RAPID7

COMPLIANCE BRIEF

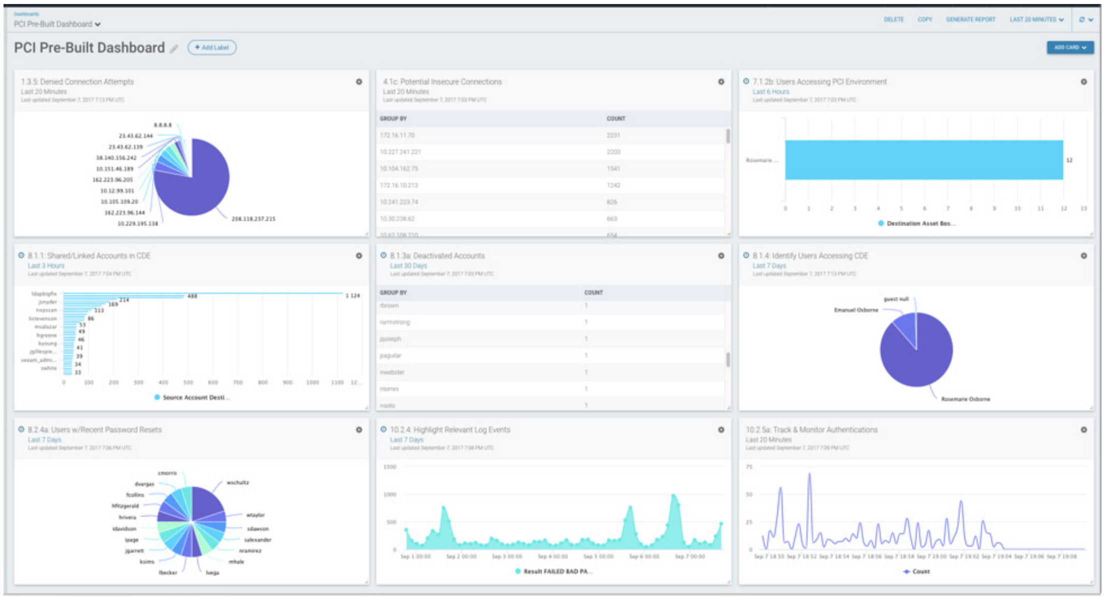
Detect Intruders and Meet PCI Compliance with InsightIDR

InsightIDR is built to find common and targeted threats across your network early in the attack chain—before there's unauthorized access to sensitive data or your cardholder data environment (CDE). In addition to helping you detect and investigate phishing, malware, and the use of stolen credentials, InsightIDR helps you fulfill many obligations mandated under the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS has three core components:

- Assess business processes that deal with cardholder data and potential vulnerabilities.
- Eliminate vulnerabilities as they are discovered; avoid storing credit card data to the fullest extent possible.
- Compile and submit required reports to demonstrate compliance.

InsightIDR, your cloud SIEM for modern detection and response, helps your team comply with multiple facets of PCI DSS across these requirements, including Requirement 10 (tracking and monitoring all access to network resources and cardholder data) and Requirement 11 (testing security systems and processes).



PCI Pre-Built Dashboard

1.3.5: Denied Connection Attempts
Last 20 Minutes
Last updated September 7, 2017 7:13 PM UTC

4.1c: Potential Insecure Connections
Last 20 Minutes
Last updated September 7, 2017 7:03 PM UTC

GROUP BY	COUNT
172.16.11.70	2231
10.227.241.221	2203
10.104.162.75	1541
172.16.10.213	1242
10.241.223.74	826
10.30.238.62	663
10.62.108.210	654

7.1.2b: Users Accessing PCI Environment
Last 6 Hours
Last updated September 7, 2017 7:03 PM UTC

8.1.1: Shared/Linked Accounts in CDE
Last 3 Hours
Last updated September 7, 2017 7:04 PM UTC

8.1.3a: Deactivated Accounts
Last 30 Days
Last updated September 7, 2017 7:03 PM UTC

GROUP BY	COUNT
rbrown	1
rarmstrong	1
pjoseph	1
paguilar	1
nwebster	1
mtorres	1
rsoto	1

8.1.4: Identify Users Accessing CDE
Last 7 Days
Last updated September 7, 2017 7:13 PM UTC

8.2.4a: Users w/Recent Password Resets
Last 7 Days
Last updated September 7, 2017 7:06 PM UTC

10.2.4: Highlight Relevant Log Events
Last 7 Days
Last updated September 7, 2017 7:08 PM UTC

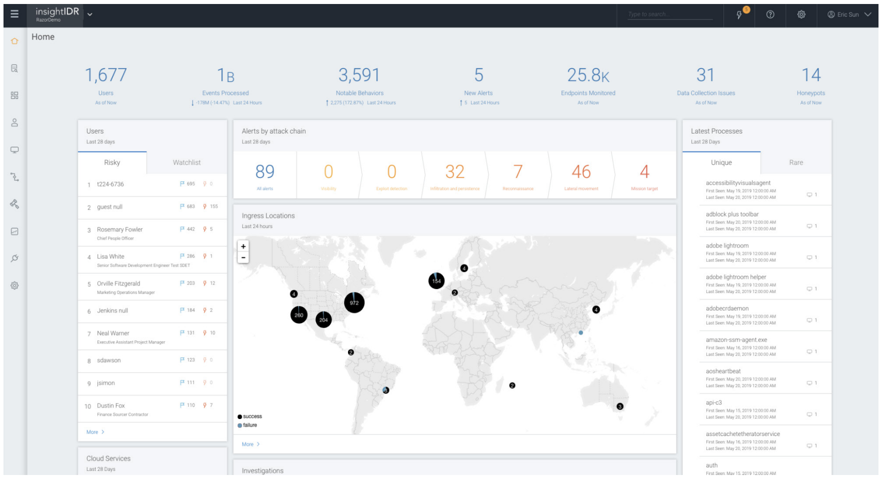
10.2.5a: Track & Monitor Authentications
Last 20 Minutes
Last updated September 7, 2017 7:09 PM UTC

Figure 1: Meet your compliance needs with real-time report cards, flexible search, and User Behavior Analytics.

Here’s a specific breakdown of PCI DSS 3.2.1 by requirement:

COMPLIANCE REQUIREMENT		HOW INSIGHTIDR HELPS SUPPORT
3.5	**Protect cardholder data** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	The included Insight Agent with InsightIDR helps you detect and respond to attacks across Windows, Mac, and Linux assets. InsightIDR supports file integrity monitoring (FIM) and can be used to monitor key and credential files on critical assets.
6.4.1	**Develop and maintain secure systems & applications** Separate development/test environments from production environments, and enforce the separation with access controls.	InsightIDR helps validate that your access control policies are being properly enforced. You can monitor multiple separated environments, define specific zones, and be alerted if access policies are violated. For example, you could set a policy that no users in the “developers” group should access the network zone “PCI Production;” you’ll be notified of any violations.
7.1 7.3	**Implement strong access control measures** Limit access to system components and cardholder data to only those individuals whose job requires such access.	After flagging systems in your CDE as restricted assets, InsightIDR will alert you on any change in behavior. This includes suspicious authentications, users with unexpected privilege escalations, and even approved users remotely accessing the CDE from a new source asset. This detects unauthorized access, risky behavior, and enforces policies set by your security team.
8.1 8.2.4 8.5	**Identify and authenticate access to system components** ● Ensure proper user identification management for non-consumer users and administrators. ● Change user passwords/passphrases at least once every 90 days. ● Do not use group, shared, or generic IDs, passwords, or other authentication methods.	InsightIDR exposes risky user behavior, including shared accounts, unknown administrators, and non-expiring passwords. This visibility into user behavior across your network helps enforce your set security policies. In addition, InsightIDR alerts on password brute forcing, pass-the-hash, and other credential-based attacks by running behavior analytics on event logs and through included deception technology, which includes honeypots, honey users, and honey credentials.
10.1 10.2 10.3 10.5 10.6 10.7	**Track and monitor access to network resources and cardholder data** ● Implement automated audit trails. ● Record audit entries; secure the audit trail. ● Use file integrity monitoring (10.5.5). ● Review logs of all critical system components. ● Review logs of all components that perform security functions. ● Retain audit trail for at least one year, with 3 months readily accessible for analysis.	InsightIDR comes with cloud-native data collection, a powerful search, and pre-built compliance dashboards to help you solve Requirement 10 and give you visibility across your modern network. With your standard InsightIDR subscription, all ingested logs are stored for one year (3 months fully accessible in “hot storage,” 9 months “cold storage”). With Managed Detection and Response (MDR), your logs are retained for audit, compliance, and search for 365 days in hot storage. As a cloud SIEM, data retention across InsightIDR and MDR can be tailored to exactly meet your business and compliance needs.

11.4 11.5	**Test security systems and processes** - Use intrusion detection and/or prevention techniques to detect and/or prevent intrusions into the network. - Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical files.	InsightIDR helps you detect phishing, malware, and the use of stolen credentials— the three most common attacker behaviors behind breaches. InsightIDR also comes with threat intelligence management and fully integrates with your existing firewalls and Intrusion Detection/Prevention Systems (IDS/IPS). Logs from IDS/IPS systems are made fully searchable for investigations and audit. InsightIDR comes with file integrity monitoring, which can be used to detect modifications to critical system files, configurations, and content.
12.5.2 12.10	**Maintain an information security policy** - Monitor and analyze security alerts and information, and distribute to appropriate personnel. - Implement an incident response plan. Be prepared to respond immediately to a system breach.	InsightIDR comes with case management and incident investigation capabilities, including log search, endpoint interrogation, and easy access to user behavior data. Alerts from your existing network and security tools can be fed into InsightIDR and then distributed to teams via email, ticketing systems, or chat tools like Slack. InsightIDR is built for modern threat detection and response and assists from initial detection to containment. Built-in automation in InsightIDR helps teams quarantine potentially compromised users immediately and initiate response plans within seconds of detecting threats.


insightIDR
RazorDemo
Type to search...
Eric Sun
Home
1,677 Users As of Now
1B Events Processed ↓ -178M (-14.47%) Last 24 Hours
3,591 Notable Behaviors ↑ 2,275 (172.87%) Last 24 Hours
5 New Alerts ↑ 5 Last 24 Hours
25.8K Endpoints Monitored As of Now
31 Data Collection Issues As of Now
14 Honeypots As of Now
Users Last 28 days
Risky
Watchlist
Alerts by attack chain Last 28 days
89 All alerts
0 Visibility
0 Exploit detection
32 Infiltration and persistence
7 Reconnaissance
46 Lateral movement
4 Mission target
Ingress Locations Last 24 hours
success
failure
More
Latest Processes Last 28 Days
Unique
Rare
Cloud Services Last 28 Days
Investigations

1	t224-6736	695	0
2	guest null	683	155
3	Rosemary Fowler Chief People Officer	442	5
4	Lisa White Senior Software Development Engineer Test SDET	286	1
5	Orville Fitzgerald Marketing Operations Manager	203	12
6	Jenkins null	184	2
7	Neal Warner Executive Assistant Project Manager	131	10
8	sdawson	123	0
9	jsimon	111	0
10	Dustin Fox Finance Sourcer Contractor	110	7

accessibilityvisualsagent
First Seen: May 19, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

adblock plus toolbar
First Seen: May 20, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

adobe lightroom
First Seen: May 19, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

adobe lightroom helper
First Seen: May 19, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

adobecrdaemon
First Seen: May 19, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

amazon-ssm-agent.exe
First Seen: May 16, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

aosheartbeat
First Seen: May 20, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

api-c3
First Seen: May 15, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

assetcachetetheratorservice
First Seen: May 16, 2019 12:00:00 AM
Last Seen: May 20, 2019 12:00:00 AM

auth
First Seen: May 15, 2019 12:00:00 AM

Figure 2: InsightIDR brings together asset, user, and behaviorial data into a single view.

About InsightIDR

Rapid7 InsightIDR, our cloud SIEM, leverages attacker analytics to detect intruder activity earlier in the attack chain, cutting down false positives and days' worth of work for security professionals. It hunts for actions indicative of compromised credentials, spots lateral movement across assets, detects malware, and sets traps for intruders.

To learn more about InsightIDR or start a free trial, visit www.rapid7.com/insightidr.

Support

call +1.866.380.8113

Customer Portal