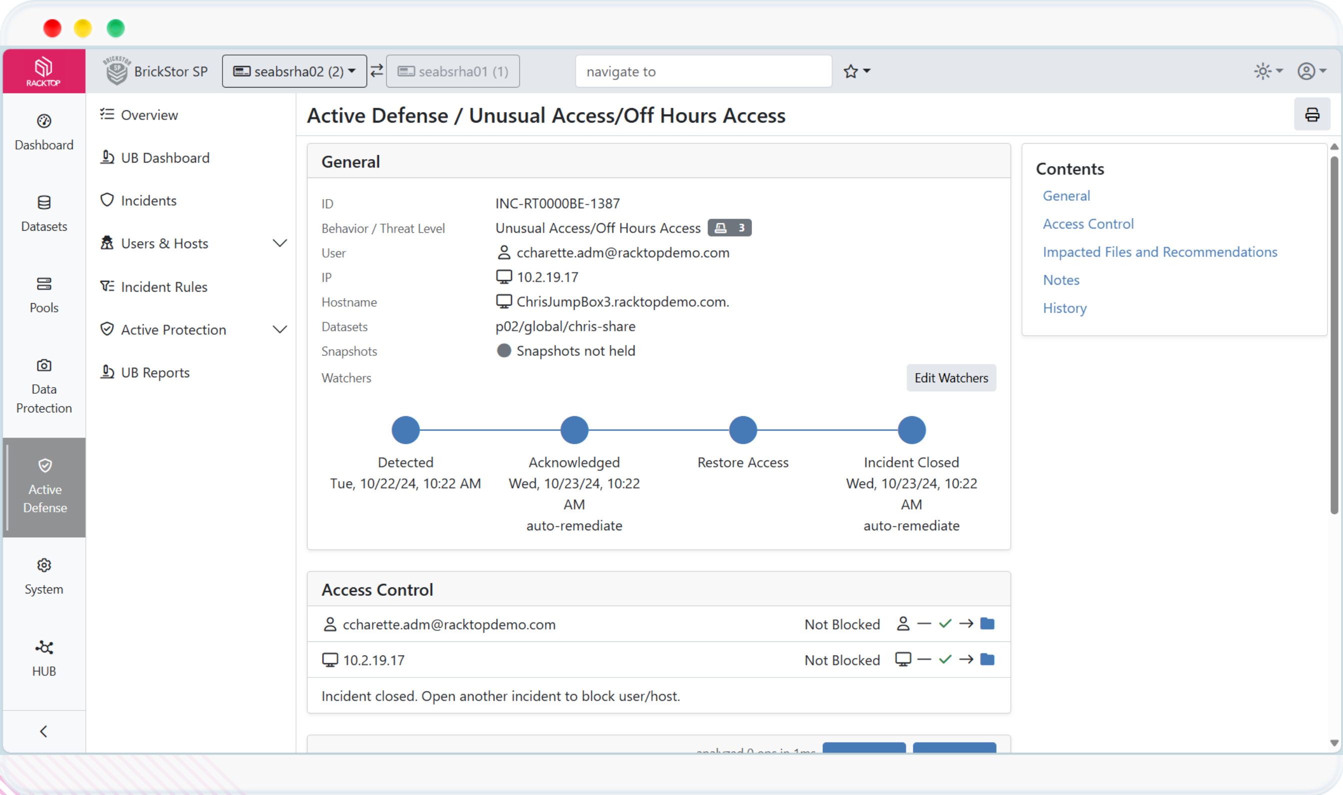
Risk Management Framework (RMF)

Compliance requires implementation of controls, continuous monitoring and enforcement, as well as evidence of controls and enforcement

RMF Overview

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions…;
- Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems; and
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e. common controls).



Active Defense / Unusual Access/Off Hours Access

General

ID	INC-RT0000BE-1387
Behavior / Threat Level	Unusual Access/Off Hours Access 3
User	ccharette.adm@racktopdemo.com
IP	10.2.19.17
Hostname	ChrisJumpBox3.racktopdemo.com.
Datasets	p02/global/chris-share
Snapshots	● Snapshots not held
Watchers	

Detected: Tue, 10/22/24, 10:22 AM

Acknowledged: Wed, 10/23/24, 10:22 AM, auto-remediate

Restore Access

Incident Closed: Wed, 10/23/24, 10:22 AM, auto-remediate

Access Control

ccharette.adm@racktopdemo.com	Not Blocked
10.2.19.17	Not Blocked

Incident closed. Open another incident to block user/host.

Contents

- General
- Access Control
- Impacted Files and Recommendations
- Notes
- History

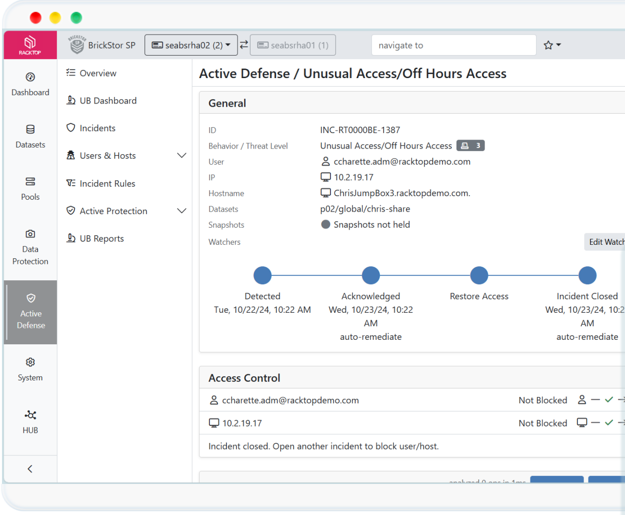
Access control

BrickStor SP Maps to All Relevant Areas of RMF

Example Controls from NIST 800-37, 53, 137

- **Access Controls** – Account Management, Least Privilege, Atypical Usage, Access Enforcement, Information Flow, Support for Attribute Based Access Control (ABAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC), and Mandatory Access Control (MAC)
- **Audit and Accountability** – Content of Audit, Audit Storage Capacity, Timestamps, Review and Analysis, Reduction and Reporting
- **Configuration Management** – Access Restrictions, Signed Software Updates
- **Contingency Planning** – Information System Recovery and Reconstitution
- **Identification and Authentication** – Device Authentication, Authentication Management, Authentication Feedback
- **Media Protection** – Media Sanitization
- **System and Communications Protection** – Security Function Isolation, Cryptographic Key Establishment and Management, Cryptographic Protection, Transmission Confidentiality and Integrity, Protection of Information at Rest
- **System and Information Integrity** – Software Firmware Integrity, Information Handling and Retention

Integrated compliance reports demonstrate ongoing evidence of controls and compliance



Active Defense / Unusual Access/Off Hours Access

General

ID	INC-RT0000BE-1387
Behavior / Threat Level	Unusual Access/Off Hours Access 3
User	ccharette.adm@racktopdemo.com
IP	10.2.19.17
Hostname	ChrisJumpBox3.racktopdemo.com.
Datasets	p02/global/chris-share
Snapshots	Snapshots not held
Watchers	

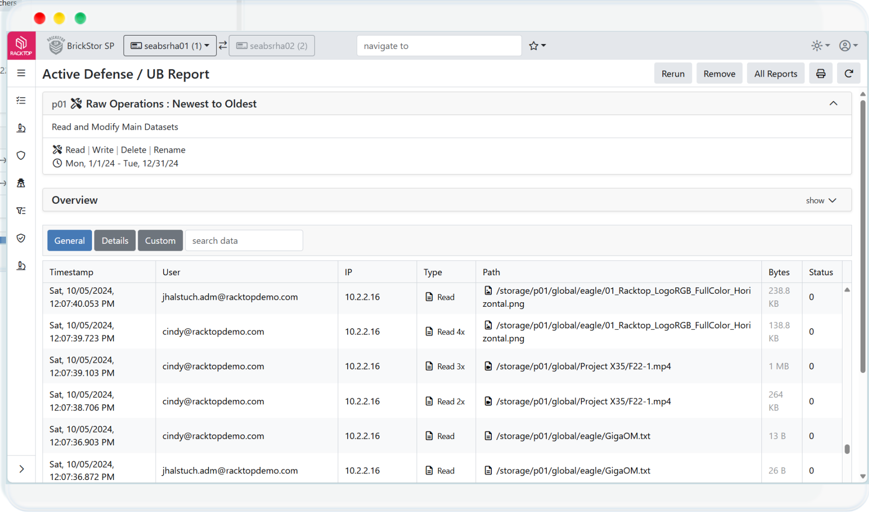
Detected
Tue, 10/22/24, 10:22 AM — Acknowledged
Wed, 10/23/24, 10:22 AM
auto-remediate — Restore Access — Incident Closed
Wed, 10/23/24, 10:2… AM
auto-remediate

Access Control

ccharette.adm@racktopdemo.com	Not Blocked
10.2.19.17	Not Blocked

Incident closed. Open another incident to block user/host.

Audit report



Active Defense / UB Report

p01 Raw Operations : Newest to Oldest

Read and Modify Main Datasets

Read | Write | Delete | Rename
Mon, 1/1/24 - Tue, 12/31/24

Overview

Timestamp	User	IP	Type	Path	Bytes	Status
Sat, 10/05/2024, 12:07:40.053 PM	jhalstuch.adm@racktopdemo.com	10.2.2.16	Read	/storage/p01/global/eagle/01_Racktop_LogoRGB_FullColor_Horizontal.png	238.8 KB	0
Sat, 10/05/2024, 12:07:39.723 PM	cindy@racktopdemo.com	10.2.2.16	Read 4x	/storage/p01/global/eagle/01_Racktop_LogoRGB_FullColor_Horizontal.png	138.8 KB	0
Sat, 10/05/2024, 12:07:39.103 PM	cindy@racktopdemo.com	10.2.2.16	Read 3x	/storage/p01/global/Project X35/F22-1.mp4	1 MB	0
Sat, 10/05/2024, 12:07:38.706 PM	cindy@racktopdemo.com	10.2.2.16	Read 2x	/storage/p01/global/Project X35/F22-1.mp4	264 KB	0
Sat, 10/05/2024, 12:07:36.903 PM	cindy@racktopdemo.com	10.2.2.16	Read	/storage/p01/global/eagle/GigaOM.txt	13 B	0
Sat, 10/05/2024, 12:07:36.872 PM	jhalstuch.adm@racktopdemo.com	10.2.2.16	Read	/storage/p01/global/eagle/GigaOM.txt	26 B	0

User behavior auditing