Identity Detection & Response (IDR)

Delivers the data and team to detect and stop possible identity-based risks

With the cloud enabling access to data and applications from any device, the user identity has become the most valuable information for an attacker to capture.

Once an account is compromised, even worse if it has privileged administrative access, malicious actors have an open door into the network gaining access to more accounts, systems, and data and compromising them along the way.

Gartner predicts that at least 99% of cloud security failures will result from business security inadequacies versus an oversight from the cloud provider.

Focusing on strengthening identity security will ensure that only authorized users have access to the data they need and prevent malicious actors from compromising corporate accounts and spreading laterally throughout the network.

Identity Detection and Response (IDR) delivers complete visibility, protection, and response by ProArch's SOC for on-premises Active Directory accounts and cloud-native identities to stop account and credential-based threats.

WHAT'S INCLUDED?

Identity Threat Detection & Investigation:
24x7 SOC monitoring for suspicious user behavior using machine learning-based analytics that enable effective threat investigation and remediation.

24x7 Account Monitoring & Response:
ProArch SOC monitors on-premises Active Directory accounts and cloud-native identities for compromise.

Conditional Access & Privileged Identity Governance:
Implementation of access control policies to block risky log-in attempts and role-based activation alerts to mitigate misused access permissions on critical resources.

Security Incident Response:
Seamless transition to Incident Response (IR) Team including architecture experts and engineers that rebuild compromised systems and data.

ADDED BENEFITS

- ProArch SOC investigates and remediates suspicious user activities and advanced attacks
- Gain visibility and apply conditional access to policies to protect privileged accounts that have top-level access to corporate data
- Uncover vulnerabilities in account setup configuration
- Mitigate risky sign-ins by blocking or requiring multi-factor authentication challenges
- Threat intelligence that turns raw data into contextual information about attackers strategy so controls can put in place
- Protect against identity and credential-based threats
- Quarterly report with recommendations to remediate identity weaknesses and vulnerabilities

Managed Detection and Response (MDR) Services

Skilled Security Teams and Advanced Threat Intelligence that Stop Attackers in Their Tracks

To outsmart attackers, speed is everything. When threats are detected earlier, the risk of a destructive breach is mitigated and your cyber resilience improves.

Without the technology, budget, skillset, and methodology to rapidly identify threats before they become an incident—cybercriminals have the advantage.

Managed Detection and Response (MDR) services from ProArch takes on the responsibility of investigating and responding to security threats before additional accounts or systems are compromised. ProArch's Security Operations Center (SOC) Analysts act as an extension of your team working 24x7 to stop malicious actors from impacting productivity, reputation, and confidential information.

Endpoint Detection & Response (EDR)

Keep threats off devices that are a clear path to corporate resources

Identity Detection & Response (IDR)

Prevent corporate account compromises that lead to data breaches

Extended Detection & Response (XDR)

Stop threat activity across the IT environment and custom log sources

- **We perform complex 24x7 threat monitoring and response** so you don't have to
- **Rapid deployment in under 24 hours** supported by 100% cloud-native toolset
- **Speed threat detection and response times** with threat intelligence, next-gen SIEM and SOAR, and AI-driven automation
- **Have a predictable security spend** and improve return on security investment
- **Deliver reports to leadership** backed by data and expert guidance
- **Protect data** and comply with regulatory compliance requirements
- **Seamless transition to Incident Response Team** if an incident occurs

At ProArch, our customers are confident in our ability to manage security risks effectively and protect their data against potential threats. With an ISO 27001 certification, we demonstrate our commitment and adherence to the highest standards of information security. Your security is our number one priority.

proarch

letstalk@proarch.com · **proarch.com**

United States:
Atlanta, Georgia
Rochester, New York
Syracuse, New York

Europe & Asia:
London, United Kingdom
Bangalore, India
Hyderabad, India