# DARK WEB MONITORING

**Whether you've experienced a data breach, seen exfiltration through your own investigations, or simply want to know if your organization's information is out on the Dark Web, the Arete Cyber Threat Intelligence (CTI) team can help.**

## WHY HAVE ARETE MONITOR THE DARK WEB FOR YOU?

The Dark Web is where threat actors collaborate, share information, and buy and sell a variety of illicit products, services, and compromised data. Unfortunately, this could mean your sensitive or proprietary company data is at risk.

The Arete Cyber Threat Intelligence (CTI) team understands the geography of the Dark Web as well as the behaviors and patterns of cybercriminals. They know what threat actors exploit and how they monetize what they've stolen. And they have the resources to find stolen or disclosed data, contextualize risks, and recommend options for remediation, as necessary.

Based on client specification, the Arete CTI team monitors the Dark Web for threat actors discussing, selling, or disclosing proprietary information, such as:

| Access Credentials | Business Data | Hidden Threats |
|---|---|---|
| Domain account credentials | Intellectual property, trade secrets | Insider fraud and threats |
| User IDs and passwords | Sensitive information | Software/hardware vulnerabilities |
| Admin accounts | PII, PHI, HR data | Zero-day threats |
| Network access | Competitive/brand data | Industry-specific threats |
| Third-party service accounts | Data stolen post incident | Domain abuse detection |
| Business accounts | Financial/insurance documents | Brand attacks or impersonation |

## THE PROCESS OF DARK WEB MONITORING

The Arete CTI team monitors the Dark Web to help reduce your overall risk exposure. They have an established presence on cybercrime forums and communities and searches for instances where threat actors may, for example, be:

- Auctioning off or displaying client information.
- Freely sharing or selling fraud tutorial guides targeting specific organizations.
- Recruiting partners for cybercrime operations or development needs.

# DARK WEB MONITORING

Arete

## THE BENEFITS OF DARK WEB MONITORING

- Understanding risk exposure from actors operating on the Dark Web.
- Understanding how threat actors monetize stolen information.
- Enhanced protection against external threats via continual detection of exposed assets.
- Contextualization of risks related to discovered data.
- Options for remediation.

## POTENTIAL REPERCUSSIONS WITHOUT DISCOVERY OF DATA ON DARK WEB

- Actors leveraging stolen credentials to access your environment to deploy ransomware.
- Actors continuing to steal money from your organization because they know a way to bypass a fraud control.
- Actors accessing your customer's accounts to commit financial fraud or identity theft.
- Actors leveraging your environment to target third parties.

## THE DELIVERABLES

**The Arete CTI team delivers a formal Cyber Risk Exposure Assessment report that summarizes findings based on search criteria and schedules a key stakeholder meeting to provide additional context and discuss remediation options.**