90	TI Firewall Integrated Block Action - IBM_HP V2
91	TI Firewall Integrated Block Action - IBM_PA
92	TI Firewall Integrated Block Action - RF_CheckPoint
93	TI Firewall Integrated Block Action - RF_HP
94	TI Firewall Integrated Block Action - RF_PA

95	TI Integrated Block IP - Securaa_CP
96	TI Integrated Block IP - Securaa_CP V2
97	TI Integrated Block IP - Securaa_Fortinet
98	TI Integrated Block IP - Securaa_PA
99	TI Integrated Block IP - Securaa_PA V2
100	Get_Snow_tickets
101	Validate IP
102	Vertical Port Scan
103	WAF Directory Traversal Attack Detected