HEROIC.COM

ENTERPRISE PROPOSAL

Prepared For: ACD Direct

HEROIC Cybersecurity
Prepared by Chad Bennett, CEO
801-358-5536
chad@heroic.com

Company: Plante Morane
Headquarters: Southfield, Michigan
Primary Use Case: Penetration testing and cybersecurity reviews by internal security teams. Company protection.

Plan	Start Date	Total Price
DarkWatch Core Plan 1-YR	**[May-2025]**	**$10,000 / year**

Platform Benefits and Limits

- Full access to the online platform, APIs, and monitoring functionality
- 10 Monitored Identities (Domains, IP Addresses, etc)
- 3 admin user accounts (Admin access to the software)
- API access with 5,000 API credits per month
- Ad Hoc Searches per Month - 100
- Real-time alerting when monitored identities have discovered in breaches
- 24/7 Online Support
- Custom Reporting

Data Handling & Compliance

- All data access and usage must comply with applicable privacy laws and HEROIC's terms of service.
- Results are for internal security purposes only and may not be redistributed or resold.

Onboarding & Support

- HEROIC will provide onboarding documentation, API keys, and technical support for integration.
- Usage reporting and account management dashboards will be available to designated administrators.

Agreement

By signing below, both parties agree to the terms and conditions outlined in this Statement of Work ("SOW") and acknowledge that this SOW is governed by the HEROIC Enterprise Terms of Service, available at https://heroic.com/enterprise-software-terms/, which are incorporated herein by reference.

This SOW, together with the applicable Terms of Service and any referenced addenda or policies, constitutes the entire agreement between the parties with respect to the services described herein and supersedes all prior or contemporaneous communications, whether oral or written, relating to such subject matter.

IN WITNESS WHEREOF, the parties have executed this Statement of Work as of the date(s) written below.

Company

Full Name (print):

Signature:

Title:

Date:

HEROIC Cybersecurity

Full Name (print):

Signature:

Title:

Date:

Payment Terms

Invoices will be issued annually in advance unless otherwise agreed in writing. Payment is due immediately to initiate service, and the official start date of the service will be upon receipt of payment. Late payments may be subject to interest and/or suspension of service as outlined in the Terms of Service.

THE SILENT THREAT

HOW COMPROMISED LOGIN CREDENTIALS ARE PUTTING YOUR BUSINESS AT SIGNIFICANT RISK

In 2024 alone, **over 35 billion** online records were exposed across over 11,000+ confirmed data breaches targeting businesses across every major industry, including healthcare, finance, technology, and government. These stolen records, including usernames, passwords, and personal data are now circulating among cybercriminals on the dark web. Many of these breaches went undetected for weeks or months

Alarmingly, **nearly 9 in 10 U.S. companies (92%)** have had their information compromised by a data breach, many without ever knowing it. These exposed login credentials act as digital master keys for hackers, unlocking access to core systems

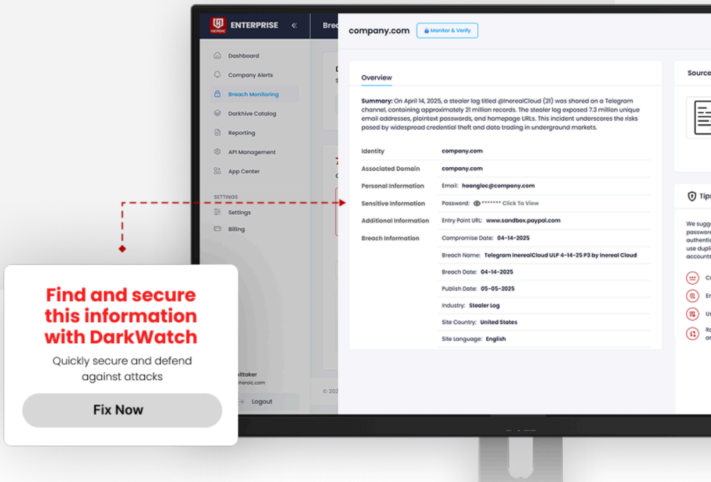
WHAT THEY HAVE ACCESS TO

- **Corporate email systems** to intercept sensitive communications and launch phishing attacks
- **Internal networks and cloud platforms** such as Microsoft 365, Google Workspace, and AWS
- **Finance and payroll systems** to divert payments, access bank accounts, or commit wire fraud
- **Customer databases and CRMs**, risking mass data exposure and compliance violations
- **Vendor and supply chain portals**, enabling attackers to move laterally across organizations
- **Admin accounts and privileged systems,** granting unrestricted access to critical infrastructure

Once accessed, hackers can commit identity theft, financial fraud, and even use compromised accounts for further attacks — resulting in potentially **devastating personal and business consequences.**

”81% of security breaches involve leveraging weak or stolen login credentials.”

— Verizon Data Breach Investigations Report, 2025



Summary: On April 14, 2025, a stealer log titled @InerealCloud (21) was shared on a Telegram channel, containing approximately 21 million records. The stealer log exposed 7.3 million unique email addresses, plaintext passwords, and homepage URLs. This incident underscores the risks posed by widespread credential theft and data trading in underground markets.

Identity	company.com
Associated Domain	company.com
Personal Information	Email: hoangloc@company.com
Sensitive Information	Password: ******* Click To View
Additional Information	Entry Point URL: www.sandbox.paypal.com
Breach Information	Compromise Date: 04-14-2025
	Breach Name: Telegram InerealCloud ULP 4-14-25 P3 by Inereal Cloud
	Breach Date: 04-14-2025
	Publish Date: 05-05-2025
	Industry: Stealer Log
	Site Country: United States
	Site Language: English

Find and secure this information with DarkWatch

Quickly secure and defend against attacks

Fix Now

GET REAL-TIME DEFENSE AGAINST COMPROMISED DATA

TAKE BACK CONTROL

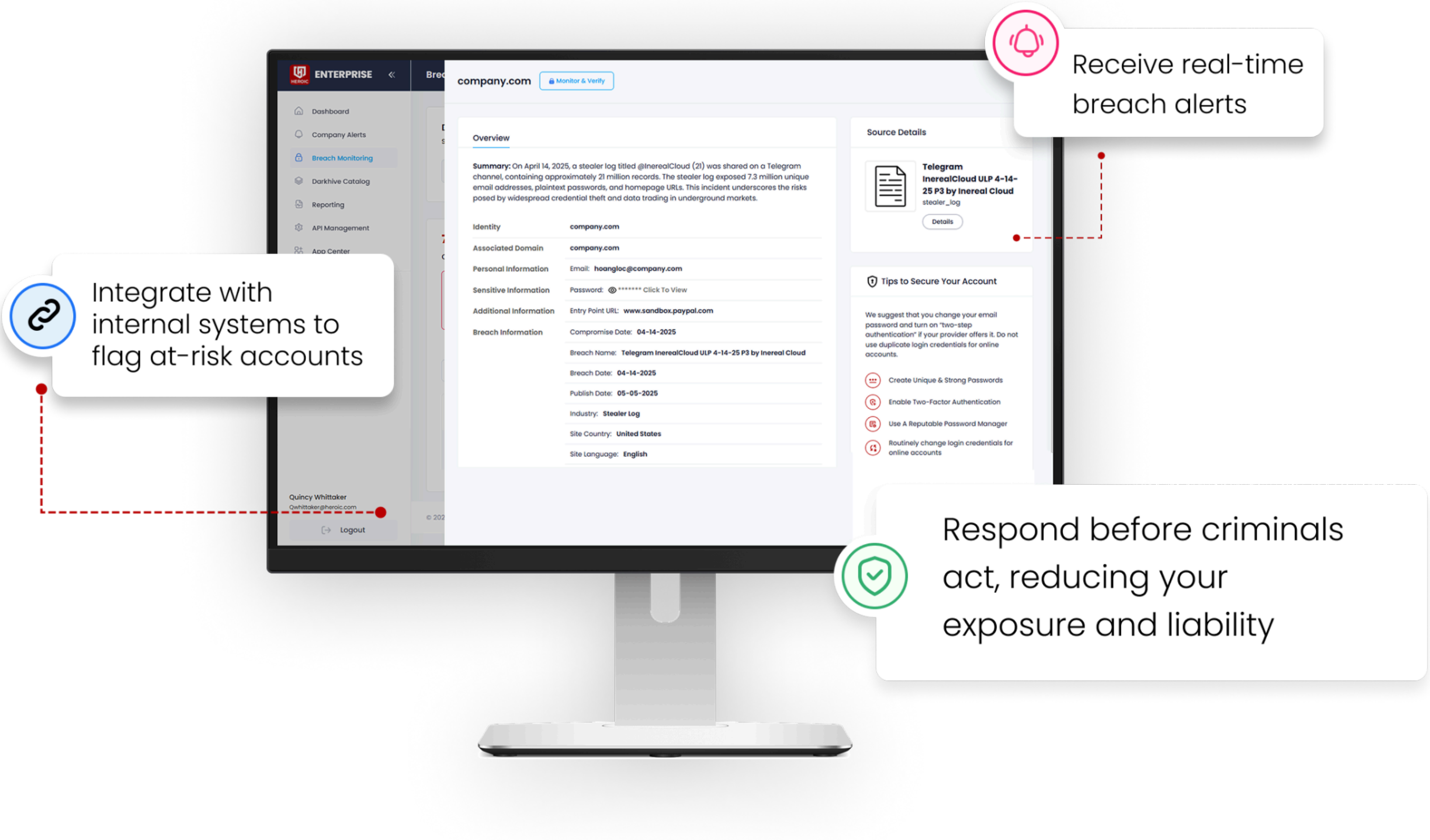
With access to over 100+ billion breached identity records and tens of thousands of confirmed breach sources, HEROIC actively monitors the dark web and criminal data exchanges to identify stolen data across thousands of databases and hacking sites.

IDENTIFY STOLEN

- Employee login credentials
- Customer emails and passwords
- Vendor and partner data
- Domain-specific data tied to your company

By detecting and responding to threats earlier, HEROIC reduces exposure windows — and empowers proactive, not reactive, cybersecurity.

Partner with HEROIC to monitor, detect, and defend against data exposure — before it turns into a breach.



company.com

Summary: On April 14, 2025, a stealer log titled @InerealCloud (21) was shared on a Telegram channel, containing approximately 21 million records. The stealer log exposed 7.3 million unique email addresses, plaintext passwords, and homepage URLs. This incident underscores the risks posed by widespread credential theft and data trading in underground markets.

Identity	company.com
Associated Domain	company.com
Personal Information	Email: hoangloc@company.com
Sensitive Information	Password: ******* Click To View
Additional Information	Entry Point URL: www.sandbox.paypal.com
Breach Information	Compromise Date: 04-14-2025
	Breach Name: Telegram InerealCloud ULP 4-14-25 P3 by Inereal Cloud
	Breach Date: 04-14-2025
	Publish Date: 05-05-2025
	Industry: Stealer Log
	Site Country: United States
	Site Language: English

Source Details

Telegram InerealCloud ULP 4-14-25 P3 by Inereal Cloud
stealer_log

Tips to Secure Your Account

We suggest that you change your email password and turn on "two-step authentication" if your provider offers it. Do not use duplicate login credentials for online accounts.

- Create Unique & Strong Passwords
- Enable Two-Factor Authentication
- Use A Reputable Password Manager
- Routinely change login credentials for online accounts

Receive real-time breach alerts

Integrate with internal systems to flag at-risk accounts

Respond before criminals act, reducing your exposure and liability

INTELLIGENTLY PROTECT YOUR BIGGEST RISK:

PROTECT COMPROMISED LOGIN CREDENTIALS

Unmatched Breach Coverage

Access one of the world's most comprehensive breach intelligence platforms—over 100 billion data points and records from tens of thousands of confirmed incidents.

Seamless API Integration

Easily integrate HEROIC's powerful API into your existing cybersecurity platforms, applications, or internal tools — no friction, no complexity.

Effortless Data Discovery

No internal team required. Our breach database is continuously updated, allowing you to instantly search for compromised data across billions of records.

Credential Monitoring at Scale

Continuously monitor employee, customer, and vendor credentials across compromised platforms to prevent account takeovers and lateral movement.

Automated Threat Monitoring

Automatically scan your users, employees and customers against newly discovered breaches in real-time — providing proactive defense without manual intervention.

Actionable Intelligence

Get instant visibility into exposed accounts, risk levels, and areas requiring immediate attention to strengthen your organization's security posture.

Export Support

Our team is here to guide your team through every step of implementing DarkWatch — helping you intelligently protect your biggest risk: compromised credentials.

AI-Powered Insights

Leverage AI to prioritize critical exposures, detect account reuse, flag high-risk users, and predict threats based on real-time behavior and breach trends.

DON'T WAIT FOR THE DAMAGE TO APPEAR IN YOUR HEADLINES.

DETECT AND RESPOND TO THREATS EARLIER WITH HEROIC ENTERPRISE