TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Brinqa

Contents

Partner Information 3
Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform 3
Palo Alto Networks Products for Integration 4
Integration Benefits 4
Integration Diagram 5
Before you begin 5
Palo Alto Networks Configuration 6
Partner Product Configuration 6
Troubleshooting 6
Technical Details 9

Partner Information

Partner information	
Date	May 30th, 2019
Partner Name	Brinqa
Web Site	https://www.brinqa.com/
Product Name	Brinqa Cyber Risk Services
Partner Contact	Syed Abdur (Director of Products, syed.abdur@brinqa.com, (213) 400-2991)
Support Contact	Support Portal : https://brinqa.atlassian.net/servicedesk/customer/portal/4/user/login Email : support@brinqa.com Phone # : (512) 372-1004
Partner Product for Integration	Brinqa Cloud Risk Service
Product Description	Brinqa Cloud Risk Service connects, models and analyzes all relevant security, context, and threat data to deliver knowledge-driven insights for risk prioritization, remediation and reporting.

Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform

- Cloud Infrastructure Risk Management
    - Elevate cloud infrastructure risk visibility to equal footing with network and software infrastructure risk.
    - Correlate cloud security vulnerabilities and alerts with additional business context, asset information, and threat intelligence for comprehensive risk analysis.
    - Identify, prioritize and remediate highest risk assets, vulnerabilities, and alerts.
    - Automate risk-aware, closed-loop remediation of vulnerabilities through rule-based creation, tracking, and escalation of tickets.
    - Leverage powerful, self-service analytics to present cloud security insights in the context of the business.

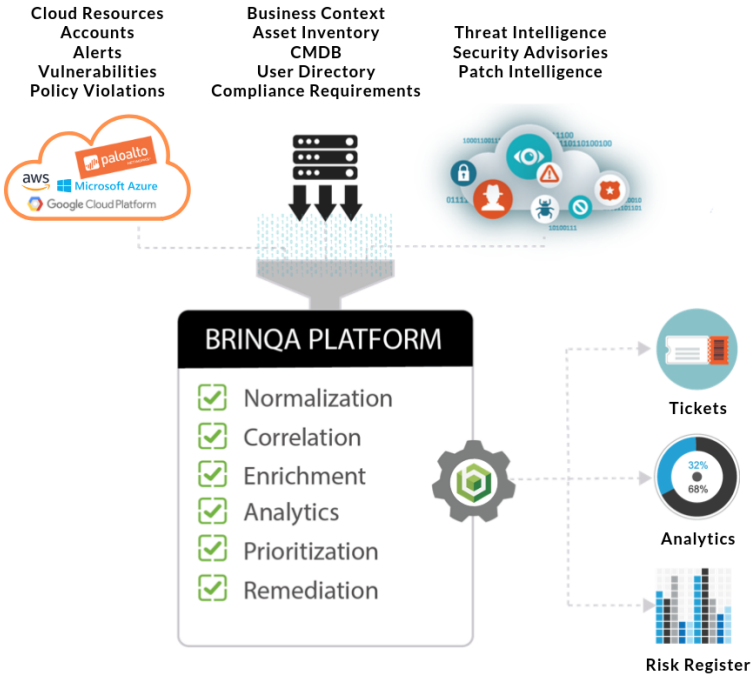
Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions supported	Brinqa versions supported
AutoFocus			
GlobalProtect			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW			
Panorama			
Prisma Access			
Prisma Public Cloud	Completed	April 2019	April 2019
Prisma SaaS			
Traps			
VM-Series			
WildFire			

Integration Benefits

- List out integration benefit for the customer.
    - Cloud infrastructure risk visibility at the same level and granularity as network and software infrastructure risk.
    - Ability to communicate cloud infrastructure risk in the context of business.
    - Ability to enforce cyber risk management mandates and policies over cloud infrastructure.
    - Analysis and prioritization of cloud security assessment result findings for automated response and remediation.
    - Rule-based ticketing for automated consolidation, ownership assignment and SLA enforcement while creating and tracking tickets in external ITSM systems.
    - Powerful BI interface for self-service metrics and reports.

Integration Diagram



- Data shared between Brinqa and Prisma Public Cloud
    - Brinqa pulls Prisma Public Cloud security policies and alerts using credentials provided by Prisma Public Cloud user/customer.
    - Data is shared between Prisma Public Cloud and Brinqa using Prisma Public Cloud APIs. The data is accessible only to a customer who has subscribed to Brinqa and Prisma Public Cloud. Also, no data is shared outside of the customer's Brinqa environment. Each Brinqa customer's data is stored in a single tenant service model.
    - Once Prisma Public Cloud data is imported into Brinqa it is used as part of Brinqa's cyber risk management services for risk remediation and reporting.

Before you begin

- Each customer will need to have Prisma Public Cloud service access and they will need to set up the integration using their Prisma Public Cloud credentials.
- Requirements for successful integration
    - Access to Brinqa and Prisma Public Cloud accounts
    - Basic understanding of how the two products work.
- Dependencies
    - The integration uses Prisma Public Cloud REST API and other than a user account to authenticate, there are no dependencies.

- Requirements for API keys
    - Prisma Public Cloud REST API requires Token based authentication using username/password. Credentials are retained in Brinqa to maintain session tokens required during connector operations.

Palo Alto Networks Configuration

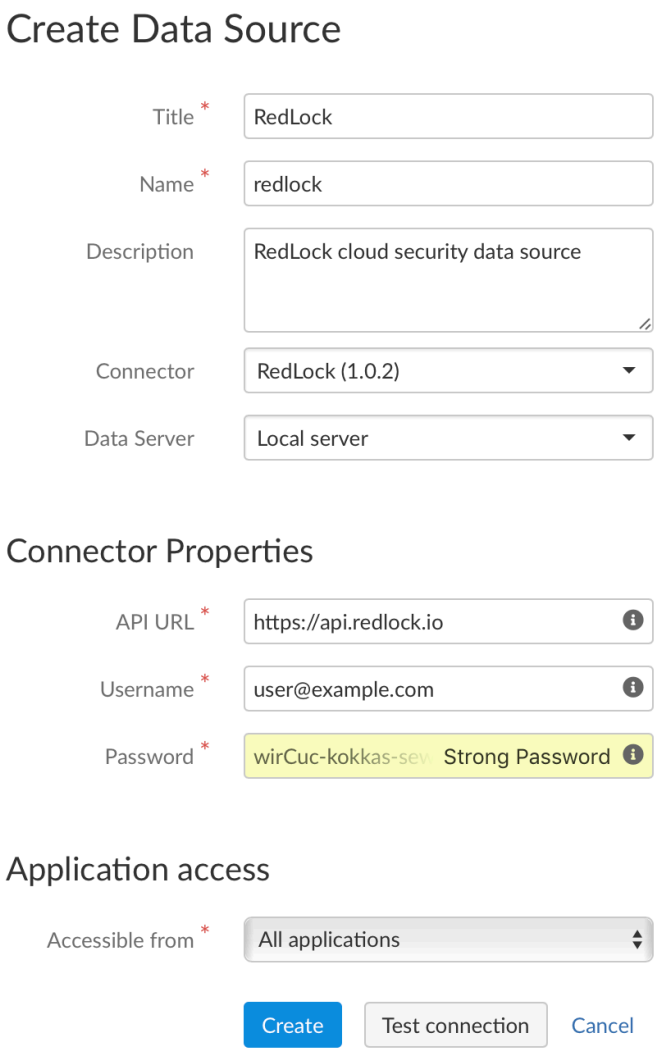
1. Create a read-only user account for Prisma Public Cloud API

   Prisma Public Cloud – Add Users
   https://support.redlock.io/hc/en-us/articles/360000992152-Add-Users

   Prisma Public Cloud – Role Based Access Controls
   https://support.redlock.io/hc/en-us/articles/360001007771-Role-Based-Access-Controls

Partner Product Configuration

1. Configure a Data Source using Brinqa Prisma Public Cloud connector by providing Prisma Public Cloud account credentials



2. Use default mapping to Brinqa data models or adjust to fine-tune Prisma Public Cloud data representation in Brinqa.

Edit Data Mapping

Title * RedLock Alert
Name * redlock_alert
Description RedLock alert mapping.
Order * 2
Options
- [x] Active
- [x] Run business rules
- [ ] Validate attributes
- [ ] Copy blank values

Data Source * RedLock
Source * Alert
Target * Alert
Operation * Create or update
Coalesce *
- (•) Match all coalesce attributes
- ( ) Match any coalesce attribute

Attribute mappings (15)

Add Attribute Mapping | Delete All Attribute Mappings | Auto Map

Order	Source Attribute	Source Type	Target Attribute	Target Type	References	Source Format	Coalesce	Actions
1	Sys ID	String	Sys ID	Text			true	
2	Policy ID	String	Policy	Reference	Sys ID (Text)		false	
3	Account ID	String	Account	Reference	Sys ID (Text)		false	
4	Status	String	Status	Status			false	
5	Cloud platform	String	Cloud Platform	Text			false	
6	Region	String	Region	Text			false	
7	Resource ID	String	Resource ID	Text			false	
8	Resource name	String	Resource Name	Text			false	
9	Resource type	String	Resource Type	Text			false	
10	Resource configuration	String	Resource Configuration	Text			false	
11	Rating	String	Rating	Text			false	

Edit Data Mapping

Title * RedLock Policy
Name * redlock_policy
Description RedLock policy mapping
Order * 2
Options
- [x] Active
- [x] Run business rules
- [ ] Validate attributes
- [ ] Copy blank values

Data Source * RedLock
Source * Policy
Target * Policy
Operation * Create or update
Coalesce *
- (•) Match all coalesce attributes
- ( ) Match any coalesce attribute

Attribute mappings (19)

Add Attribute Mapping | Delete All Attribute Mappings | Auto Map

Order	Source Attribute	Source Type	Target Attribute	Target Type	References	Source Format	Coalesce	Actions
1	Sys ID	String	Sys ID	Text			true	
2	Name	String	Name	Text			false	
3	Description	String	Description	Text			false	
4	Recommendation	String	Recommendation	Text			false	
5	Remediation	String	Remediation	Text			false	
6	Type	String	Type	Text			false	
7	Policy mode	String	Policy Mode	Text			false	
8	Cloud platform	String	Cloud Platform	Text			false	
9	Rule	String	Rule	Text			false	
10	Severity	String	Severity	Text			false	
11	Owner	String	Owner	Text			false	

3. Schedule recurring data sync in Brinqa for the data source created in Step 1.

Troubleshooting

- Common troubleshooting steps
  - Use 'Test Connection' on the data source to validation authentication; the system will report any errors on UI.
- Contact information for support
  - Email: support@brinqa.com
  - Phone: (512)3721004
  - Support Portal: https://brinqa.atlassian.net/servicedesk/customer/portal/4/user/login
- Member of TSA Net
- Resources that may be helpful
  - http://docs.brinqa.io/data-integration/data-sources/

Technical Details

- API calls that are being leveraged
  - Login
    https://api.docs.redlock.io/reference#app-login
  - List Alerts V2
    https://api.docs.redlock.io/reference#get-alerts-v2
  - List Alerts
    https://api.docs.redlock.io/reference#get-alerts
  - List Policies V2
    https://api.docs.redlock.io/reference#get-policies-v2
  - List Policies
    https://api.docs.redlock.io/reference#get-policies
- Additional technical details
  - Brinqa has developed a purpose-built connector for Prisma Public Cloud to integrate Cloud security assessment result findings into Brinqa Cyber Risk Platform, to allow prioritization, automation of response as well reporting. This connector uses Prisma Public Cloud REST API to retrieve data and there are no additional dependencies or requirements.