RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **AIR-R01**

Dynamic Defense: Security Operations Transformation

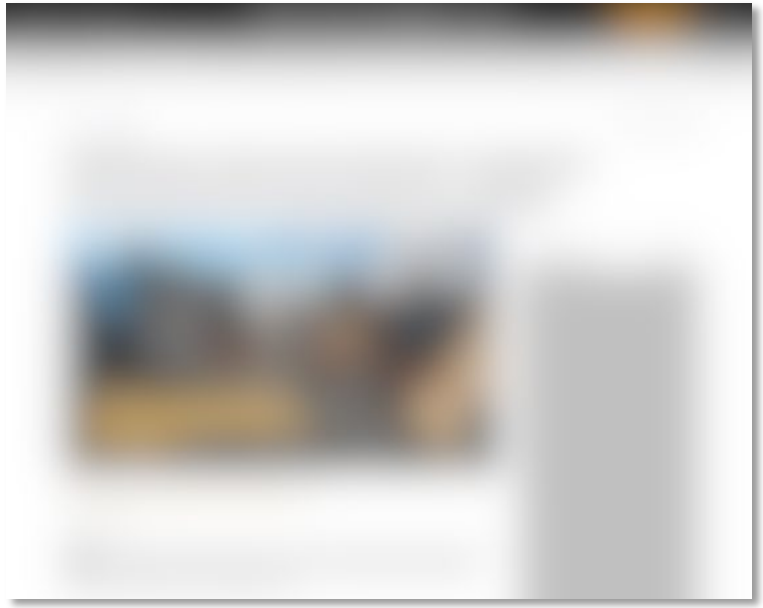
Adam Langford

Senior Associate, SecOps Modernization
Booz Allen Hamilton

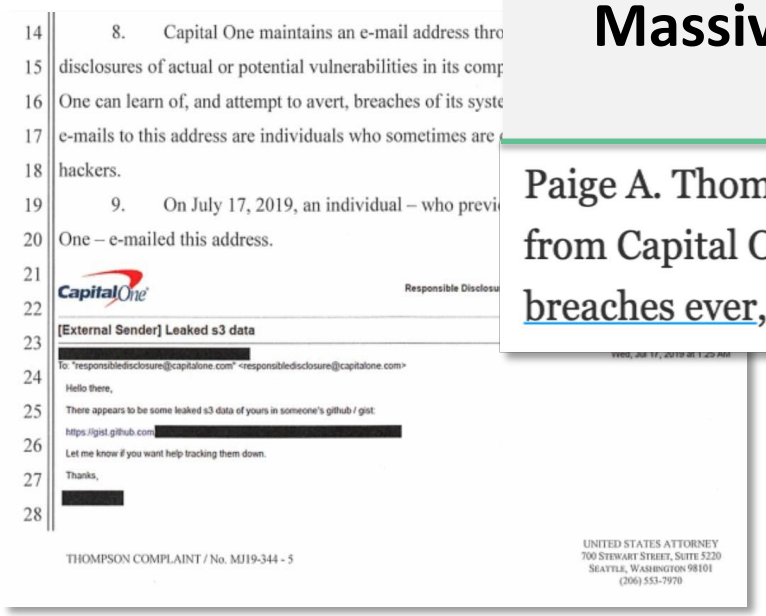
Garrettson Blight

Director, DarkLabs
Booz Allen Hamilton

3 Industries, 3 Different Attack Vectors, Same Headline



3 Industries, 3 Different Attack Vectors, Same Headline



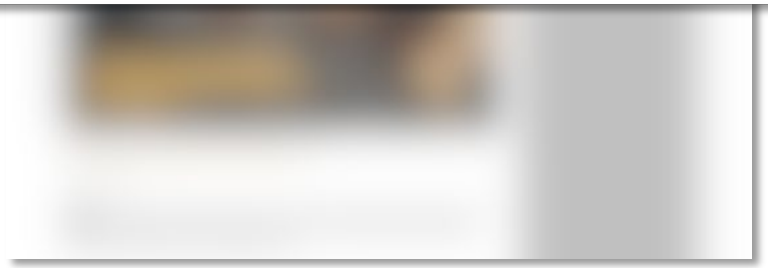
14 8. Capital One maintains an e-mail address thro
15 disclosures of actual or potential vulnerabilities in its comp
16 One can learn of, and attempt to avert, breaches of its syste
17 e-mails to this address are individuals who sometimes are
18 hackers.
19 9. On July 17, 2019, an individual – who previ
20 One – e-mailed this address.
21
22 Capital One Responsible Disclosu
23 [External Sender] Leaked s3 data
24 [redacted]
To: "responsiblediscloure@capitalone.com" <responsiblediscloure@capitalone.com>
25 Hello there,
There appears to be some leaked s3 data of yours in someone's github / gist:
26 https://gist.github.com/[redacted]
Let me know if you want help tracking them down.
27 Thanks,
28 [redacted]

THOMPSON COMPLAINT / No. MJ19-344 - 5

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Massive data breach hits Capital One, affecting more than 100 million customers

Paige A. Thompson, 33, a former software engineer, is accused of stealing data from Capital One credit card applications in what is one of the top 10 largest data breaches ever, according to USA TODAY research.



3 Industries, 3 Different Attack Vectors, Same Headline

Baltimore city government computer network hit by ransomware attack

Baltimore city government computers were infected with ransomware Tuesday, the mayor's office said, the second time in just over a year that hackers demanding payment disrupted the city's technology systems.

3 Industries, 3 Different Attack Vectors, Same Headline

LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach

In a filing today with the **U.S. Securities and Exchange Commission**, LabCorp. said it learned that the breach at AMCA persisted between Aug. 1, 2018 and March 30, 2019. It said the information exposed could include first and last name, date of birth, address, phone, date of service, provider, and balance information.

Agenda

1 WHY NOW & FRAMEWORK

- So Why Now?
- Dynamic Defense Framework

2 PRINCIPLES

- Five Principles of Dynamic Defense Transformation
- Cyber Discovery Model

3 RECOMMENDATIONS & QUESTIONS

- Takeaways
- Applications

WHY NOW & FRAMEWORK

So Why Now?

EXPONENTIALLY GROWING ATTACK SURFACE

The attack surface has expanded to **third-party integrations**, which was the primary attack vector for LabCorp

MASSIVE RESOURCE GAPS

Finding individuals versed in ***perimeter-less engineering and cybersecurity***, is increasingly challenging

INCREASED REGULATION AND OVERSIGHT

Prescriptive government action, growing public scrutiny, and farther-reaching consequences

ORGANIZATIONS ARE SLOW TO MIGRATE TO THREAT-CENTRIC OPERATIONS

Slow adoption of automation and integration of threat intel

ADVERSARY SOPHISTICATION IS OUTPACING CYBER DEFENSE

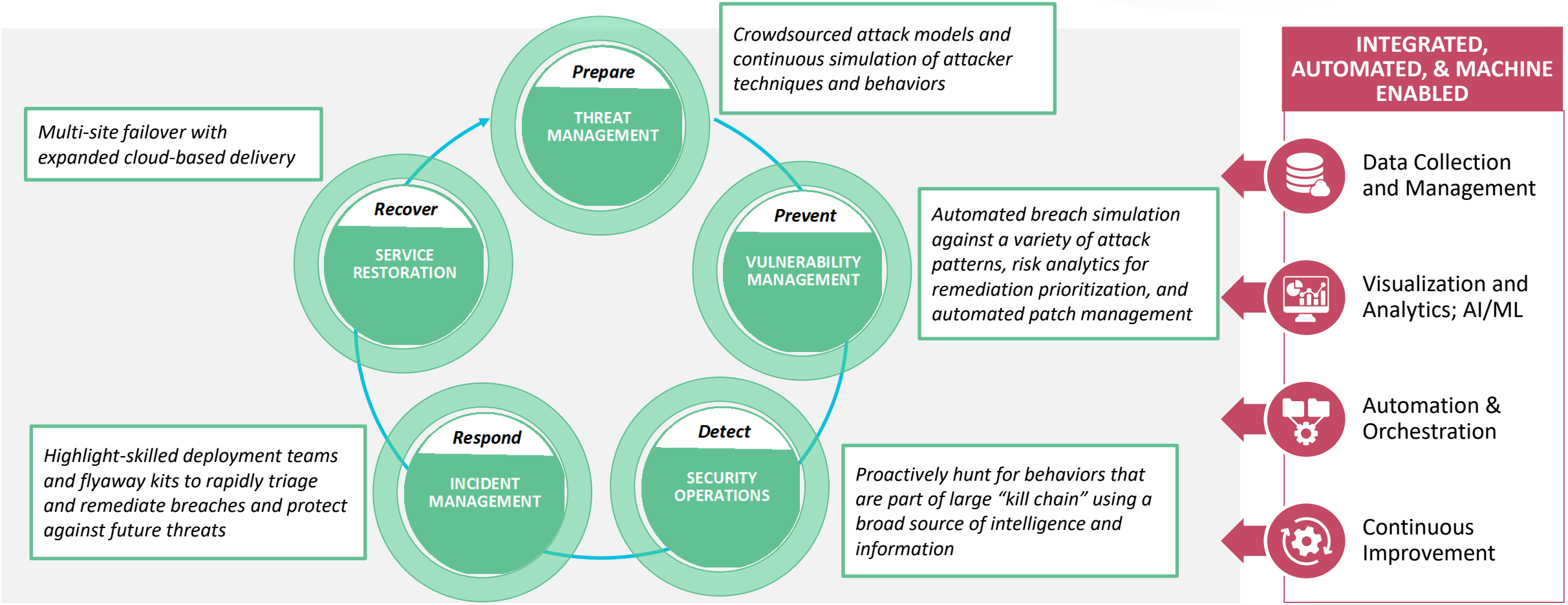
Limited enterprise-wide visibility of cyber threats combined with ***alert overload and fatigue***

TOOLS ALONE WON'T MODERNIZE OPERATIONS AND STOP CYBER THREATS

While many organizations have adopted various tools, ***data integration gaps and tuning deficiencies*** open windows for adversaries to attack undetected

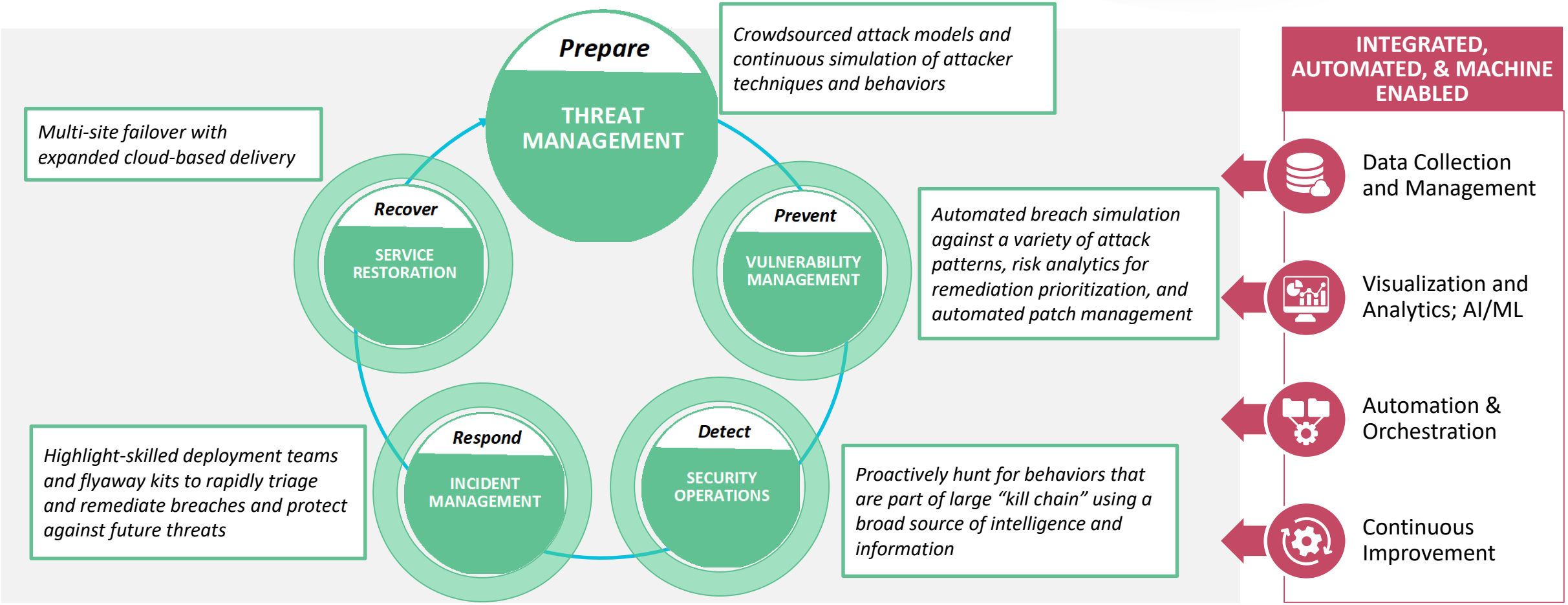
Dynamic Defense Framework

Full Spectrum Cyber Security Operations, With Greater Emphasis On Prepare And Prevent



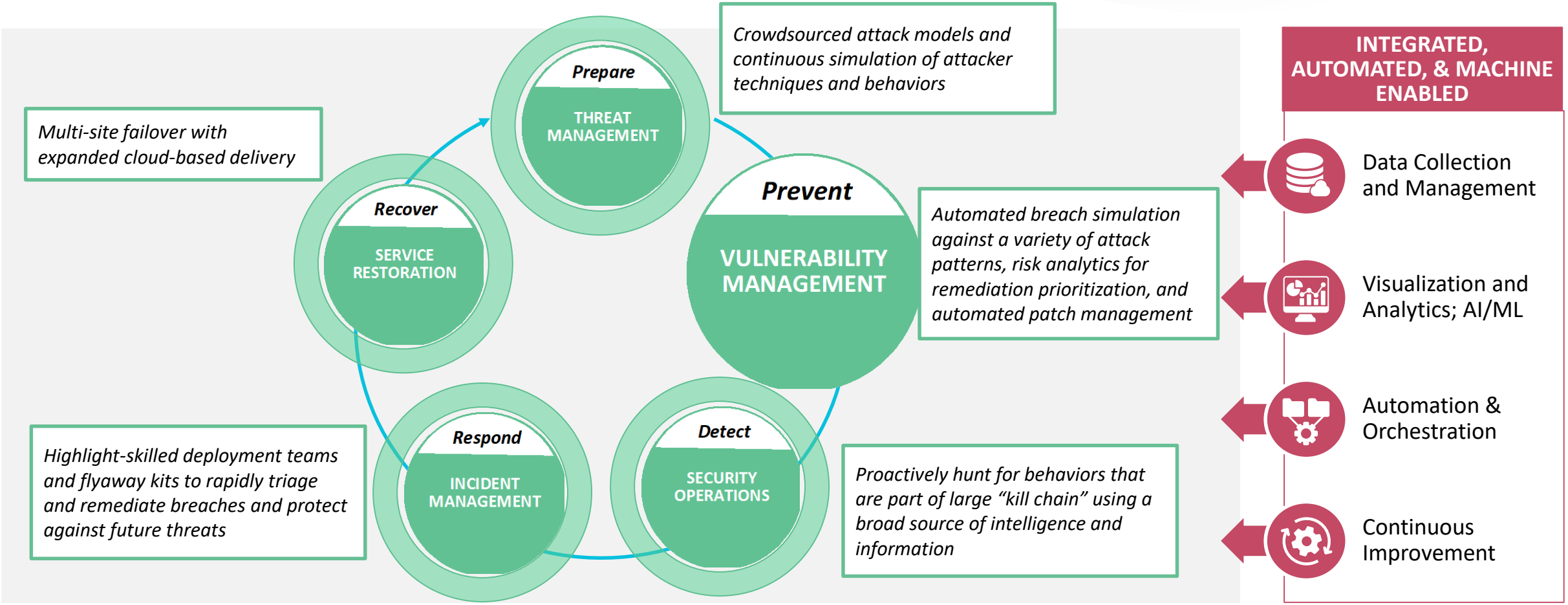
Dynamic Defense Framework

Full Spectrum Cyber Security Operations, With Greater Emphasis On Prepare And Prevent



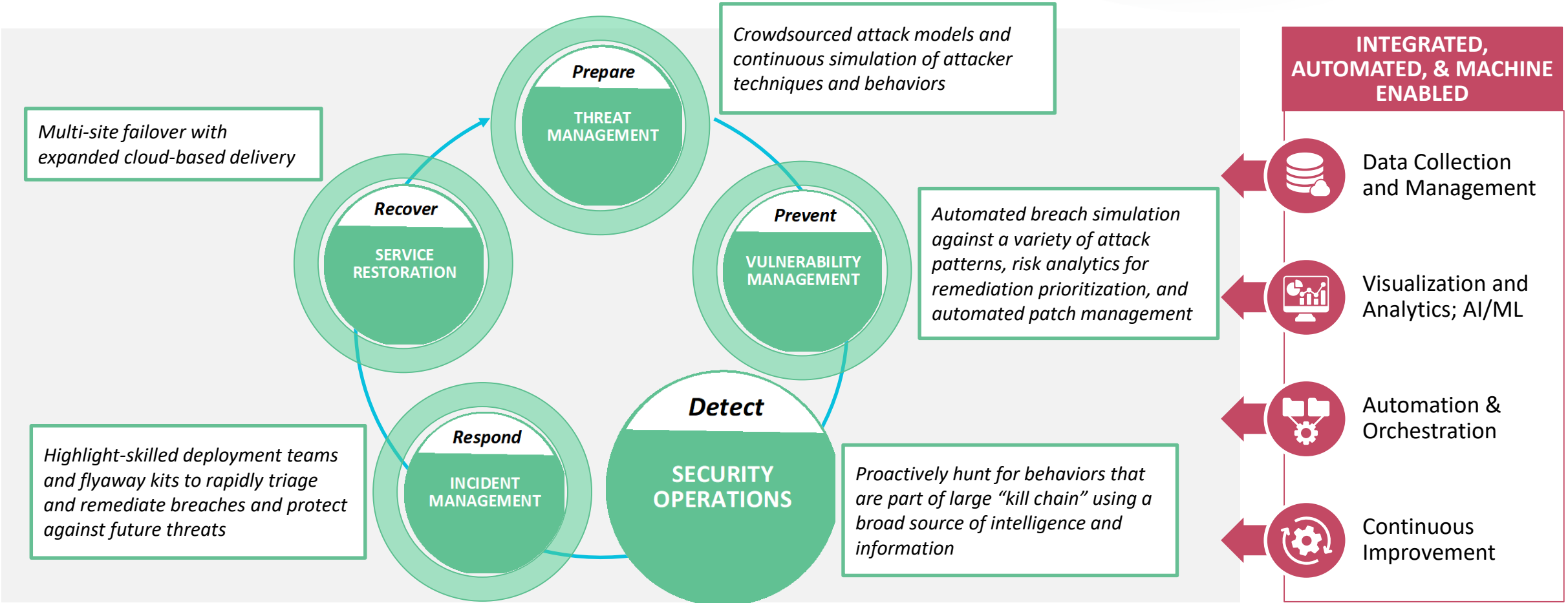
Dynamic Defense Framework

Full Spectrum Cyber Security Operations, With Greater Emphasis On Prepare And Prevent



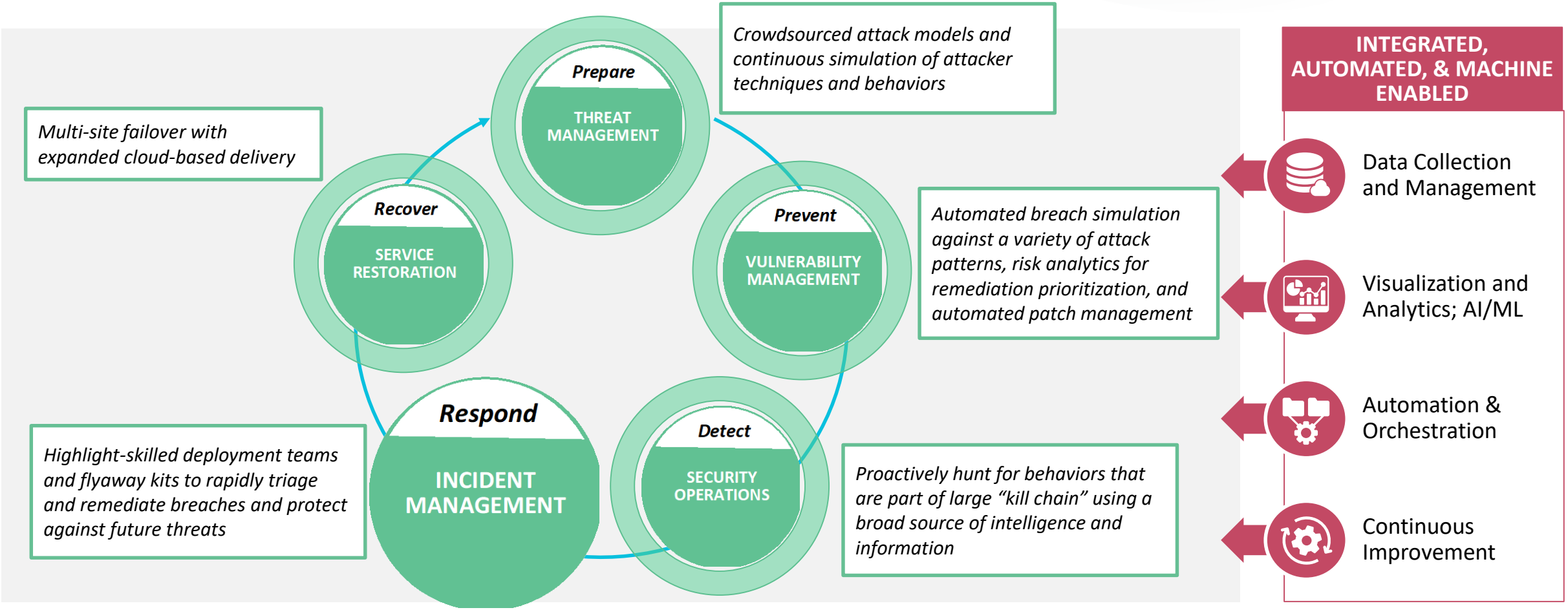
Dynamic Defense Framework

Full Spectrum Cyber Security Operations, With Greater Emphasis On Prepare And Prevent



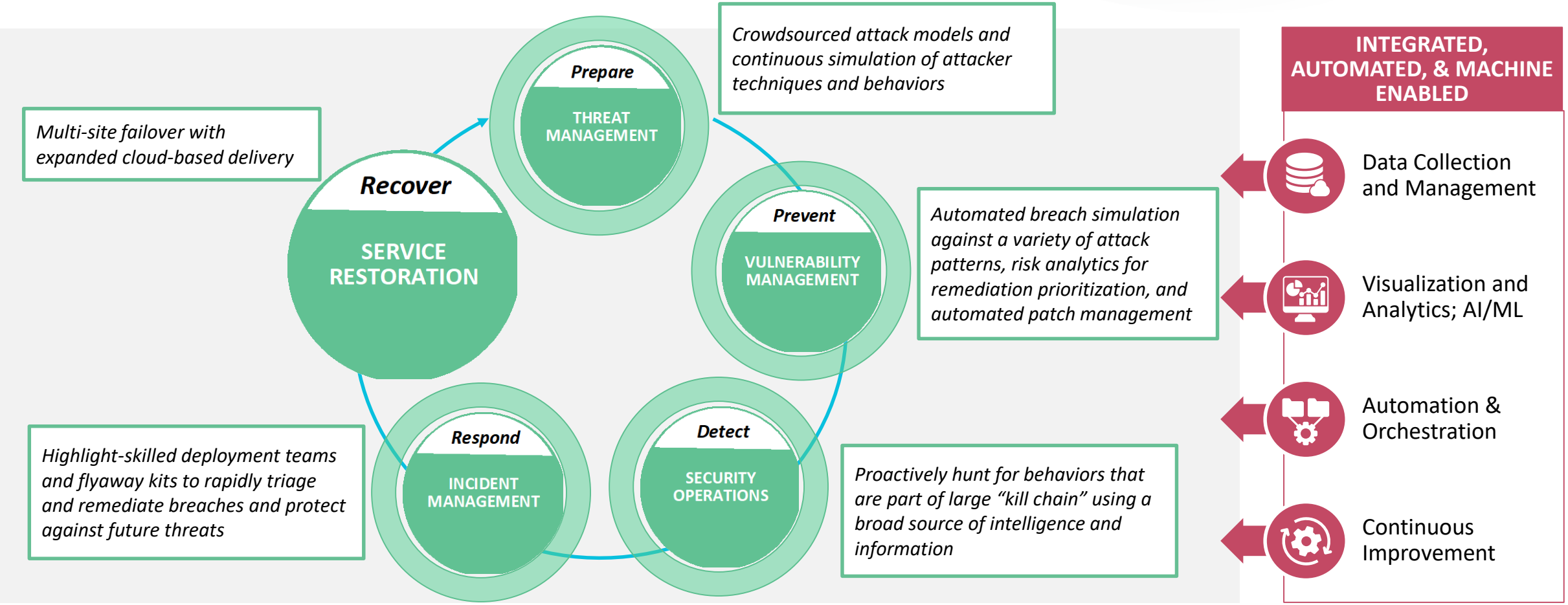
Dynamic Defense Framework

Full Spectrum Cyber Security Operations, With Greater Emphasis On Prepare And Prevent



Dynamic Defense Framework

Full Spectrum Cyber Security Operations, With Greater Emphasis On Prepare And Prevent



PRINCIPLES & CYBER DISCOVERY MODEL

Transformed Environment

Threat Actors & TTPs

The Hacktivist

The Criminal

The Nation-State Agent

The Malicious Insider

Today's Adversaries…

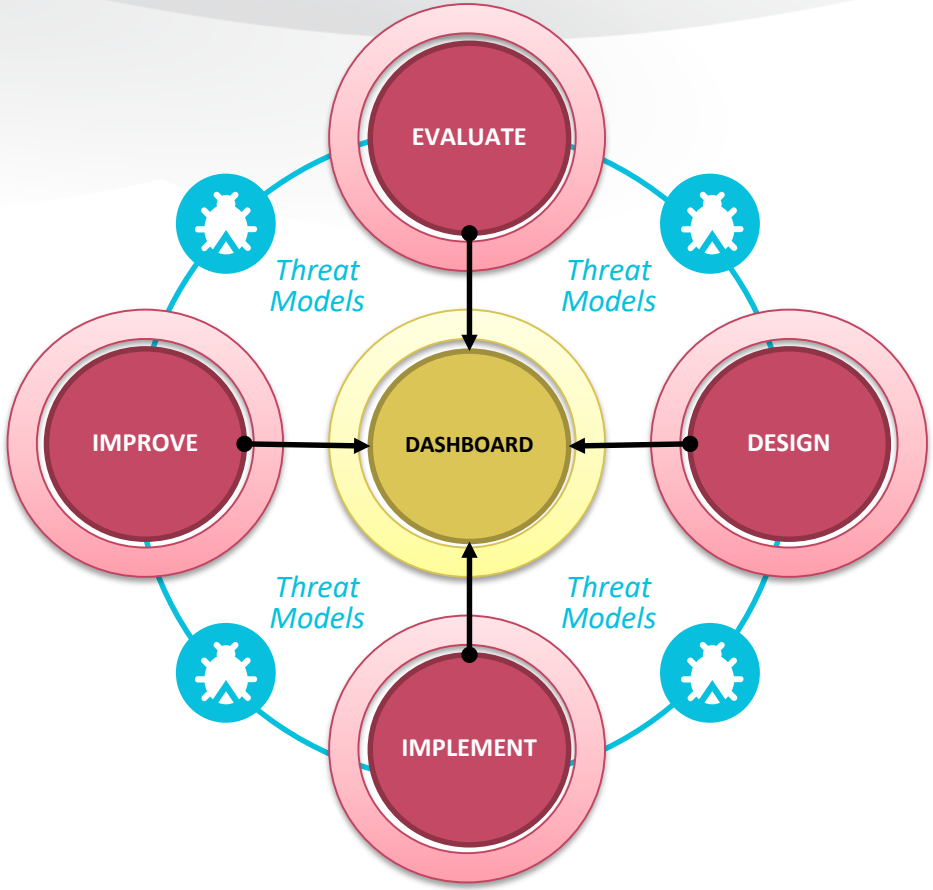
- Target weaknesses in the traditional SOC model
- Can avoid most prevention controls
- Can probe for months, avoiding triggers for threshold-based alerts
- Target the weakest link across an expanded attack surface (e.g., Cloud and OT)
- Can develop amazing levels of intelligence

Design Principles for Proactive Cyber Defense

1	CONTINUOUS IMPROVEMENT	• Program is ***routinely evaluated***, and performance metrics used to ensure controls are operating as intended
2	INTELLIGENCE DRIVEN	• Organizations consume and produce ***threat intelligence to enrich case*** work, direct investigations, gain context on suspicious activity and develop a sophisticated understanding and track specific threats
3	PROACTIVE	• Efforts geared towards ***detecting and hunting for threats*** and enabling prevention of tactics and attack methods (TTPs), in addition to prevention of discrete indicators (IOCs)
4	CONTINUOUS TESTING & EVALUATION	• Threat defenders and red team attackers continuously hunt for exploitable weaknesses and ***immediately deploy mitigating controls*** or process improvements to close gaps
5	INTEGRATED, AUTOMATED, & MACHINE-ENABLED	• ***Traditional IT and new security functions integrated*** into an agile, consolidated, and cohesive organization empowered by workflow automation and orchestration tools to rapidly respond and contain threats while managing risks • Organizations leverage emerging technologies, including advanced analytics, machine intelligence and learning, and workflow automation/ orchestration tools

1 Continuous Improvement

- **Program Evaluations**
  - ***Routinely evaluate*** your Cyber Ops capabilities to ensure you understand current state and ***deficiencies***
  - Get back to ***basics***
  - Take a ***threat-centric approach*** to transform your organization beyond compliance
- **Program Performance Measures**
  - Track the ***effectiveness*** of your controls and capabilities
  - Leverage both ***lead and lag indicators*** to provide insights over a period and quickly determine ***program impact***



"# of corrective actions taken based on threat intelligence and assessments"

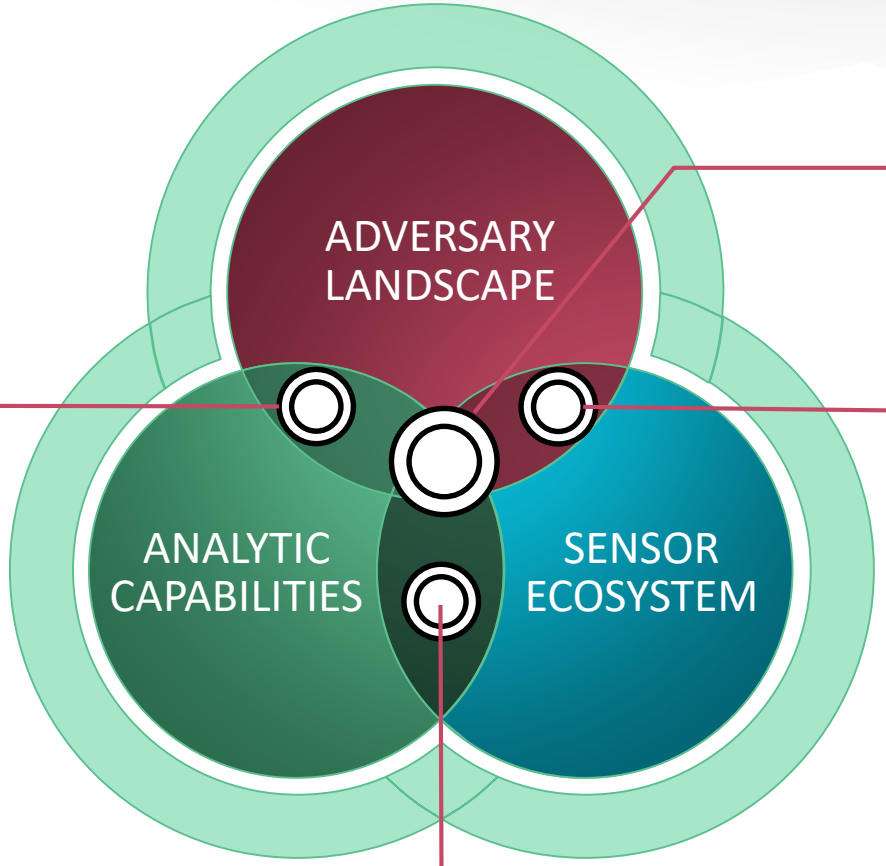
"# of corrective actions taken based on vulnerability intelligence and assessments"

"Mean time to detect an attack"

"Mean time to respond to a security incident"

"Mean time to restore to normal business operations (following a security incident)"

Cyber Discovery Model



CYBER DISCOVERY ZONE

This is our true, limited view into Cybersecurity

AREA OF INVISIBILITY

- Analytic capability w/o data collection

AREA OF INVISIBILITY

- Data collection w/o parsing or analytic processing

NOISE!

- False positives, reducing operational effectiveness

2 Intelligence-Driven

CYBER THREAT INTELLIGENCE

STRATEGIC

- "Big Picture" analysis
- Communicating threats as business risks
- "Over the horizon" view that provide leaders with warnings about possible future threats

TACTICAL

- Host and network-based artifacts and IOCs
- Signatures to detect the presence of adversary tools
- Defensive actions as the adversary moves through the MITRE ATT&CK

OPERATIONAL

- Threat actor group campaigns and planning cycles
- Threat actor group capabilities and tool sets
- MITRE ATT&CK framework analysis of adversary tactics

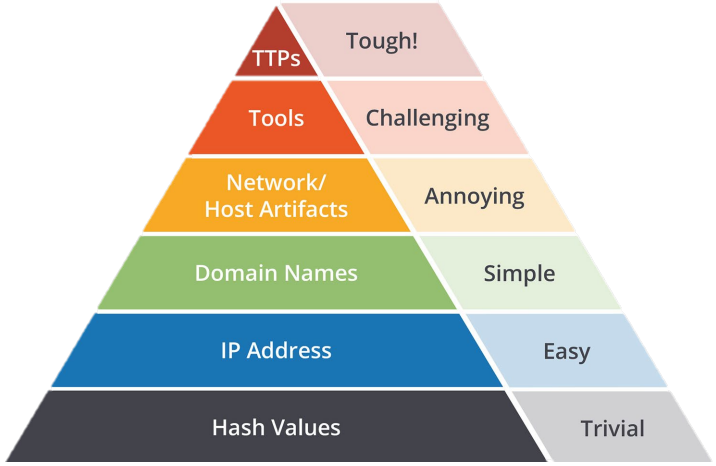
CONTEXT IS KEY

The Security Industry is rooted in a lie…

Despite what you have been told

YOU CAN PREVENT ATTACKS!

3 Proactive



CYBER PAIN PYRAMID

- Threat Actors can change their Hashes, IPs, and domains with ease
- Advanced threats thrive off hiding in the noise of your environment
- Network data becomes challenging as encryption becomes ubiquitous
- Hunting for TTPs at the endpoints pushes adversaries further up the pain pyramid

	IOCs/Signatures	Detection	Threat Based TTP	Heuristics	Haystacks
# Hits	Low	Low-Med	Medium	High	100,000+
TP %	95%	85%	35%	2%	< 1%

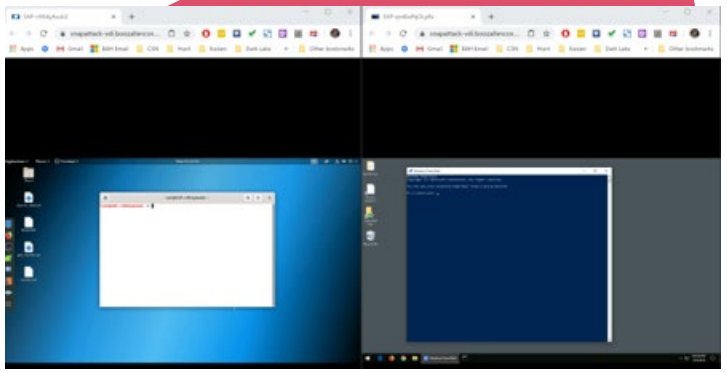
KNOWN VS. UNKNOWNS

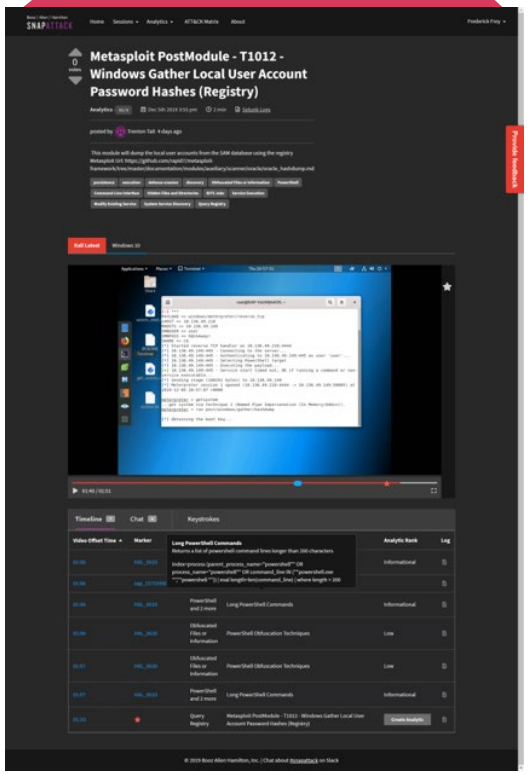
REACTIVE DETECTION vs. **HYPOTHESIS DRIVEN DISCOVERY**

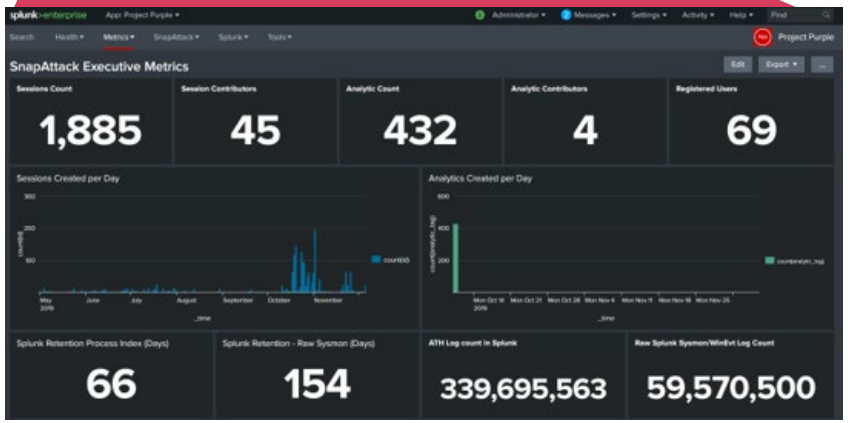
Real-time **Cyclical**

*Threat hunting is an **analyst-centric** process that enables organizations to proactively uncover **hidden threats**, lurking in the noise of your environment.*

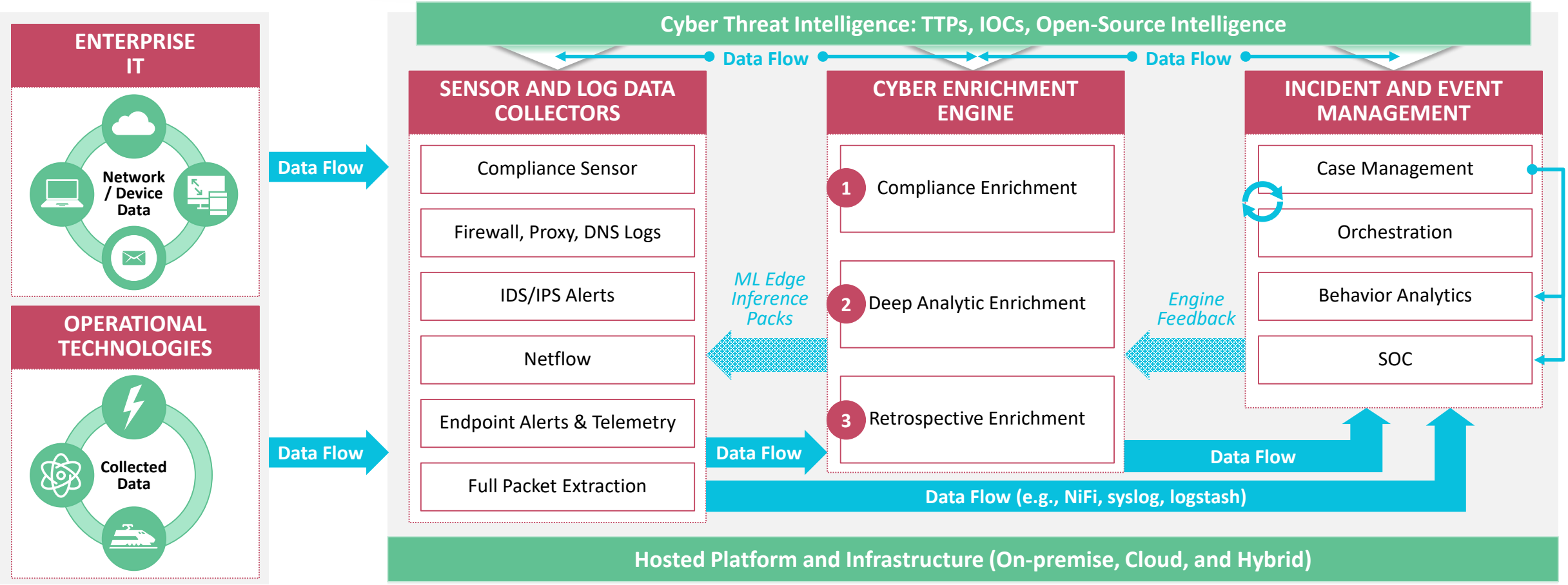
4 Continuous Testing & Evaluations







5 Integrated, Automated, & Machine-based



1 COMPLIANCE ENRICHMENT
Integrates business and mission context

2 DEEP ANALYTIC ENRICHMENT
Leverages deep packet inspection, AI/ML, and proprietary hunt analytics to develop tailed behavioral models

3 RETROSPECTIVE ENRICHMENT
Leverages new threat intel to uncover persistent threats in historical data

RECOMMENDATIONS

Takeaways

1 CONTINUOUS IMPROVEMENT	2 INTELLIGENCE DRIVEN	3 PROACTIVE	4 CONTINUOUS TESTING & EVALUATION	5 INTEGRATED, AUTOMATED, & MACHINE-ENABLED
Routinely evaluate your program and leverage KPIs to continuously monitor performance	Incorporate threat information and intelligence into tailored detection logic and prioritized remediation efforts	Integrate Vulnerability Management capabilities in Cyber Ops functions, expand vulnerability testing across the full asset stack, and proactively hunt for threats	Implement frequent testing and review of defensive tactics and controls	Automate routine activities and accelerate manual actions efficiently utilizing available resources

BENEFITS				
Automate the low hanging fruit, while increasing mitigations against the advanced threats	Single-view of your environment's vulnerabilities	Efficiently identify and leverage investments, tools, capabilities	Improved event evaluation based on threats instead of static indicators	Increased information exchanges and tool integrations

Apply What You Have Learned Today

RSA 2020

Action #1: Enjoy the presentation!

+1 MONTH

Action #1: Identify critical assets

Action #2: Perform a cyber operation's program evaluation

Action #3: Inventory your program metrics

+3 MONTHS

Action #1: Create a detection logic using the Sigma Project (https://github.com/Neo23x0/sigma)

Action #2: Enhance program metrics where applicable

Action #3: Perform kill chain analysis across 3 critical threats

+6 MONTHS

Action #1: Create mitigation strategy

Action #2: Integrate vulnerability information

Action #3: Create program transition plan where applicable

Questions?