Authomize

OpenITDR

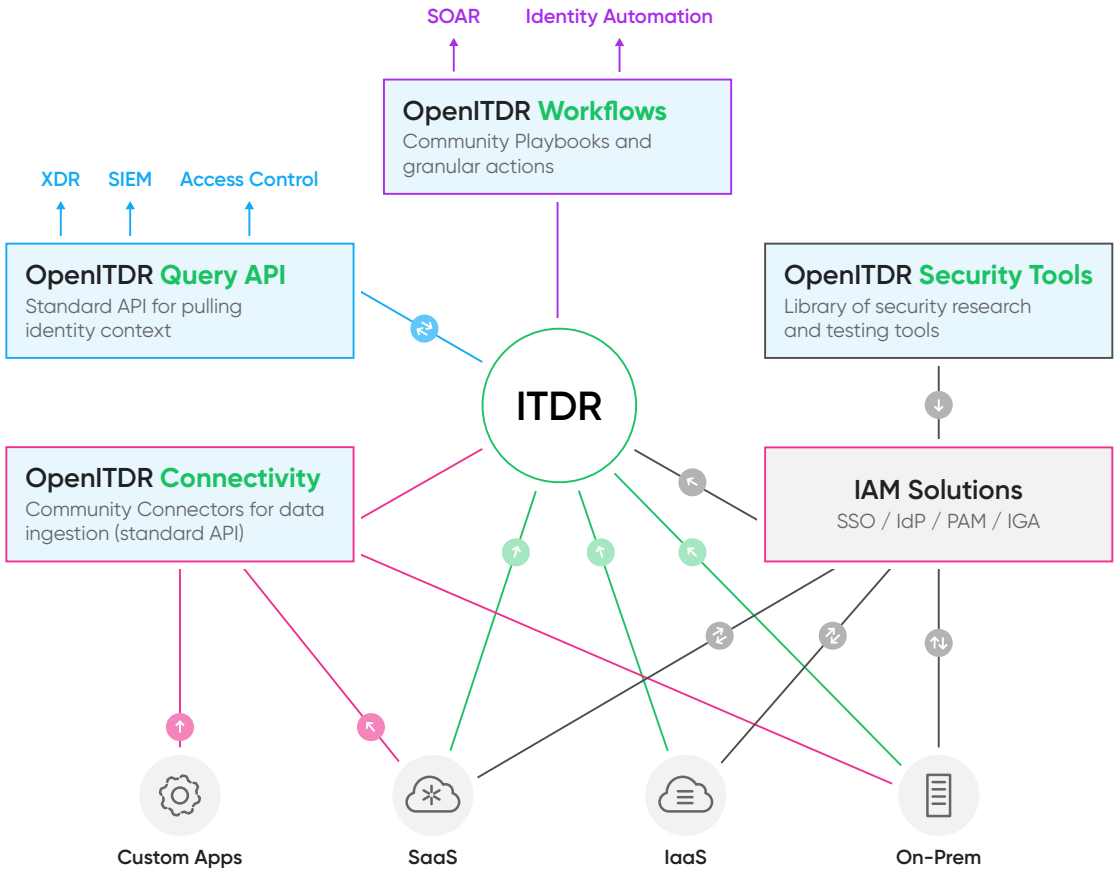
The Open Framework

for the Identity Threat Detection and Response Community

Protecting organizations from Identity-based attacks depends on mounting an effective response. Achieving the necessary level of response is increasingly difficult for security teams as they face a highly distributed identity and access landscape across multiple environments. They are missing the critical, centralized layer of visibility, connectivity, contextual intelligence, and control to effectively detect and remediate risks and mitigate threats to their identity infrastructure.

Introducing the OpenITDR Framework

OpenITDR is a new open framework initiative to ease the path to adoption of Identity Threat Detection and Response (ITDR) tools for all. An open source collection of APIs and playbooks, it will allow organizations to seamlessly integrate ITDR contextual intelligence into every part of their identity plane to streamline remediation of Identity-based threats.



OpenITDR Framework Architecture

Spearheaded by Authomize, OpenITDR is an open framework to connect identity and security that is available on GitHub for ITDR customers, identity vendors, partners, and the wider ITDR community to use and expand upon collectively.

Open Connectors for All Environments

Authomize is offering a REST API-based standard for consumption of identity and access data from any type of service, cloud infrastructure, and application. In addition, a repository of open source connectors based on the aforementioned API that were provided by members of the Open ITDR community is provided for free. The community is encouraged to use the standardized API to develop their own connectors and share with the community, exponentially expanding the reach and utility of ITDR for all.

Open Inquiry API for Rich Context

Enrich systems with contextual identity and access intelligence to drive smarter decision making, aiding in risk scoring and enabling remediation through actionable insights.

Automated Workflows to Streamline Remediation

Build automated workflows to respond effectively to Identity-based risks and threats. Pre-configured playbooks streamline remediations, harnessing automation to save security operations teams valuable time and focus. Authomize is open-sourcing three automated workflows to automatically respond to high-priority risks and threats.

Sample Workflows

- Protect Compromised Okta Users: Return users affected by Okta SCIM application clear text password exposure and exfiltration risk
- Remediate over-privilege in AWS: Refactor AWS access policy to automatically contain risky access and achieve Least Privilege
- Eliminate the risk of exposed Git repositories: Immediately fix public Git repositories that expose sensitive data

Open Sourcing ITDR Tools and Security Research

Alongside the OpenITDR framework's connectors and playbooks, the OpenITDR project will be a place for sharing tools, research, and resources for the benefit of the identity security community. The open source PassBleed testing tool to help detect risky misconfigurations in Okta deployment is available under the OpenITDR repository.

Connecting to Authomize

The OpenITDR framework can be used to connect to any system in the identity infrastructure and to any ITDR vendor. Connecting to Authomize offers several advantages including:

- The most granular identity visibility across all cloud and IAM environments
- The richest contextual data on identity, access privileges, assets, and usage
- Advanced detection capabilities to protect against attacks targeting IAM infrastructure

Learn more about the OpenITDR vision and community by visiting the GitHub repository.