



Managed Cybersecurity Services



Disclaimer

General

The information provided in this presentation pertaining to Integrate Cyber, Inc ("Integrated Cyber" or the "Company"), its business assets, strategy, and operations is for general informational purposes only and is not a formal offer to sell or a solicitation of an offer to buy any securities, options, futures, or other derivatives related to securities in any jurisdiction and its content is not prescribed by securities laws. Information contained in this presentation should not be relied upon as advice to buy or sell or hold such securities or as an offer to sell such securities. This presentation does not take into account, nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information in this presentation is believed to be accurate and reliable, Integrated Cyber and its agents, advisors, directors, officers, employees, and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information and Integrated Cyber expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Integrated Cyber reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient thereof.

The information contained in this presentation is intended only for the persons to whom it is transmitted for the purposes of evaluating the Company. The information contained in this presentation supersedes any prior presentation or conversation concerning the Company. Any information, representations, or statements not contained herein shall not be relied upon for any purpose.

Neither we nor any of our representatives shall have any liability whatsoever, under contract, tort, trust, or otherwise, to you or any person resulting from the use of the information in this presentation by you or any of your representatives or for omissions from the information in this presentation. Additionally, the Company undertakes no obligation to comment on the expectations of, or statements made by, third parties in respect of the matters discussed in this presentation.

Confidentiality

This presentation is confidential and is intended, among other things, to present a general outline of the Company. The contents are not to be reproduced or distributed to the public or press. Each person who has received a copy of this presentation (whether or not such person purchases any securities) is deemed to have agreed: (i) not to reproduce or distribute this presentation, in whole or in part, without the prior written consent of the Company, other than to legal, tax, financial and other advisors on a need to know basis, (ii) if such person has not purchased securities, to return this presentation to the Company upon its request, (iii) without the prior written consent of the Company, not to disclose any information contained in this presentation except to the extent that such information was (a) previously known by such person through a source (other than the Company) not bound by any obligation to keep such information confidential, (b) in the public domain through no fault of such person, or (c) lawfully obtained at a later date by such person from sources (other than the Company) not bound by any obligation to keep such information confidential, and (iv) to be responsible for any disclosure of this presentation, or the information contained herein, by such person or any of its employees, agents or representatives.

Forward-Looking Statements and Financial Projections

Certain information in this presentation and oral statements made in any meeting are forward-looking and relate to Integrated Cyber and its anticipated financial position, business strategy, events, and courses of action. Words or phrases such as "anticipate," "objective," "may," "will," "might," "should," "could," "can," "intend," "expect," "believe," "estimate," "predict," "potential," "plan," "is designed to" or similar expressions suggest future outcomes. Forward-looking statements and financial projections include, among other things, statements about: our expectations regarding our expenses, sales, and operations; our future customer concentration; our anticipated cash needs, our estimates regarding our capital requirements, our need for additional financing; our ability to anticipate the future needs of our customers; our plans for future products and enhancements of existing products; our future growth strategy and growth rate; our future intellectual property; and our anticipated trends and challenges in the markets in which we operate. Forward-looking statements and financial projections are based on the opinions and estimates of management at the date the statements are made and are subject to a variety of risks and uncertainties, and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements and financial projections. Although we believe that the expectations reflected in the forward-looking statements and financial projections are reasonable, there can be no assurance that such expectations will prove to be correct. We cannot guarantee future results, level of activity, performance, or achievements, and there is no representation that the actual results achieved will be the same, in whole or in part, as those set out in the forward-looking statements and financial projections.

By their nature, forward-looking statements and financial projections involve numerous assumptions, known and unknown risks and uncertainties, both general and specific, that contribute to the possibility that the predictions, forecasts, projections and other forward-looking information will not occur, which may cause the Company's actual performance and financial results in future periods to differ materially from any estimates or projections of future performance or results expressed or implied by such forward-looking statements and financial projections. Important factors that could cause actual results to differ materially from expectations include, but are not limited to: business, economic and capital market conditions; the heavily regulated industry in which the Company carries on business; current or future laws or regulations and new interpretations of existing laws or regulations; legal and regulatory requirements; market conditions and the demand and pricing for our products; our relationships with our customers, developers and business partners; our ability to successfully define, design and release new products in a timely manner that meet our customers' needs; our ability to attract, retain and motivate qualified personnel; competition in our industry; competition; technology failures; failure of counterparties to perform their contractual obligations; systems, networks, telecommunications or service disruptions or failures or cyber-attack;

ability to obtain additional financing on reasonable terms or at all; our ability to manage risks inherent in foreign operations; litigation costs and outcomes; our ability to successfully maintain and enforce our intellectual property rights and defend third party claims of infringement of their intellectual property rights; our ability to manage foreign exchange risk and working capital; and our ability to manage our growth. Readers are cautioned that this list of factors should not be construed as exhaustive.

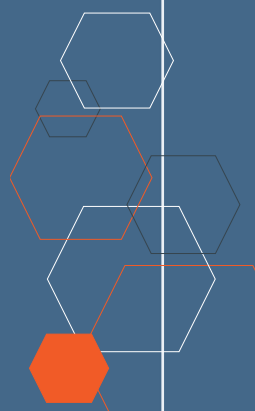
The forward-looking statements and financial projections contained in this presentation are expressly qualified by this cautionary statement. Except as required by law, we undertake no obligation to update or revise publicly any forward-looking statements, whether as a result of new information, future events, or otherwise, after the date on which the statements are made or to reflect the occurrence of unanticipated events. Readers are cautioned not to place undue reliance on forward-looking statements or financial projections.

Prospective investors should not construe the contents of this presentation as legal, tax, investment, or other advice. All prospective investors should make their own inquiries and consult their own advisors as to legal, tax, investment, and related matters concerning an investment in the securities of the Company.

United States Disclaimer

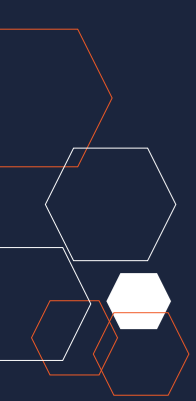
This document does not constitute an offer to sell or a solicitation of an offer to buy securities in the United States. The securities offered hereby have not been, and will not be, registered under the United States Securities Act of 1933, as amended (the "U.S. Securities Act"), or under any of the securities laws of any state of the "United States" (as defined in Regulation S under the U.S. Securities Act). Accordingly, the securities offered hereby may not be offered or sold, directly or indirectly, to, or for the account or benefit of, a person in the United States or a "U.S. person" (as defined in Regulation S under the U.S. Securities Act) unless exempt or excluded from the registration requirements of the U.S. Securities Act, and the securities laws of all applicable states of the United States or pursuant to registration under the U.S. Securities Act and under the securities laws of all applicable states of the United States. None of the United States Securities and Exchange Commission or any other securities commission or regulatory authority in the United States has approved or disapproved of the securities of the Company or determined if this document is truthful or complete. Any representation to the contrary is a criminal offense.

Also, please reach out to your U.S. counsel to confirm the extent you can use this slide deck to offer special warrants in the US, especially since 1332996 BC Ltd isn't registered with the SEC. As we are not licensed in the US, we cannot advise on this subject. If your current counsel doesn't have expertise in securities laws, please let us know and we can recommend a U.S. law firm.



Integrated Cyber Solutions delivers managed cybersecurity services to the Small-to-Medium Business (SMB) and Small-to-Medium Enterprise (SME) segments.

We integrate best-in-class capabilities from multiple third-party cybersecurity providers. By providing cybersecurity as a managed service, we can continuously evolve services as technology (and providers), thus future-proofing our customers' investment.

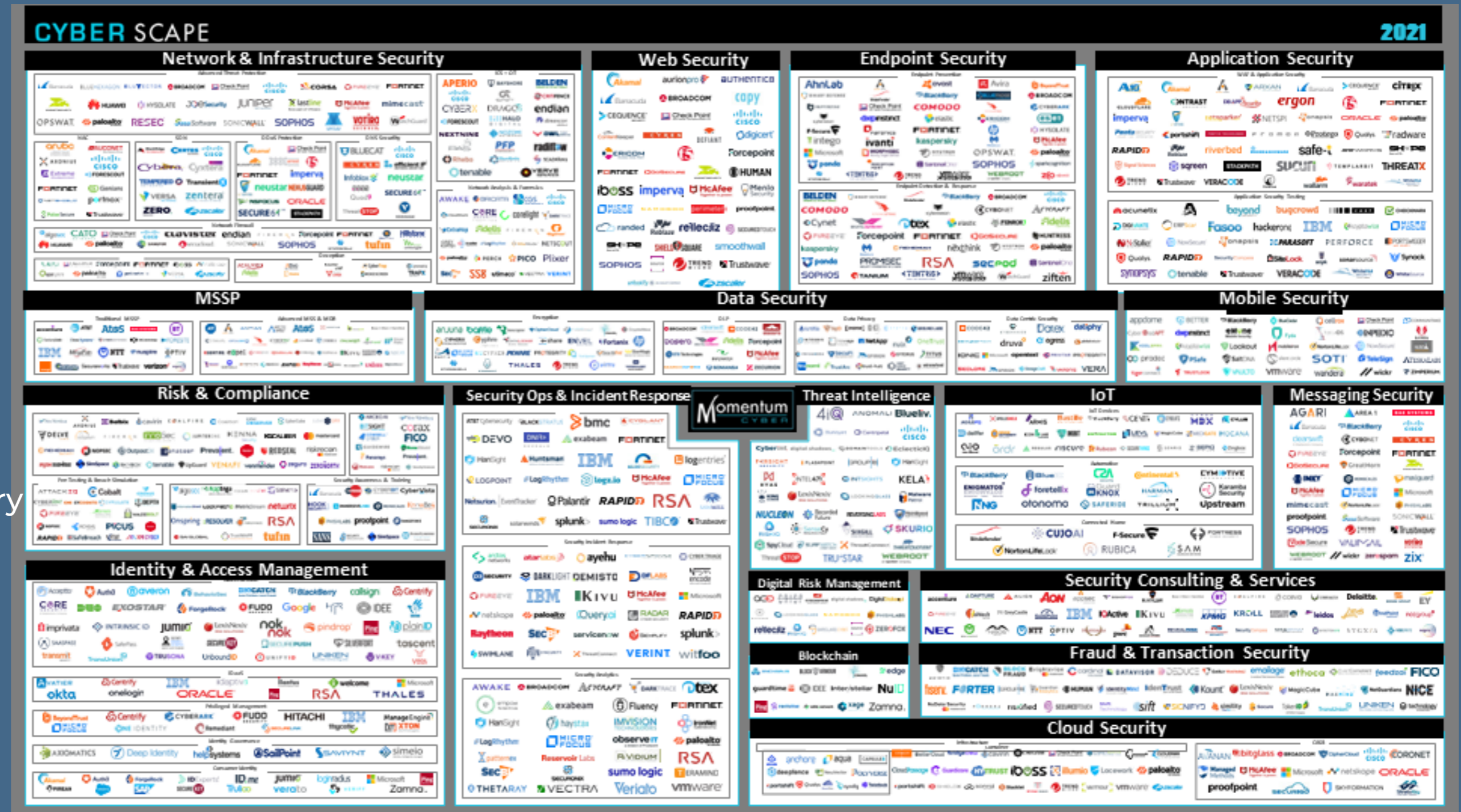


Key Highlights

- The cyber industry includes **hundreds of point solutions** addressing different threats, environments, and approaches.
 - We focus our resources and market differentiation around three core pillars:
 - **Vulnerability Management**
 - **Managed Detection & Response**
 - **Cyber Training & Awareness**
 - Integrated eco-system for IT management spanning NOC/SOC; with rich opportunities for enabling consulting services, adjacent products, training
- Represents and **integrates** top cybersecurity software platforms
 - Selling both **direct** and through **partners**, with products, services, consulting/compliance advisory
 - Focused on the **US & Canada** markets
 - **Predictability** – Annual and multi-year subscription contracts
 - **Affordability** – Low overhead model
- **Acquire** synergistic companies to drive rapid growth, customer acquisition, technology expansion, market reach, and talent expansion.
 - **Exit strategy** - Position to be acquired by a major IT Services Company or Cyber product company, or MSSP

The Challenges Facing SMB/SME Businesses

- Too many choices
- Too hard to understand
- Full of jargon
- Challenge to implement
- Challenge to integrate
- Challenge to operate, especially 24x7
- Challenge to stay on top of this fast-moving industry





The Exploding Market – Breaches & Spending

Cybersecurity presents a large opportunity

**\$10+
BILLION**

Cybercrime COSTS businesses billions. FBI reports \$4.2B in 2020 and the Canadian Chamber of Commerce states \$5B to \$7B annually

**\$376
BILLION**

Fortune Business Insights estimates the global cybersecurity market is expected to grow 13.4% annually by 2029 to \$376B

**ONLY
47 to 80%**

Only 47% of US and 80% of Canadian businesses have a cybersecurity plan in place

41%

of executives don't think their security initiatives have kept up with digital transformation

50% More

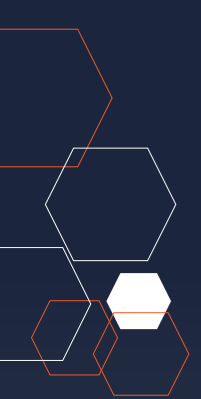
Businesses suffered an increase of 50% in cyber attack attempts per week in 2021

3.5 MILLION

unfilled cyber jobs expected to remain through 2025



Protecting SMB & SME companies through a focused services portfolio



Focusing on the three most important pillars that proactively protect a business

Vulnerability Assessments & Remediation

From one-time assessments and pen tests to full vulnerability management and remediation services.

Cyber Training & Awareness

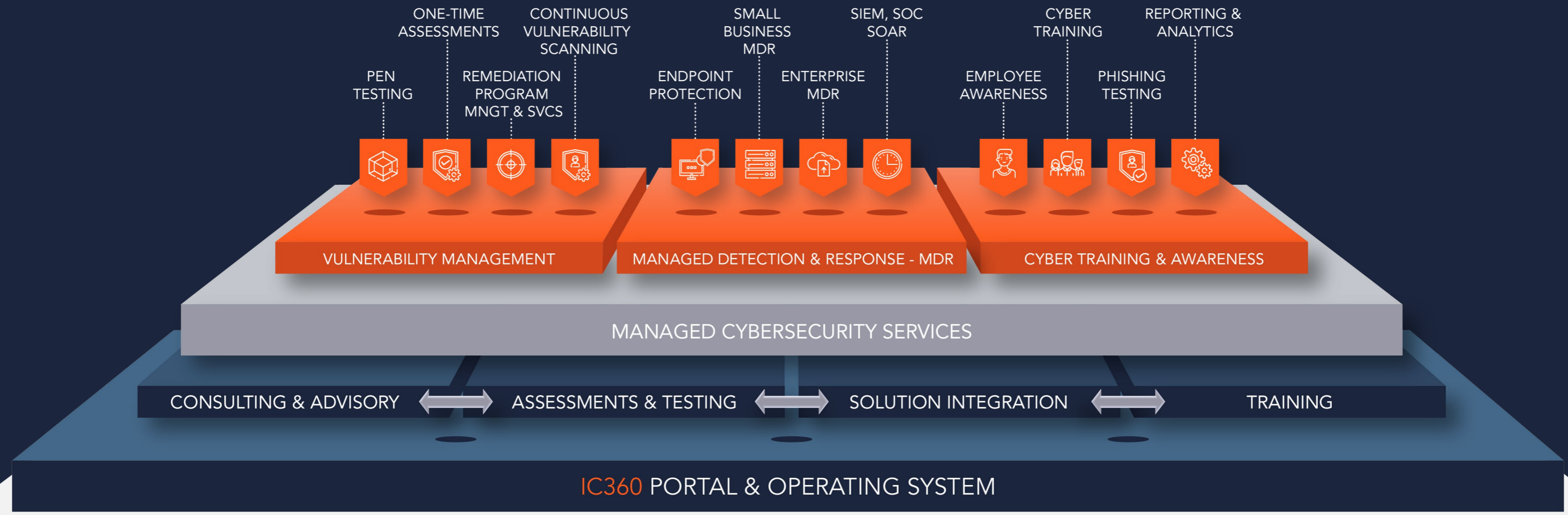
A full managed service spanning training, phishing tests, and improvement analytics.

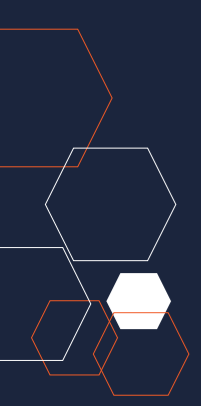
Managed Detection & Response

A complete MDR or XDR service tailored for small business or a large enterprise.



Our Services Stack



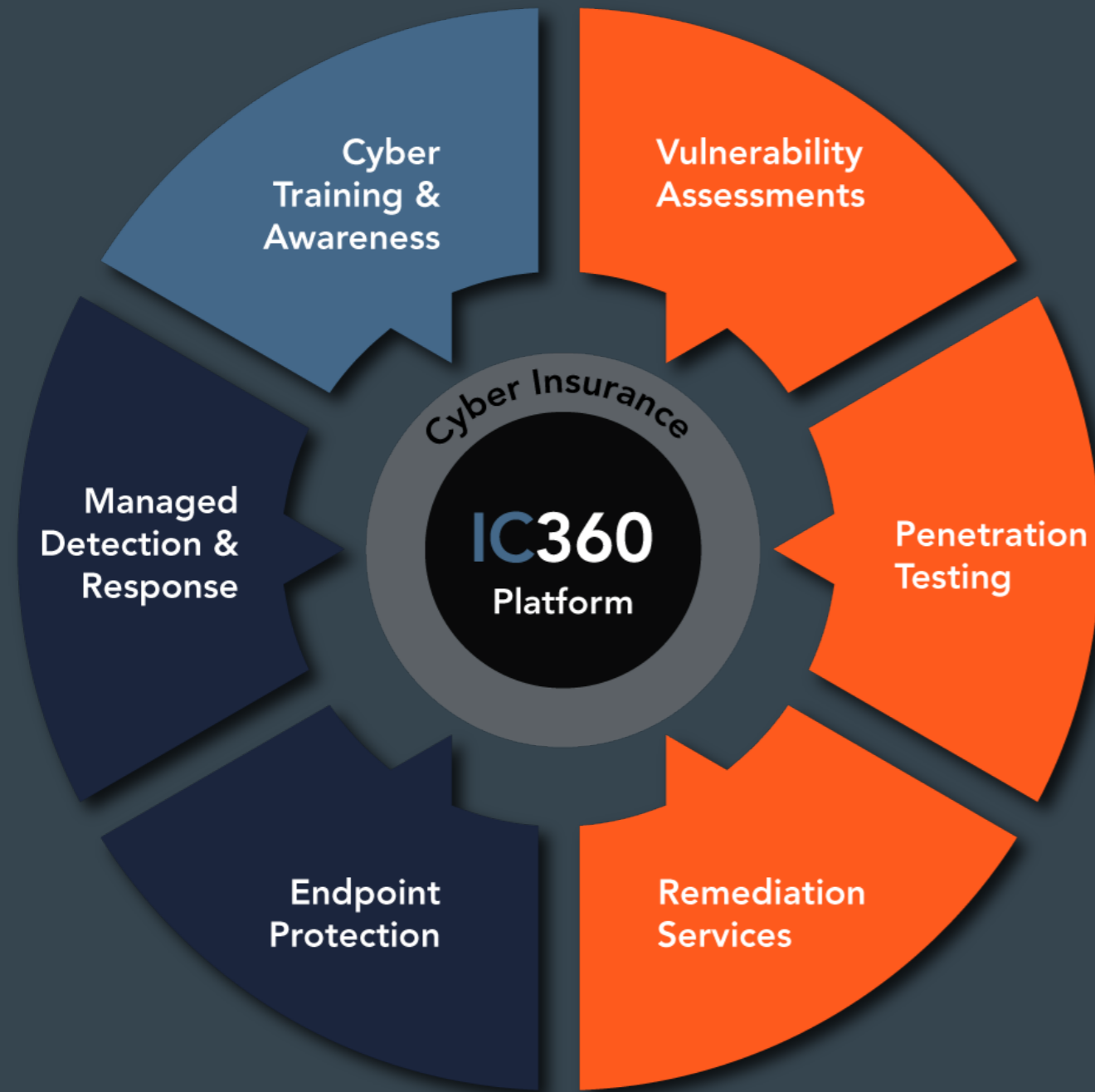


Artificial Intelligence (AI) & Machine Learning (ML)

Artificial Intelligence (AI) is revolutionizing the cybersecurity industry, and Integrated Cyber is incorporating AI technology across our applications to keep our customers safer than ever before.

- AI drives **cyber training** by determining **behavior patterns** and learning styles to personalize security training for each employee
- Vulnerability management leverages machine learning (ML) algorithms to **analyze large datasets of security-related information** to identify patterns and anomalies.
- AI helps us **detect and respond to threats instantly**, reducing the risk of cyber attacks. It also analyzes large amounts of data to **identify patterns** that humans may overlook, enabling proactive vulnerability management. We prioritize customer protection and stay ahead of the curve.

Our Focus & Differentiation



In a world of fragmented solutions, jargon, and overwhelming noise, our mission is to make cyber security:

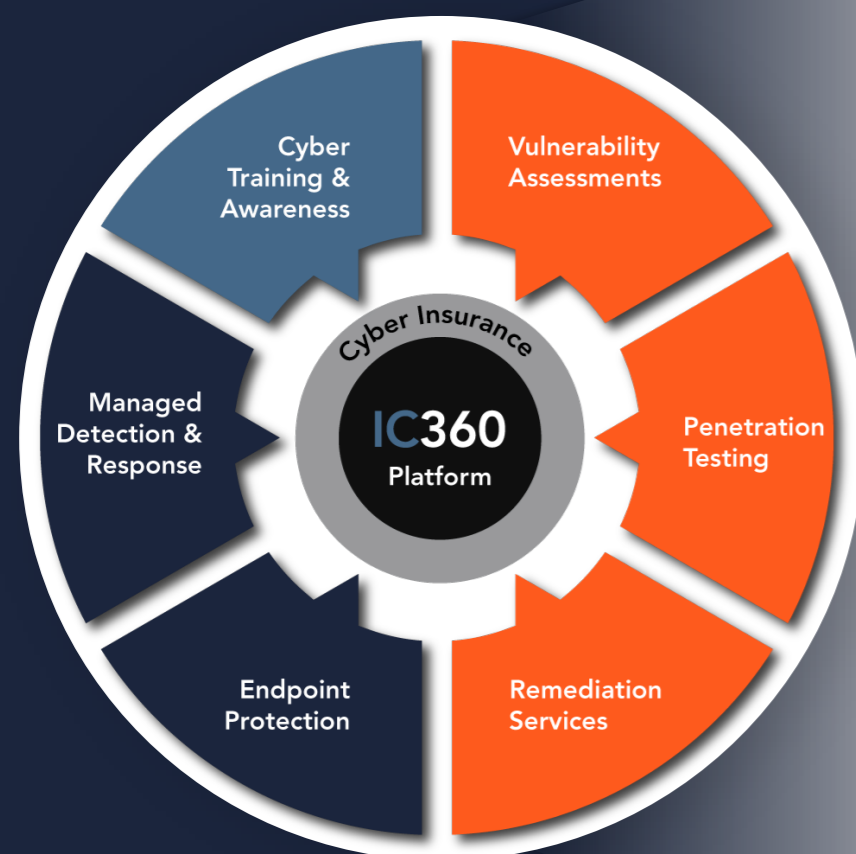
UNDERSTANDABLE & ACTIONABLE

We do this with owned IP that:

- Integrates and correlates data from multiple systems, providing a single, understandable source of truth
- Translates raw data into actionable insights, presented to the right people at the right time
- Enables a single Master Scheduler for our clients across all cyber-related activities



IC360 – The Cyber Command Center



Insights Center

- Single pane of glass
- Flexible dashboards
- Actionable insights

Response Center

- Notification Manager
- Threat Intelligence
- Response playbooks

Master Planner

- Integrated scheduler
- Plan vs. Actuals tracker
- Comprehensive plan

Microservice and Workflow Orchestration

Third Party
Cyber
Platforms

Insights, Correlation, and Intelligence (AI/ML)

IC360 Data Lake
Correlated, integrated data from all cyber platforms



Vulnerability Management

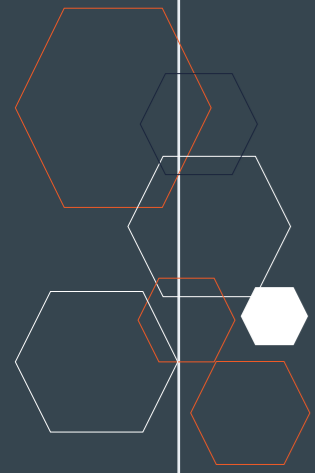
560,000 new malware pieces are produced EVERY DAY
1 Billion malware programs are installed worldwide

AV Test – The Independent IT-Security Institute

Vulnerability Management

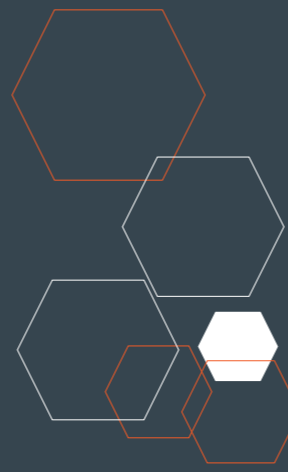
- Vulnerability Management focuses on the **identification** and **proactive** remediation of cyber risks before they can be exploited
- This includes discovery of assets, scanning for vulnerabilities, and prioritized recommendations for remediation
 - **One-time or regularly scheduled** vulnerability assessments and penetration testing or...
 - **Continuous** vulnerability scanning when environments are more dynamic
 - **Remediation** recommendations and prioritization, including program management oversight if required
- Vulnerability assessments identify what needs to get done.
- Remediation Services ensure that happens.





Cyber Training & Awareness

88% of cyber breaches are caused by human actions

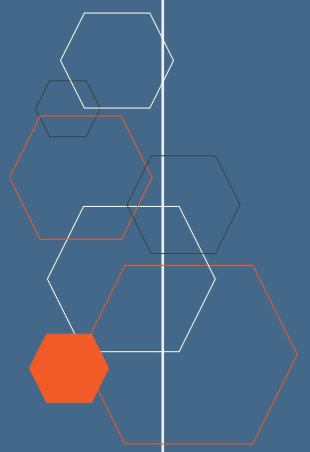


Cyber Training & Awareness

Hackers are relentless, so we execute monthly outbound campaigns to educate, train, and test our customer's employees.

- We enable employees to be the strongest defense against cyber attacks.
- Old-school Security Awareness Training once a year doesn't hack it anymore.
- The cyber threat is constantly changing.
- Humans learn best when fed information in bite-sized pieces on a regular basis.
- It's vital to have a preventative education program that protects a company.

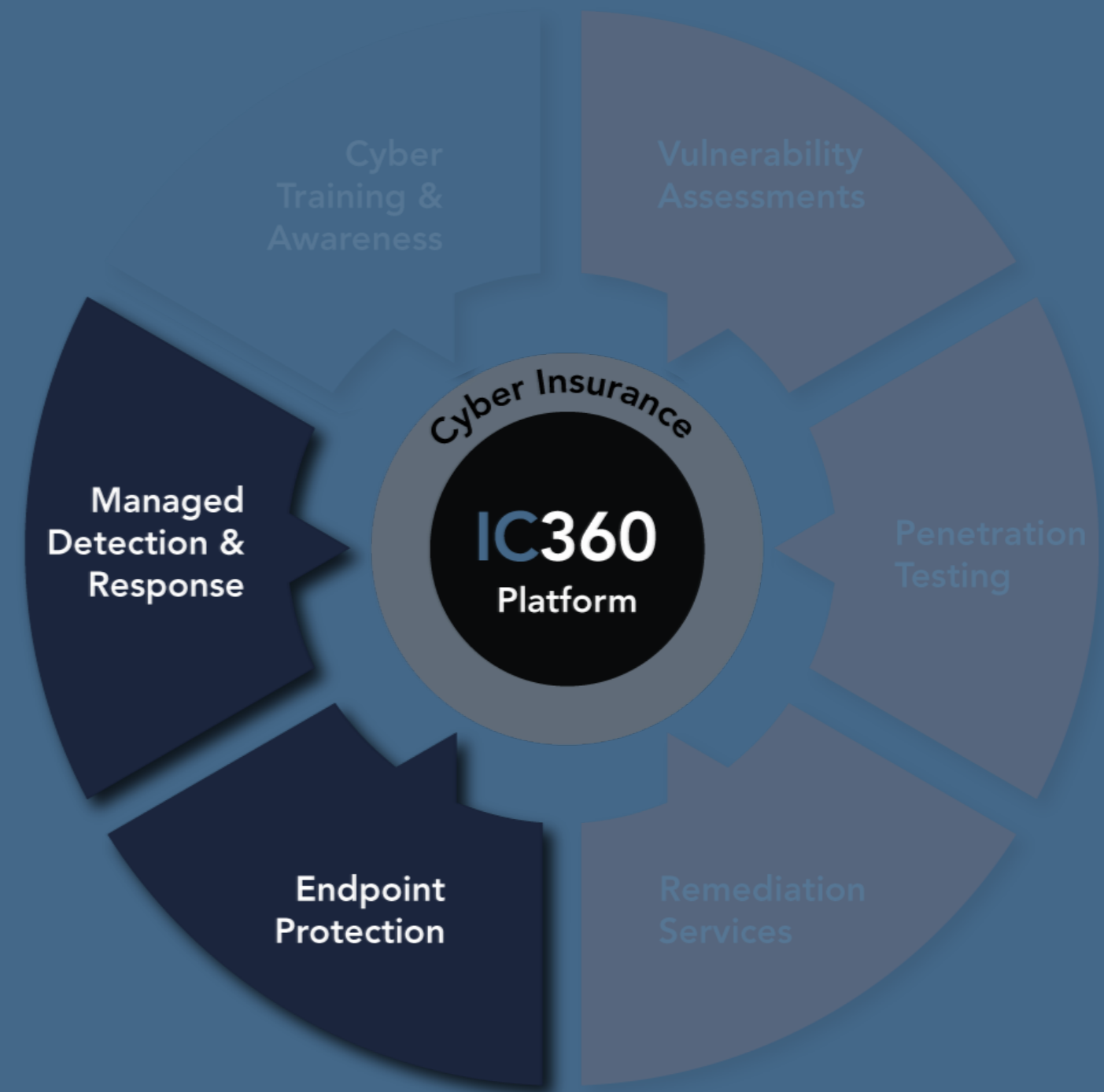




Managed Detection & Response - MDR

Managed Detection & Response (MDR)

- MDR is one of the fastest-growing areas of cybersecurity. Gartner estimates that 50 percent of organizations will be using MDR services by 2025.
- Considered the **core capability** in an organization's cyber defense spanning the critical **lifecycle** of detecting, analyzing, responding, and where possible – remediating after getting hit by a cyber threat.
- We offer two editions to meet the different needs of our customers:
 - Enterprise Edition
 - Small Business Edition



We envision a world where SMB and SME companies have the same level of cyber **protection** afforded to large enterprise organizations.



The SMB/SME segments are well positioned for our services



Segment	Profiles	Vital Statistics	Average Annual Revenue Potential
Small	<ul style="list-style-type: none"> Often Privately owned Highly localized; single or few sites Low technical competency Short sales cycles Retail 	<ul style="list-style-type: none"> Ideal Target between \$25M and \$100M Annually Employees: 25 and 250 Cost sensitive 	<ul style="list-style-type: none"> \$180K annual recurring revenue with expansion in subsequent years
Medium	<ul style="list-style-type: none"> Increasing complexity, multi-site Higher technical competency Short sales cycles Retail, Industrial, Education 	<ul style="list-style-type: none"> Between \$100M and \$750M Annually Potentially thousands of employees / workers Value for cost sensitive 	<ul style="list-style-type: none"> Up to \$360K annual recurring revenue Excellent upside potential
Large	<ul style="list-style-type: none"> Multi-site, multi-business units IT capabilities, including Security team Procurement governance/barriers Longer sales cycles (months) Retail, Industrial 	<ul style="list-style-type: none"> Between \$750M and \$3B Annually Thousands and sometimes tens of thousands of employees / contractors based on industry Value/Capability for cost sensitive 	<ul style="list-style-type: none"> \$660K annual recurring revenue Significant upside potential
Extra-Large	<ul style="list-style-type: none"> Enterprises or Public Sector (non-Defense) Financial Services, Healthcare Enterprise-class competency Enterprise-class processes / barriers Long sales cycles 	<ul style="list-style-type: none"> \$3B and above Tens of thousands of employees High complexity / diversity of infrastructure Value/Capability sensitive but negotiate hard 	<ul style="list-style-type: none"> \$1M+ annual recurring revenue in initial year(s) Significant upside growth potential in subsequent years



Business Model

The core pillars of the business

Provide managed cybersecurity

Services focused on core proactive and reactive capabilities to deliver customer & shareholder value

Partner with premier providers

Integrated their deep cybersecurity platforms to address the multiple needs within the cyber stack

Build IC360, our AI platform

The platform will provide value across the technology stack by horizontally correlating cyber events so we can increase security

Acquire synergistic companies

We will drive rapid growth, customer acquisition, technology expansion, market reach, increased share of wallet, and talent expansion



Growth Plan

Growth thru acquisition and organic growth

A Dual Plan For Growth

Acquisitions
Internal growth

Acquisition Activity Upon Listing

Customer base
Revenue base

Goal to Acquire 4 Companies Per Year

Start with smaller firms
Increase size as market cap grows



Management Team

ALAN GUIBORD CEO

Alan has more than 35 years of global IT and management experience. Currently, he is the Chairman and Co-Founder of Integrated Cyber. Alan is also co-founder of The Advisory Council International, an organization of over 25 former Fortune 100 CIOs providing technical guidance to Board-level and C-suite executives as well as coaching and direction to IT Leaders 2004-present. During his career, he has served as the President and CEO of Computerworld 2001-2003, a media firm for IT Executives, CIO of Fort James Corp., a pulp and paper company later acquired by Georgia-Pacific LLC 1997-2001, CIO of R.R. Donnelley & Sons Publishing Corp, a commercial printer 1995-1997.

ROBERT CONSAGA CFO

Robert has more than 35 years of financial management experience and is responsible for the financial management of ICS. He has worked for a Fortune 100 company and International Public Accounting firm, focused on multiple small businesses and startup companies in high tech, real estate, construction and multinational companies. Bob specialized in providing tax strategies and planning opportunities to companies with sales that ranged from \$20 million to over \$1 billion. He founded a CPA firm in his name in 1991 where he has provided financial and tax services in the manufacturing, high technology, retail, construction, real estate and professional industries.

PETE KAROLCZAK COO

Pete brings over 30 years of experience in IT, IT Services, Software and Consulting experience from Fortune 10 global enterprises to early-stage startups to Integrated Cyber. Prior to joining Integrated Cyber, Pete held several executive positions at Hewlett Packard Company from 1987 to 2016. From 2011 until his retirement as senior vice president and general manager of the IT Outsourcing division at Hewlett-Packard Company, Pete was responsible for managing a \$15 billion division of Hewlett-Packard Company, which included managed security services, enterprise cloud and mobility services. Pete obtained a Bachelor Degree in Mathematics and Computer Science from Stanford University.

KEVIN THOMAS CMO

Kevin has 36 years of marketing, sales enablement, and sales operations experience across multiple technology companies, including cybersecurity, data storage, AI & ML, data center, enterprise technology services, geospatial, software, and telecommunications sectors. Kevin was an executive with Hewlett Packard, leading global sales enablement for their enterprise services division. He has held executive marketing roles at Iverify Security, NTT RagingWire Data Centers, Intermap Technologies, and others. Kevin has a Bachelor of Science degree in Business Administration, Marketing, from the University of Nevada, Reno.



Board of Directors

ALAN GUIBORD
CEO & DIRECTOR

Alan will serve as the company's CEO and a member of the Board of Directors.

ROBERT CONSAGA
CFO & DIRECTOR
AUDIT COMMITTEE

Robert will serve as the company's CFO and a member of the Board of Directors.

PETE KAROLCZAK
COO & DIRECTOR

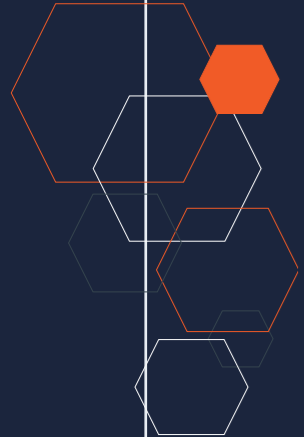
Pete will serve as the company's COO and a member of the Board of Directors.

ROB BAIN
DIRECTOR
AUDIT COMMITTEE

Robert is a businessman with an extensive career in accounting, finance, and capital raising in financial markets. He has an honorary bachelor's degree in accountancy and management from Sheffield University and is part of the Institute of Chartered Accountants in England and Wales. He has experience in financial auditing and advising clients on business mergers and acquisitions. He has spent over 27 years working in various financial sector roles. Robert is the managing director of a water business in the UAE. He has worked at EY and PKF for over 10 years and 8 years as CEO and managing partner of VV Capital LLP, a small UK-based investment and private equity firm. He has extensive experience growing small and medium-sized businesses, has successfully developed investment strategies, and raised capital within private equity markets.

JERI DUNN
DIRECTOR
AUDIT COMMITTEE

Jeri is a businesswomen with a wealth of management experience in the information technology sector. Jeri has an associated degree in computer technology from Edinboro State University, and she is a founding member of the Arkansas Chapter for Women in Technology. She has experience managing business information systems for large multi-national corporations, and she has recently spent her professional time mentoring and providing coaching to executives through Boston University and CIO Executive Council's Pathways program.



Thank you

www.Integrated-Cyber.com