Hosted by **ENTERPRISE LEADERSHIP NETWORK (ELN)**
at **MONTEREY PLAZA HOTEL & SPA**

ELN

2023

Cybersecurity, Privacy and Data Protection Retreat

eDiscovery & Information Governance Retreat

Monterey Plaza Hotel & Spa, Monterey CA

Tuesday - September 12, 2023

Monterey Plaza
Hotel & Spa

Agenda

Tuesday - September 12, 2023
Panel Discussions

8:30-9:20AM - Carmel 1
50-Minute Panel Discussion

Organizations Will Invest in Meta-Data Management

Metadata can be a great source of information that explains the what, where, and who, questions of data sorting. This piece of information can also answer the questions - how, when and why, when that piece of information is accessed by anybody in the organization. When metadata is managed and actively used, it can help provide great insights, and solution providers that simplify metadata management will be able to provide value to organizations.

Moderator: Kyle Kelly, Founder and CEO at preDiscovered
Panelist: David Plotkin, Manager of Metadata Services at MUFG Union Bank
Panelist: Aarti Ramanan, Sr. Project Manager - Data Governance | CDO at MUFG
Panelist: Sriram Rangarajan, Sr. Manager-Data & AI at Accenture
Panelist: Nitin Singhal, VP of Engineering at SnapLogic
Panelist: Senguttuvan Thangaraju, Enterprise Data Management Leader at Splunk
Panelist: Weiwei (Victoria) Xie, Senior Loan Accountant at Mosaic

8:30-9:20AM - Carmel 2
50-Minute Panel Discussion

Cyber Risk Management Will be a Top Priority for Business Leaders in 2023

When it comes to the governance and oversight of cyber risk, our system is broken. It'sno longer what it used to be fifteen years ago - we are dealing with higher stakes and fragile enterprise reputations. As a result of this, in 2023, we will see companies double down on cyber risk management. Boards will need to have a much clearer role and responsibility when it comes to the process of ensuring adequate controls and reporting cyberattacks. Cyber risk governance is not just the domain of the CISO it is now clearly a Director and Officer level concern. When it comes to cyber, plausible deniability is dead. Join us, as we discuss best practices for cyber risk.

Moderator: Edwin Covert, Head of Cyber Risk Engineering at Bowhead Specialty
Panelist: Fred Cohen, CEO at Management Analytics
Panelist: Pasha Sternberg, Partner (Principal) at Polsinelli
Panelist: Jay Schneider, Senior Information Technology Security Officer at Vantage Systems, Inc.
Panelist: Kamran Salour, Partner at Lewis Brisbois

Continued on next page

8:30-9:20AM - Big Sur 1 & 2
50-Minute Panel Discussion

Artificial Intelligence and Its Impact

With AI being introduced in all market segments, this technology with a combination of machine learning has brought tremendous changes in cybersecurity. AI has been paramount in building automated security systems, natural language processing, face detection, and automatic threat detection.

Although, it is also being used to develop smart malware and attacks to bypass the latest security protocols in controlling data. AI enabled threat detection systems can predict new attacks and notify admins for any data breach instantly.

Moderator: Benjamin Brink, IMAC Technician III at Milestone Technologies, Inc.
Panelist: Greg Leighton, Shareholder at Polsinelli
Panelist: Steve Millendorf, Partner at Foley & Lardner LLP
Panelist: Jordan MacAvoy, Founder and CEO at TalPoint
Panelist: Megan Bell, CISO at Contra Costa Health Services
Panelist: Paul Starrett, Founder at PrivacyLabs

9:20-9:35AM - Fairway Hospitality
15-Minute Exhibit Hall Break (Visit w/Exhibitors)

9:35-10:25AM - Carmel 1
50-Minute Panel Discussion Sponsored by Complete Discovery Source

Technology Solution Update from Corporate, Law Firm and Service Provider Perspective

eDiscovery and information governance is directly impacted by the technologies available to teams that need them. Technology has come a long way, but it still poses challenges. This panel will talk about current challenges (e.g. mobile devices and BYOD) and technologies like Office 365 are both solving problems and creating new ones.

Sponsor: Complete Discovery Source
Moderator: William Wallace Belt Jr., Managing Director at Complete Discovery Source
Panelist: Paul E. Petruska, Attorney at Law at Greensfelder, Hemker & Gale, P.C.
Panelist: Jim Dowell
Panelist: Robert D. Snow Jr., Counsel-Litigation Support Group at Federal Deposit Insurance Corporation
Panelist: Vanessa Quaciari, Senior eDiscovery Counsel at Baker Botts
Panelist: Brandon Carney, Founder and CEO at Divergent Language Solutions

9:35-10:25AM - Carmel 2
50-Minute Panel Discussion Sponsored by Token

The Rise of Double-Extortion Ransomware

Ransomware has been a growing threat in recent years. A number of high-profile attacks demonstrated to cybercriminals that ransomware was profitable, driving a rapid increase in cybercrime groups operating this malware.

The ransomware industry has also experienced numerous innovations in recent years. Ransomware as a Service (RaaS) operators develop and sell ransomware, expanding their reach and providing less sophisticated threat actors with access to high-quality malware.

Another recent trend is the "double extortion" ransomware campaign. Instead of simply encrypting files and demanding a ransom for their recovery, ransomware groups now steal sensitive and valuable data from their victims as well. If the target organization does not pay the ransom, this data is posted online or sold to the highest bidder.

In 2023, ransomware attacks continued to grow in popularity, and more groups are switching to the "double extortion" model. For example, the relatively new DarkSide group uses this technique and has carried off attacks like the one against Colonial Pipeline that was deemed a national emergency in the U.S.

Join us as we discuss best practices for detecting ransomware activity.

Sponsor: Token
Moderator: Tim Leow, Vice President of Sales at Token
Panelist: Zach Grieshop, CISO at PlayOn! Sports
Panelist: Jerome Prescod, Snr Program Manager Content Security at The Walt Disney Company
Panelist: Chris Loehr, EVP at Solis Security

Continued on next page

9:35-10:25AM - Big Sur 1 & 2
50-Minute Panel Discussion

Privacy Isn't About Compliance - It's About the Economy Stupid

Data is an asset, which depreciates very quickly. The need for businesses to protect their ability to collect data, and use data, is really what should drive privacy compliance.

While the law does generate risks around data use, the real risk is the simple fact that if you don't respect the privacy rights of individuals, you will dilute, or even destroy, ongoing access to high-quality, relevant, and monetizable data.

Fundamentally, privacy programs are about how to effectively monetize data over a strategic time period without adding unnecessary "taxes" onto the data ecosystem (either for the business OR for the data subject).

Moderator: Michael Gregson, Business Analyst – Data Privacy at Waste Management
Panelist: Liz Harding, Shareholder, Vice Chair Technology Transactions and Data Privacy at Polsinelli
Panelist: Matt Linde, President at Privily
Panelist: Peter McLaughlin, Partner at Armstrong Teasdale LLP
Panelist: Chris Hydak, Assistant General Counsel at Microsoft

10:25-10:40AM - Fairway Hospitality
15-Minute Exhibit Hall Break (Visit w/Exhibitors)

10:40-11:30AM - Carmel 1
50-Minute Panel Discussion Sponsored by TackleAI

Leveraging AI for Discovery

How is AI currently being used in discovery and where it may go in the future? What are the potential benefits and risks to be considered? We'll also discuss the differences between analytics, machine learning and AI.

Sponsor: TackleAI
Moderator: Tom Spaulding, Vice President of Tech Sales at TackleAI
Panelist: Sergio Suarez Jr., Founder and CEO at TackleAI
Panelist: Alexis Leah Hayman, Customer Success Manager at ECFX
Panelist: Eric Wieder, eDiscovery Counsel at Baker Botts
Panelist: Ausra O. Deluard, Partner at Dentons
Panelist: Jim Barrick, eDiscovery and Investigations Consultant at Cohesity
Panelist: Marnie Carter, Manager of Legal Operations at Starwood Property Trust

10:40-11:30AM - Carmel 2
50-Minute Panel Discussion Sponsored by Hoxhunt

Building a Security-Aware Culture in 2023 and Beyond

Perhaps the most important step that can be taken at any organization is to ensure that it is working towards initiating and fostering a culture of awareness around cybersecurity issues. Today, it's no longer good enough for employers or employees to simply think of cybersecurity as an issue for the IT department to take care of. In fact, developing an awareness of the threats and taking basic precautions to ensure safety should be a fundamental part of everyone's job description in 2023!

Phishing attacks rely on "social engineering" methods to trick users into divulging valuable information or installing malware on their devices. No one needs technical skills to learn to become aware of these types of attacks and to take basic precautions to avoid falling victim. Likewise, basic security skills like the safe use of passwords and developing an understanding of two-factor authentication (2FA) should be taught across the board and continually updated. Taking basic precautions like this to foster a culture of cybersecurity-awareness should be a core element of business strategy at organizations that want to ensure they build resilience and preparedness over the coming 12 months.

Sponsor: Hoxhunt
Moderator: Jeff Platon, Chief Marketing Officer at Hoxhunt
Panelist: Bill Dougherty, Chief Information Security Officer at Omada Health
Panelist: Andre Samokish, Privacy Manager at Teladoc Health
Panelist: Austine J. Ohwobete, Cybersecurity Strategizing & Litigation at Cryptoforensics Technologies Corporation
Panelist: Chirag Shah, Information Security Officer & DPO at Model N

10:40-11:30AM - Big Sur 1 & 2
50-Minute Panel Discussion

Cybersecurity Training

In 2023, will we see continued advances in cybersecurity training? Humans didn't evolve to spot dangers in the digital world. The school system doesn't teach them defense against the dark arts of

Continued on next page

cyber-attack. It's on us. Human risk is an organizational problem. Equipping our people with the skills to stay safe from phishing attacks is our responsibility.

Automation, adaptive learning, and artificial intelligence/machine learning can help deliver personalized training at scale. Why is that important? Because people need to participate frequently with relevant training that stays at the edge of their skill level in order to improve and stay engaged. A long, dry video followed by a punishment-based phishing simulation has been proven not to work. Fixating on failure leads to failure. Rewarding people as they acquire skills in a dynamic learning environment confers measurable improvement. This approach broadly describes gamification, whose demonstrated success is grounded in established principles of behavioral science and business and will be key to protecting organizations of all sizes in the year ahead.

Moderator: Robert Kirtley, Director of Cybersecurity at iDiscovery Solutions
Panelist: Bob Fabien Zinga, CO at USNR
Panelist: Sam Lyhin, Founder at LSCP, LLC
Panelist: Ayman Elsawah, Fractional CISO and Founder at Cloud Security Labs
Panelist: Doug Simmons, CEO at Influen8

11:30-11:45AM - Fairway Hospitality
15-Minute Exhibit Hall Break (Visit w/Exhibitors)

11:45-12:35PM - Carmel 1
50-Minute Panel Discussion

Zero Trust - Another Security Buzzword or a Real Paradigm Shift?

Zero trust is gaining momentum as organizations increasingly reject outdated perimeter-based strategies. As organizations have begun to adopt a zero trust strategy, many best practices and lessons learned have emerged. At the same time, there are numerous misperceptions surrounding zero trust, especially with regard to legacy systems. This panel will provide concrete tips and different approaches to zero trust, while also addressing any perceived challenges that may be preventing organizations from pursuing a zero trust strategy.

Moderator: Kirk Hanson, Senior Sales Engineering Manager at Splunk
Panelist: Rick Moy, Chief Product Officer at Accuknox
Panelist: Anusha Vaidyanathan
Panelist: Eric Herzog, Chief Marketing Officer at Infinidat
Panelist: David W. Kravitz, Sr. Director of Research at Spring Labs

11:45-12:35PM - Carmel 2
50-Minute Panel Discussion Sponsored by Thales

Why Critical Data is Being Comprised?

Securing critical data and information was where this industry started a long time ago but it became more challenging with the rapid growth of enterprise data in an interconnected world. The pandemic forced organizations to support a remote workforce and expose critical systems that were once only accessible from inside the company's network. We've increased the attack surface and the number of vulnerabilities which has led to more data breaches. With the technology advancements in access management, data discovery and encryption we can once again shift the focus to securing our data and information. In this presentation, we will discuss a unified data-centric security approach and strategy to protecting your most critical data and information.

Sponsor: Thales
Moderator: Christopher Stewart, Data & Cloud Security Strategic Advisor at Thales
Panelist: Benjamin Longuechaud, Senior Sales Engineer at Thales
Panelist: Fidel Hernandez, IT Security Governance Risk and Compliance at Hyundai AutoEver America
Panelist: Bob Fabien Zinga, CO at USNR
Panelist: Randy Muyargas, Director, Information Security, Systems and Technology | Information Security Officer at Cordoba Corporation

11:45-12:35PM - Big Sur 1 & 2
50-Minute Panel Discussion

Phishing Continues to Be a Problem

Phishing is one of the most common types of cyberattacks, mainly because it is often an effective technique for gaining access to an organization's network and systems. It's usually easier to trick an employee into handing over sensitive data (like login credentials) or running a piece of malware on a company computer than it is to accomplish these goals through other means.

As a result, phishing will continue to be a problem in 2023 and into the future as long as it remains effective. However, the changing

Continued on next page

nature of work in the wake of the COVID-19 pandemic has its impacts on phishing as well.

For example, the surge in remote work caused by the COVID-19 pandemic drove many organizations to adopt online collaboration such as Zoom, Slack, etc. The focus on email in phishing awareness training means that employees often do not consider it a threat on these platforms, and workers often believe that only legitimate users can access these platforms, which is not always true. As a result, phishing attacks on these platforms are more likely to be effective than via email, where employees are more likely to be on their guard and companies may have anti-phishing solutions in place. Cybercriminals have noticed this, and the use of non-email collaboration platforms for phishing has become more common and is likely to continue to do so into 2023.

Join us as we discuss best practices to identify and mitigate phishing attacks.

Moderator: Harry Belt, Director – Information Security & Risk Management at Germantown Technologies
Panelist: Valerie Finn, Director, Trademark & Brand Protection at Corsearch
Panelist: Mandy Cartwright, Partner and Vice Chair - Privacy & Cybersecurity at Lewis Brisbois
Panelist: Terry S. McCorkle CEO and Founder at PhishCloud, Inc

12:35-1:35PM - South Promenade
60-Minute LUNCH

1:35-2:25PM - Carmel 2
50-Minute Panel Discussion Sponsored by Token

Next Generation Wearable Biometric Authentication... No Password Required

Losses to data breaches and ransomware attacks are at all time highs and growing, doubling the last 2 years in a row. 83% of organizations were victims of 2 or more data breaches last year and the overwhelming majority of these were caused by failed legacy MFA.

Token will review how their next generation MFA wearable, biometric, passwordless authentication FIDO2 certified solution solves the inherit problems with legacy MFA.

Sponsor: Token
Moderator: Tim Leow, Vice President of Sales at Token

1:35-2:25PM - Big Sur 1 & 2
50-Minute Panel Discussion

Escalating Cyber Risk From the IT Department to the Boardroom

Despite today's frequent headlines regarding companies falling victim to cyberattacks or suffering data breaches, cyber risk is still a relatively new threat - is it? While companies may have an idea about the potential effects on reputation and impact on the overall business, many are yet to experience one first-hand, or at least not on a high-profile scale. That means there's still unfamiliarity around how exactly to manage the risk. Many companies are changing their approach, in some cases; cybersecurity is still departmentalized and seen as the remit of the IT team.

- How do you incorporate a cybersecurity strategy into the company's overall governance, risk, and compliance structure? What's the best approach?

Moderator: Greg Silberman
Panelist: Harry Belt, Director – Information Security & Risk Management at Germantown Technologies
Panelist: Yogita Parulekar, Founder & CEO at Invi Grid Inc.
Panelist: Katey Wood, Principal Product Marketer, Privacy and Compliance at Amazon Web Services (AWS)
Panelist: Perry Pederson, Owner at Pederson Enterprises LLC
Panelist: Ganesh Krishnan, Co-Founder & CEO at Anzenna Inc

Continued on next page

Host

ELN

Sponsors

Token

INFINIDAT

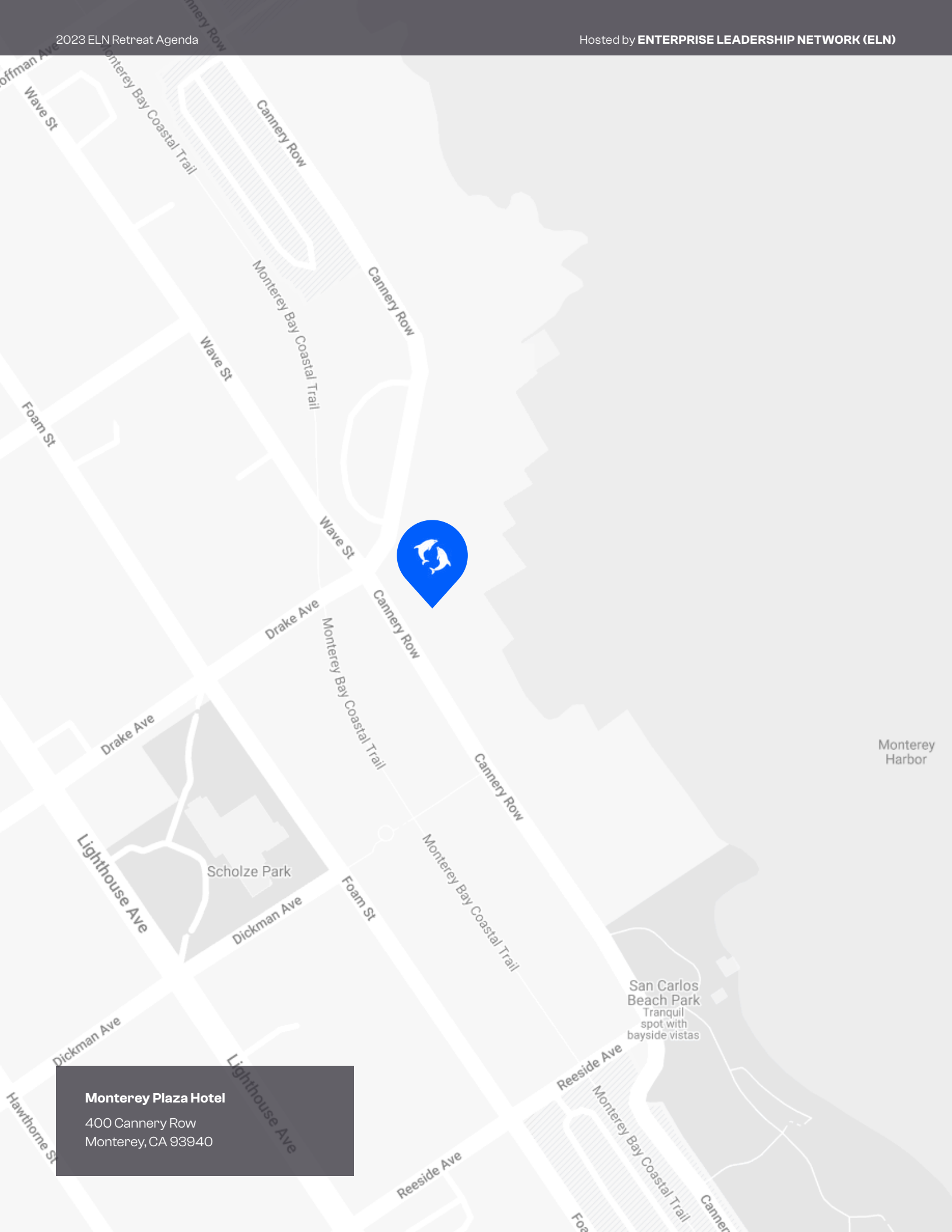
tackleai
The **logical** solution.

THALES

CDS COMPLETE DISCOVERY SOURCE

HOXHUNT

Continued on next page



Monterey Plaza Hotel
400 Cannery Row
Monterey, CA 93940

Genelle LaCour
Events@enterprisemindset.com

100 Spectrum Ctr Dr, Ste 900
Irvine, CA 92618

EnterpriseMindset.com