ENZOIC INTEGRATION WITH ITDR SOLUTIONS

Strengthening Defense Against Dark Web Threats

ITDR

Recent findings from IBM's Cost of a Data Breach Report and Verizon's DBIR have identified compromised credentials as the leading cause of data breaches. For ITDR (Identity Threat Detection and Response) solutions, confronting this vulnerability directly is key to ensuring the safety of end users' environments. Organizations are particularly at risk when credentials are exposed on the Dark Web, making them prime targets for cybercriminals. Enzoic provides an advanced integration of Dark Web intelligence and compromised credential data into these solutions, boosting your competitive edge and your customers' security.

Enhancing ITDR with Enzoic

Real-Time Compromised Credential Monitoring

Enzoic's proprietary tools and threat research team continuously scan the Dark Web and other illicit sources for compromised credentials, providing real-time alerts when users' account details are compromised. This integration enables ITDR solutions to promptly notify end users of compromised accounts, prompting immediate password changes and securing accounts before they can be exploited.

Automated Response and Remediation

Integrating Enzoic allows ITDR solutions to automate responses to compromised credentials. This includes enforced password resets, account lockouts, and MFA enforcement, ensuring that compromised accounts are quickly secured. These proactive measures significantly mitigate the risk of unauthorized access and data breaches.

IP Address Monitoring

Enzoic's integration enhances threat intelligence by continuously scanning the Dark Web and other illicit sources for your exposed IP addresses. This proactive monitoring helps ITDR solutions detect and flag suspicious activity linked to your IPs, allowing for timely alerts and automated responses.

Extending Reach Beyond Endpoints

By incorporating Dark Web data, Enzoic extends the reach of ITDR solutions from merely monitoring user identities to encompassing external sources and deeper areas of the internet. This broader scope enhances overall threat visibility and protection, allowing security solutions to detect and respond to threats originating from outside the organization.

Automated Threat Intelligence Enrichment

Automatically enrich threat intelligence feeds with Dark Web data to provide deeper insights into threats and enhance the context of security alerts.

Business Credit Card and Bank Account Protection

Monitor business credit card numbers and bank accounts for exposure on the Dark Web. Trigger alerts and implement protective measures such as freezing cards or accounts if they appear in compromised data sets, protecting financial assets from fraud.

Incident Response Enhancement

Enzoic's threat intelligence can inform adaptive access control policies, adjusting user permissions in real-time based on detected threats. For example, access to sensitive systems can be restricted if a user's credentials appear on a list of compromised accounts, limiting potential damage.

Password Hygiene and Policy Enforcement

Enzoic's password database integration ensures that strong password policies are enforced and detects the use of compromised passwords in real-time during user creation and password updates. This prevents the use of known compromised passwords, enhancing overall security.

Password Standards Compliance

Organizations can comply with standards such as HITRUST, NIST 800-63b, and NIST IA-5, which require ensuring that passwords are not compromised. This involves monitoring the Dark Web for exposed credentials to prevent the use of compromised passwords.

Insider Threat Detection

Monitor Dark Web data for mentions of internal employee data being sold or discussed, which might indicate an insider threat or data leakage, allowing for early detection and response.

YOUR COMPETITIVE ADVANTAGE

Contemporary compliance standards and industry research show the important role of compromised credentials in data breaches. As organizations prioritize this area of risk, the integration of Enzoic's enhanced security features into ITDR solutions is increasingly necessary. By addressing credential-based threats comprehensively, these solutions align with market demands for robust security measures, thereby driving higher sales and revenue for ITDR providers. Additionally, incorporating Enzoic's Dark Web data helps providers stay competitive with other solutions that are beginning to include this functionality.

ITDR solutions can stay ahead of attackers by providing the best protection and peace of mind to their end users.