sonraí SECURITY

Enrich Azure Sentinel Security Analytics With

Identity & Data Intelligence From Sonrai Dig

Deliver rich security findings for identity and data governance across Amazon Web Services, Microsoft Azure, and Google Cloud platform from the Sonrai platform to Azure Sentinel.

Give your team a comprehensive view of all issues across your cloud. Correlating intelligence from multiple sources increases the effectiveness of Azure Sentinel. The integration with Sonrai brings a deep understanding of identity and data intelligence, providing additional context around events and unearthing access alerts in a single view.

With an alert-level integration, organizations can send high-impact public cloud security findings seamlessly from Sonrai to Sentinel. The security findings provide your team with a complete view of information across all of your public cloud accounts to identify the severity and urgency of an event.

Microsoft Azure
Azure Sentinel

A Multicloud SIEM Dashboard Enriched with Access Intelligence

Blending Azure Sentinel capabilities with Sonrai Dig public cloud intelligence gives you a unified view for making decisions on incident response. With an easy setup, strong integration, and Sonrai's comprehensive identity-to-data path graphing technology, Sentinel becomes the single command center for administering events on the public cloud.

sonraísecurity.com | info@sonraísecurity.com | 646.389.2262

sonraí SECURITY

How it works

Import Incidents

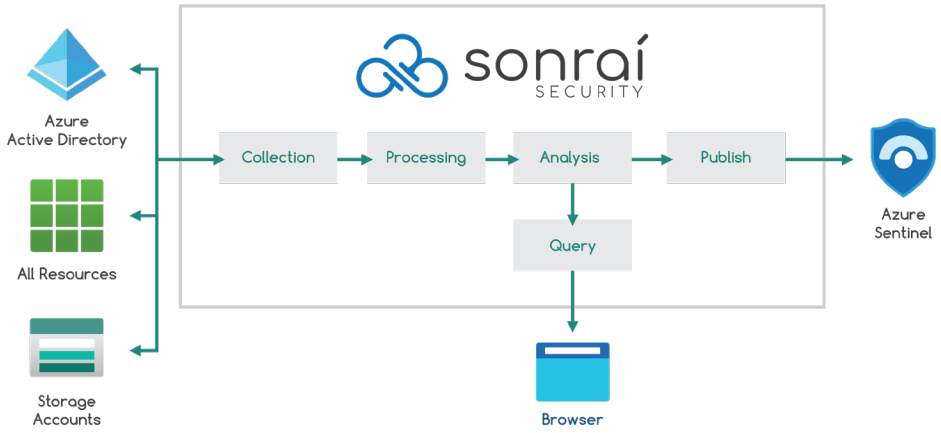
Automatically import alerts and display a native Sentinel dashboard based on Sonrai Dig incidents.

Alert Enrichment

Use Azure Sentinel's native search capability to probe and set up alerting for Sonrai Dig incidents.

Seamless Visibility

Use the Azure Sentinel platform for a single view including high-impact reporting and incidents from Sonrai Dig.



Integration Features & Benefits

- Centralized visibility of all relevant alerts inside Sentinel
- Comprehensive public cloud security findings on identity & data access from Sonrai's patented graphing technology
- Unified command center for all issues across multi-cloud environments

Answer Important Questions

- Who has accessed resources and data?
- Who can access workload data and its components?
- Does the configuration properly protect data if a credential is stolen or mis-used?

Respond & Remediate with Additional Context

- View rich ticket metadata from Sonrai in Sentinel
- Leverage Sonrai's auto-remediation capabilities while managing the ticket from Sentinel
- Leverage Sentinel's automation and orchestration tools with new triggers available via enriched tickets from Sonrai

Connecting is easy!

Connect Sonrai Dig and Azure Sentinel workspaces with an easy-to-use setup wizard. Define what Sonrai events you want to feed into Sentinel, and leverage Sonrai's swimlanes feature to mark the environments that should be integrated with Sentinel.

sonraísecurity.com | info@sonraísecurity.com | 646.389.2262

sonraí SECURITY

sonraí SECURITY

Why Sonrai Security?

As application workloads and critical data migrate to the cloud, the support for security orchestration and automation across people and non-people identities is of increasing importance. Our integration allows Sonrai Security to deliver security, configuration, identity and data relationship findings to Sentinel, bringing complete visibility of the cloud environment to you.

Sonrai's integration with Sentinel allows our joint customers to capitalize further on their current investments, so they can have a clear and automated plan for remediation in a multi-cloud environment, all in one easy-to-read dashboard.

Focus on Meaningful Alerts

The alerts that are delivered by Sonrai Security help your team by providing additional context and allow your team to rank based on urgency and severity.

Assess Policy Change Risk

Relentlessly monitor configuration drift against an approved baseline. Strong audit capabilities of changes to configuration and data access.

Breadth of Resources

The intelligence gathered by Sonrai Security on your public cloud gives your organization the highest level of visibility on your identity and access risk.

Easy Consolidation

Integration with Sonrai Security is quick and easy using Azure Sentinel solutions and Data Connectors. On-boarding is straightforward and focused on increasing your team's productivity.

Mitigate Identity & Data Risk

The combination of Azure Sentinel and Sonrai Security enables organizations to streamline incident management and correlate security alerts across your public cloud so that your organization can mitigate risks effectively.

Want to see Sonrai Security and Azure Sentinel in action? Contact us!

sonraisecurity.com | info@sonraisecurity.com | 646.389.2262

sonraí SECURITY