Recorded Future and Securonix

PRODUCT OVERVIEW

Securonix is a leader in the Gartner MQ for SIEM. The Securonix Security Operations & Analytics Platform provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, with zero infrastructure to manage.

While security threats become more challenging, business technologies generate an ever-increasing amount of data making legacy security monitoring solutions obsolete as they struggle with an inability to scale with limited resources and architectural challenges.

Built on AWS, the Securonix platform delivers unlimited scale, powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases security through improved visibility, actionability, and security posture while reducing management and analyst burden.

JOINT INTEGRATION DESCRIPTION

The Securonix Security Operations and Analytics Platform ingests Recorded Future Threat Intelligence (TI) indicators via API. All common threat indicators such as domain, IP, URL, etc. are ingested and indexed in the Securonix Data lake. This information is correlated using the Securonix Analytics AI-based engine enriched with other indicators from other assets in a customer's ecosystem.

The joint solution can help mitigate risk associated with malicious domains, URLs, and Ips, by enriching the data lake with known risk scores.

CHALLENGES OVERCOME THROUGH INTEGRATION

The joint solution enables SOC teams to proactively detect attacks and take preemptive countermeasures. This can be used to prevent attacks and contain threats before they occur, and thus bridge the gap between pre-attack and post-attack activities.

For example, if attempts to go to a malicious domain or IP that is reported by Recorded Future, SOC analysts now have the ability to not only have blocked that access attempt but quickly see the threat indicators & risk scores that go into why a domain/IP is a bad actor. Additionally, users are able to threat hunt and enrich alerts already identified down to the entity level.

USE CASES

Through the ingestion and enrichment of Recorded Future Threat Data, mutual customers will benefit from higher fidelity alerts and therefore more accurate and quicker response times.

Threat Prevention

- Pre-emptively auto-block Domains, URLs, and IPs
- Reduce the number of incidents to investigate.

Threat Containment: Hunt and Contain Threats

- High fidelity threat analysis reduces dwell times.
- Alerts enriched

Alert Enrichment

- Enrich alerts with Recorded Future Intelligence
- Correlate Recorded Future data with other ecosystem meta-data to create or enrich existing alerts

Recorded Future®

SECURONIX™

BENEFITS:

Threat Prevention

- Pre-emptively auto-block Domains, URLs, and IPs
- Reduce the number of incidents to investigate.

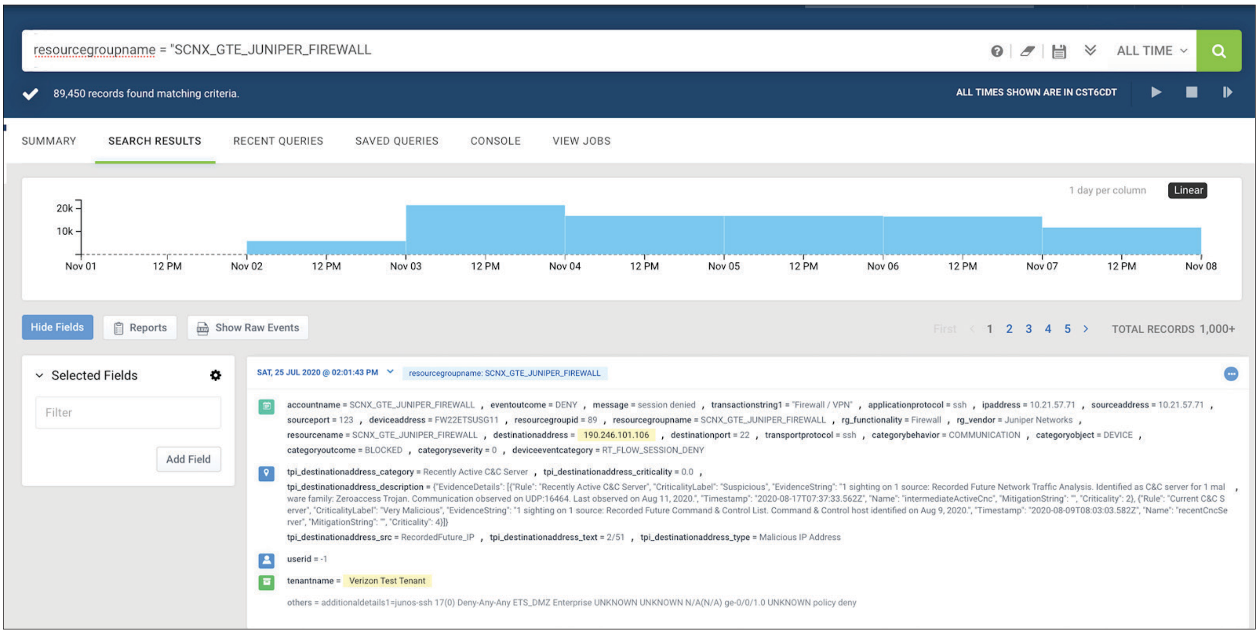
Threat Containment: Hunt and Contain Threats

- High fidelity threat analysis reduces dwell times.
- Alerts enriched

Alert Enrichment

- Enrich alerts with Recorded Future Intelligence
- Correlate Recorded Future data with other ecosystem meta-data to create or enrich existing alerts

DATA SHEET



SAT, 25 JUL 2020 @ 02:01:43 PM resourcegroupname: SCNX_GTE_JUNIPER_FIREWALL

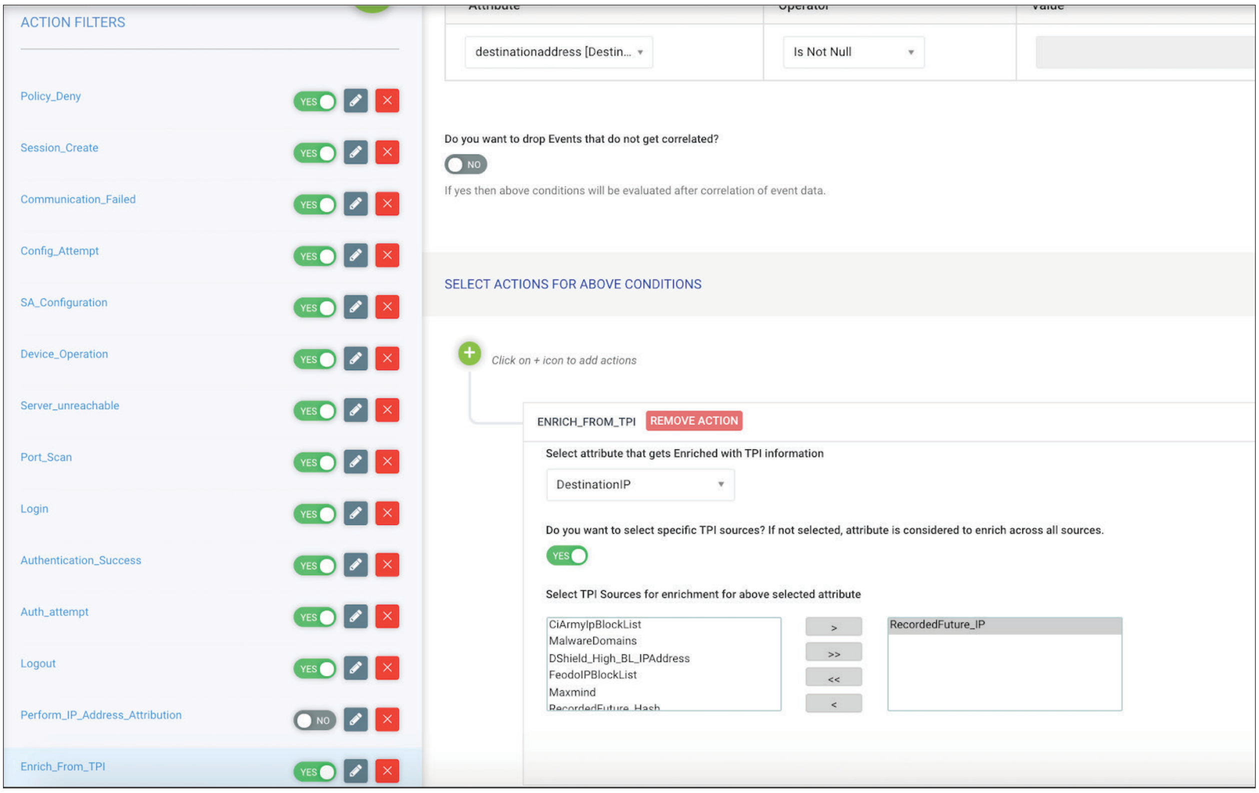
accountname = SCNX_GTE_JUNIPER_FIREWALL , eventoutcome = DENY , message = session denied , transactionstring1 = "Firewall / VPN" , applicationprotocol = ssh , ipaddress = 10.21.57.71 , sourceaddress = 10.21.57.71 , sourceport = 123 , deviceaddress = FW22ETSUSG11 , resourcegroupid = 89 , resourcegroupname = SCNX_GTE_JUNIPER_FIREWALL , rg_functionality = Firewall , rg_vendor = Juniper Networks , resourcename = SCNX_GTE_JUNIPER_FIREWALL , destinationaddress = 190.246.101.106 , destinationport = 22 , transportprotocol = ssh , categorybehavior = COMMUNICATION , categoryobject = DEVICE , categoryoutcome = BLOCKED , categoryseverity = 0 , deviceeventcategory = RT_FLOW_SESSION_DENY

tpi_destinationaddress_category = Recently Active C&C Server , tpi_destinationaddress_criticality = 0.0 ,
tpi_destinationaddress_description = {"EvidenceDetails": [{"Rule": "Recently Active C&C Server", "CriticalityLabel": "Suspicious", "EvidenceString": "1 sighting on 1 source: Recorded Future Network Traffic Analysis. Identified as C&C server for 1 malware family: Zeroaccess Trojan. Communication observed on UDP:16464. Last observed on Aug 11, 2020.", "Timestamp": "2020-08-17T07:37:33.562Z", "Name": "intermediateActiveCnc", "MitigationString": "", "Criticality": 2}, {"Rule": "Current C&C Server", "CriticalityLabel": "Very Malicious", "EvidenceString": "1 sighting on 1 source: Recorded Future Command & Control List. Command & Control host identified on Aug 9, 2020.", "Timestamp": "2020-08-09T08:03:03.582Z", "Name": "recentCncServer", "MitigationString": "", "Criticality": 4}]} ,
tpi_destinationaddress_src = RecordedFuture_IP , tpi_destinationaddress_text = 2/51 , tpi_destinationaddress_type = Malicious IP Address

userid = -1

tenantname = Verizon Test Tenant

others = additionaldetails1=junos-ssh 17(0) Deny-Any-Any ETS_DMZ Enterprise UNKNOWN UNKNOWN N/A(N/A) ge-0/0/1.0 UNKNOWN policy deny


ACTION FILTERS

Policy_Deny	YES
Session_Create	YES
Communication_Failed	YES
Config_Attempt	YES
SA_Configuration	YES
Device_Operation	YES
Server_unreachable	YES
Port_Scan	YES
Login	YES
Authentication_Success	YES
Auth_attempt	YES
Logout	YES
Perform_IP_Address_Attribution	NO
Enrich_From_TPI	YES

Attribute	Operator	Value
destinationaddress [Destin...	Is Not Null	

Do you want to drop Events that do not get correlated?

NO

If yes then above conditions will be evaluated after correlation of event data.

SELECT ACTIONS FOR ABOVE CONDITIONS

Click on + icon to add actions

ENRICH_FROM_TPI REMOVE ACTION

Select attribute that gets Enriched with TPI information

DestinationIP

Do you want to select specific TPI sources? If not selected, attribute is considered to enrich across all sources.

YES

Select TPI Sources for enrichment for above selected attribute

CiArmyIpBlockList
MalwareDomains
DShield_High_BL_IPAddress
FeodoIPBlockList
Maxmind
RecordedFuture_Hash

RecordedFuture_IP

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com