The Next Evolution

Using Automation to Outsmart Attackers

proarch

MEET OUR PRESENTERS

Michael Wurz

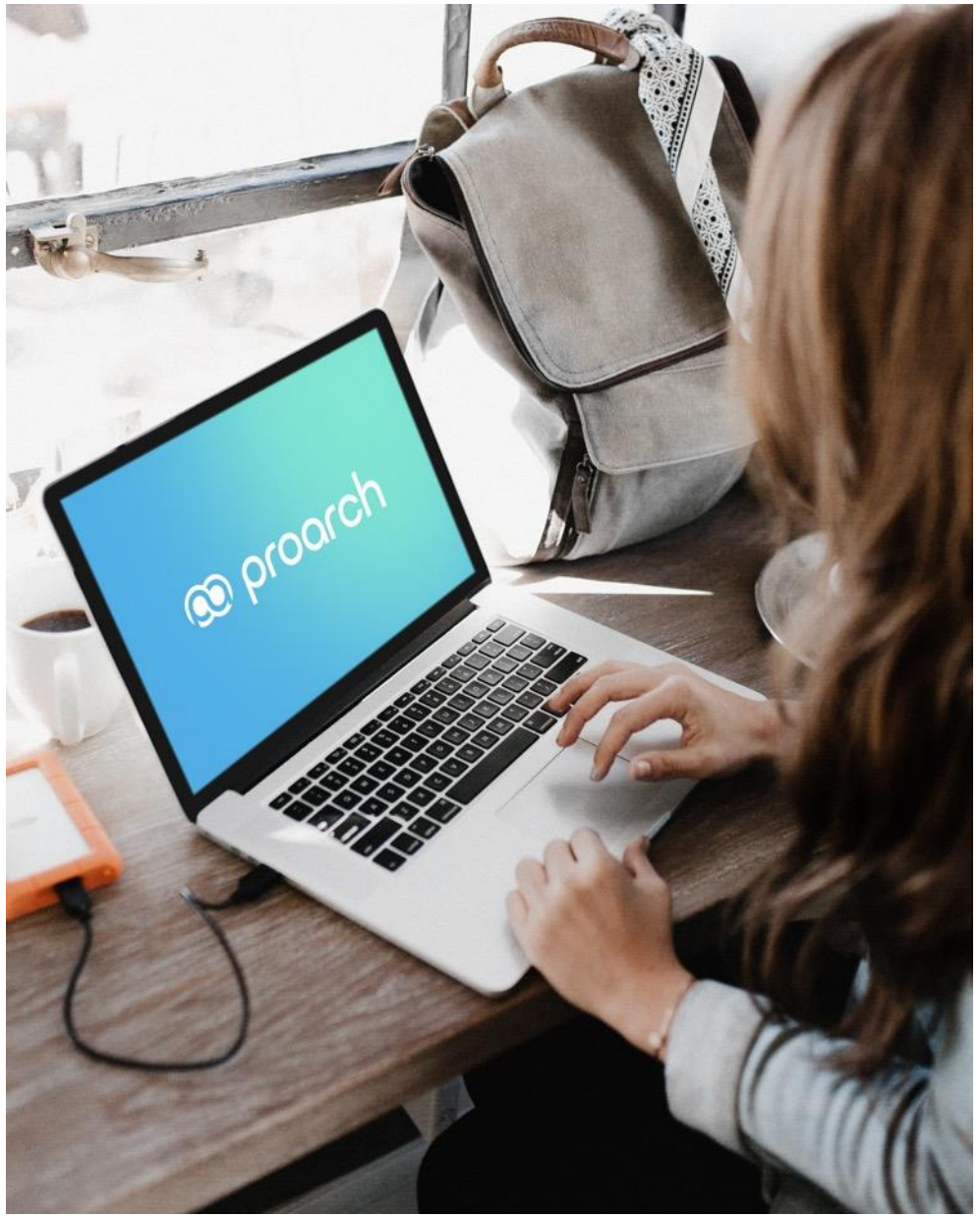
Security Solution Architect &
Technical Lead

Brian Rowe

Security Team Lead

Today's Agenda

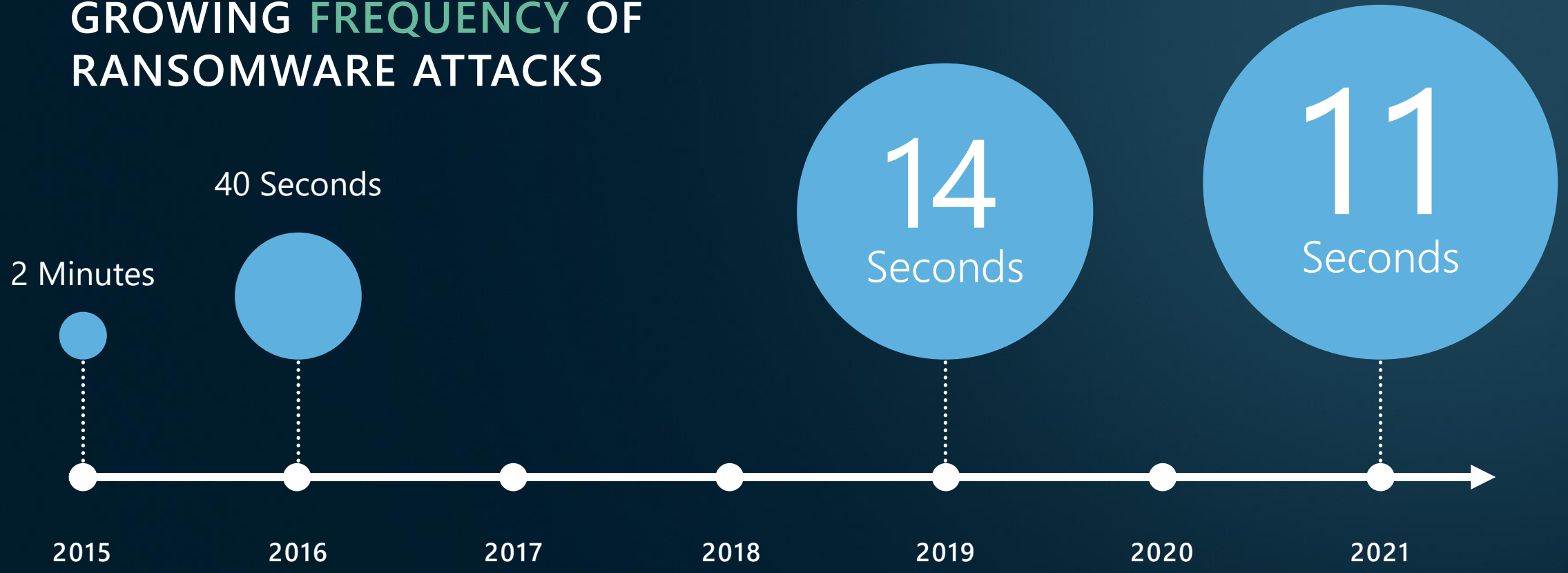
- What's changed in cybersecurity
- How ProArch is responding
- New Managed Detection and Response architecture
- Demo: D3 Security - SOAR
- Demo: Recorded Future – Threat Intelligence
- What's this means for our clients



proarch

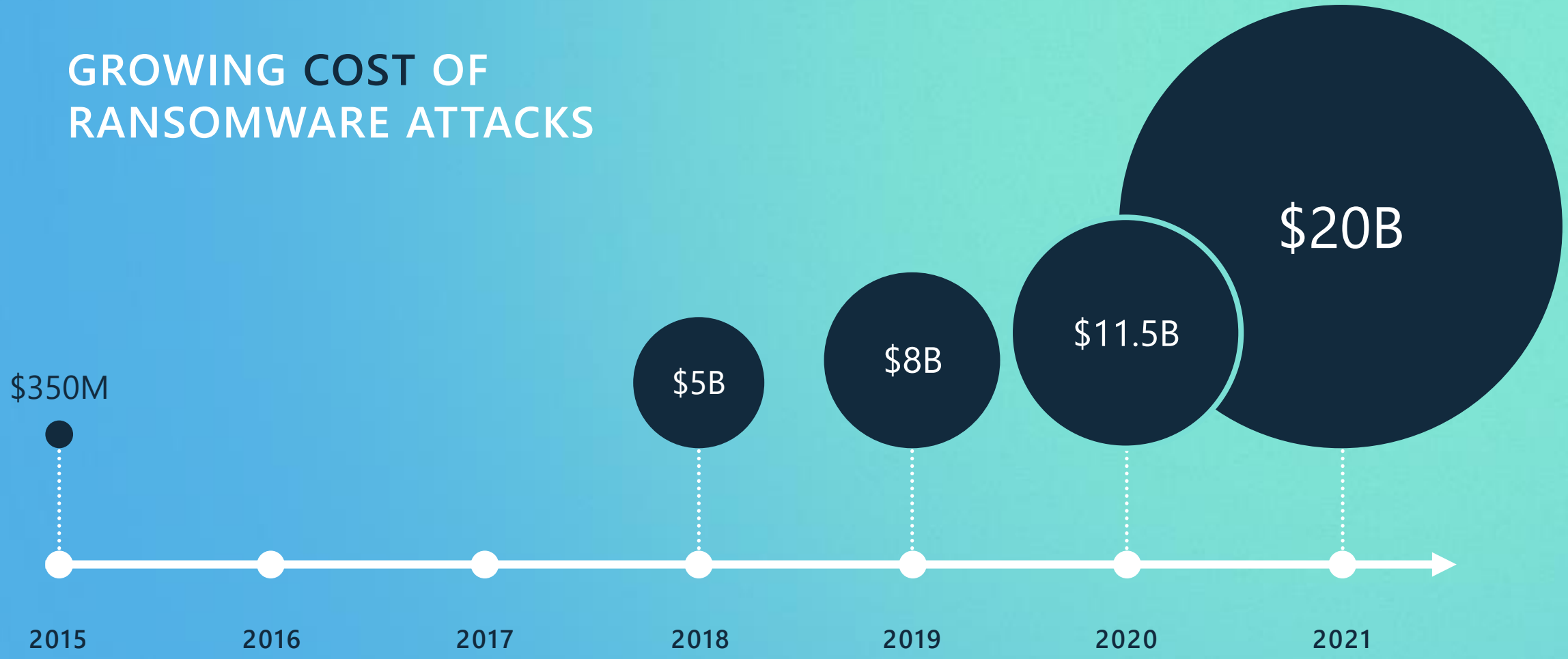
What's Changed in Cybersecurity?

GROWING FREQUENCY OF RANSOMWARE ATTACKS



By 2031, attacks will occur every 2 seconds

GROWING COST OF RANSOMWARE ATTACKS



The cybercriminal economy reached **$6 trillion** last year

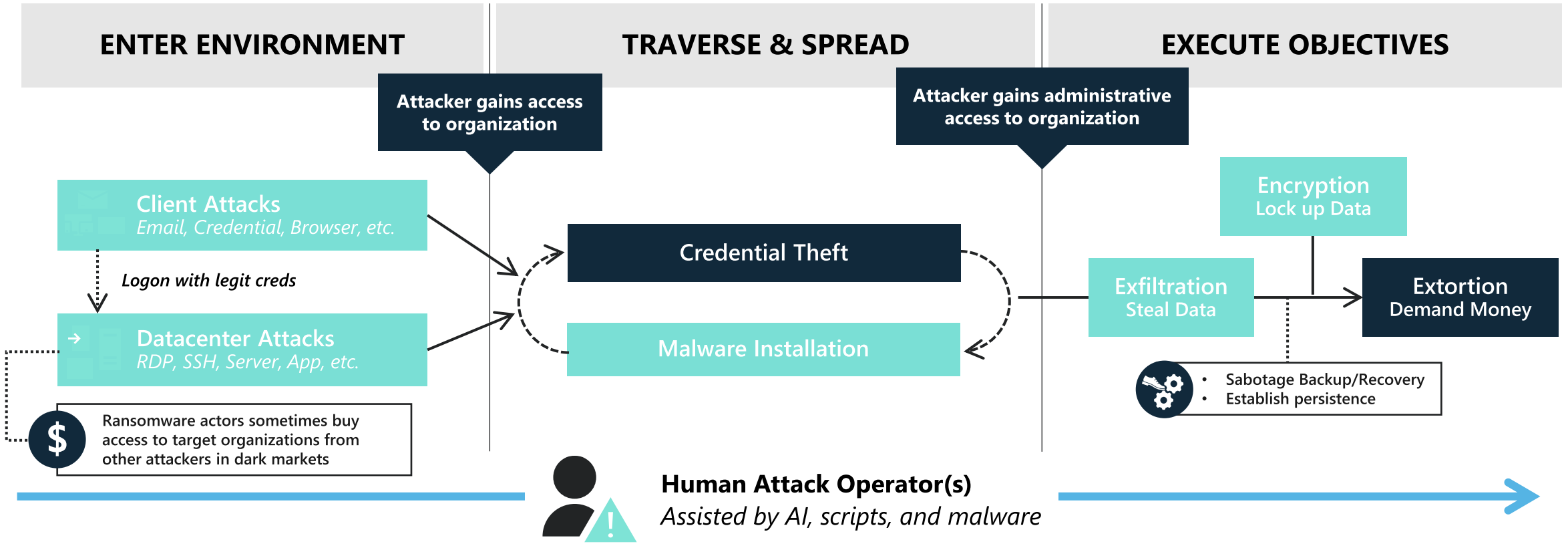
Attackers Are Taking Advantage

- Expanding attack surface
- Modern technology
- Remote workforce

- Volume of activity
- Alert overload
- Talent and skills shortage

- Exploit marketplace
- Ransomware-as-a-service
- Cryptocurrency

Automation: Not Just for the Good Guys



Automation Gives Attackers the Upper Hand

Automated attacks can constantly mutate, meaning security solutions don’t see the same attack twice.

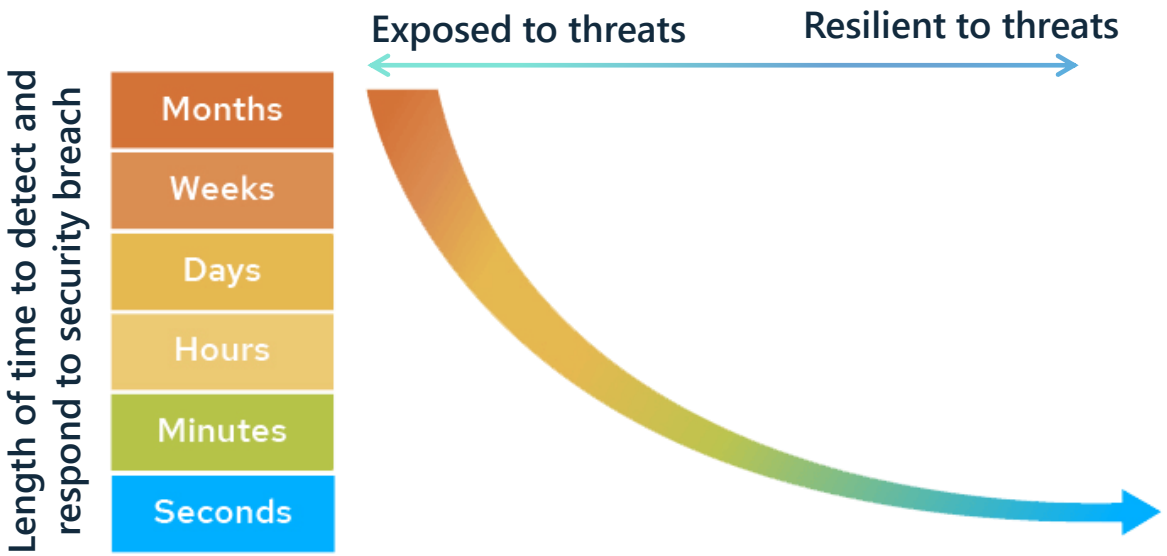
Attacks are cheaper to produce, resulting in ability to spray more sophisticated attacks widely.

Attackers learn targets’ online behavior and launch automated phishing campaigns at scale that are challenging to detect.

KPIs: The Need for Speed

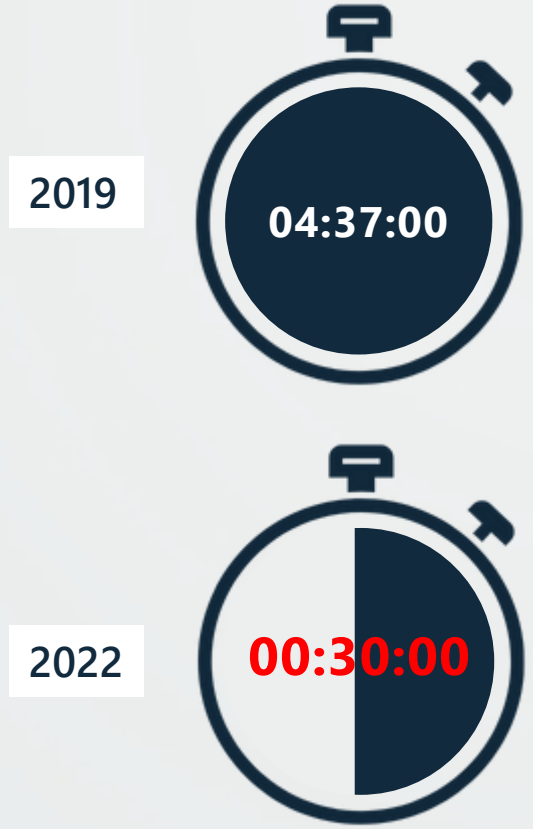
Mean-Time-To-Detect: Average time to identify a threat that requires analysis and response.

Mean-Time-To-Respond: Average time to respond and resolve an incident.



Breakout Time

Average time an adversary moves laterally.



proarch

How is ProArch Responding

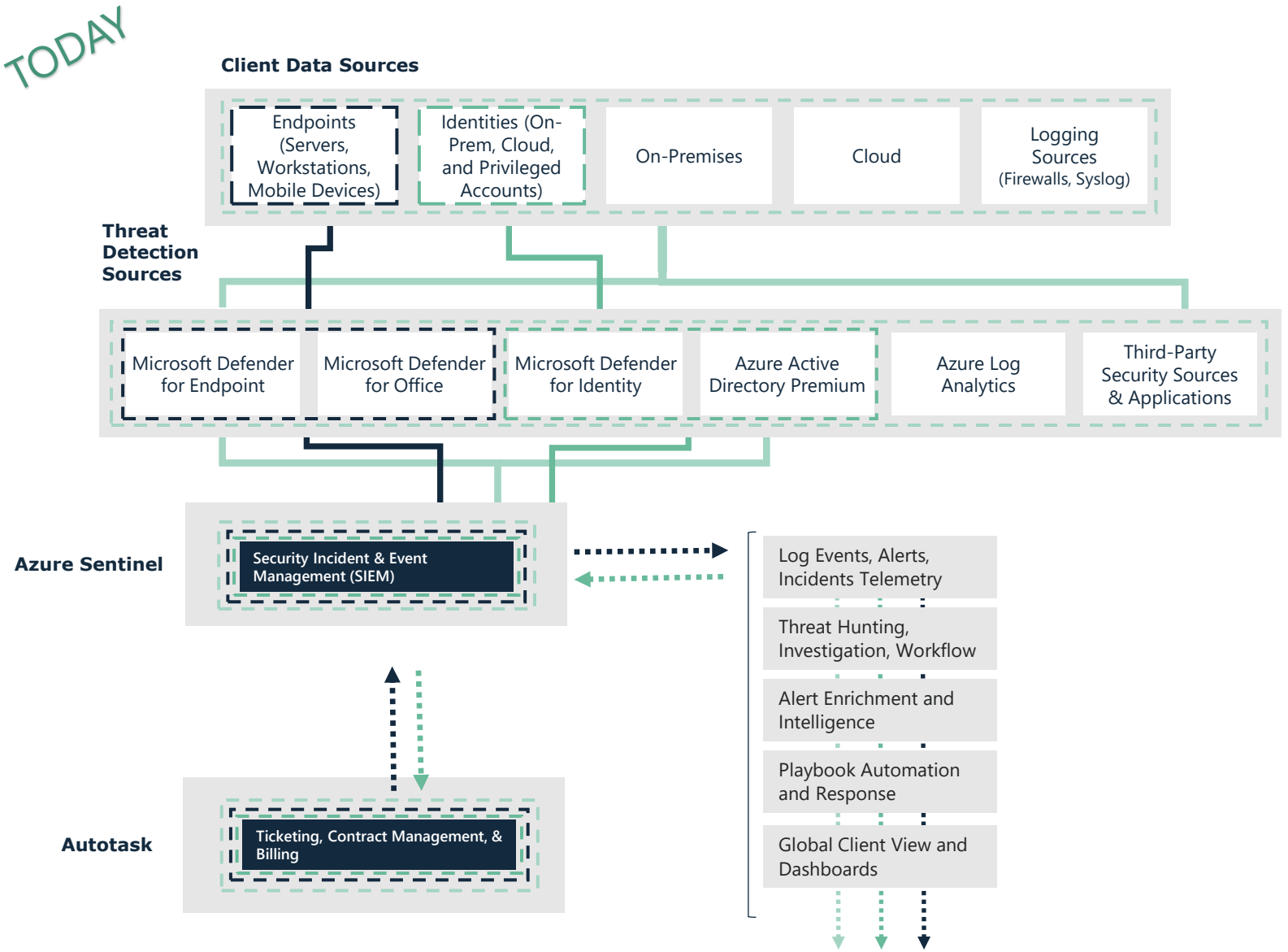
How MDR Works

Threat detection sources and sensors are deployed across networks, cloud services, endpoints, and identities collecting telemetry- making it possible to ingest real-time risk data-points.

Threat intelligence backed by deep context, customer information, and the MITRE ATT&CK framework enhances risk data.

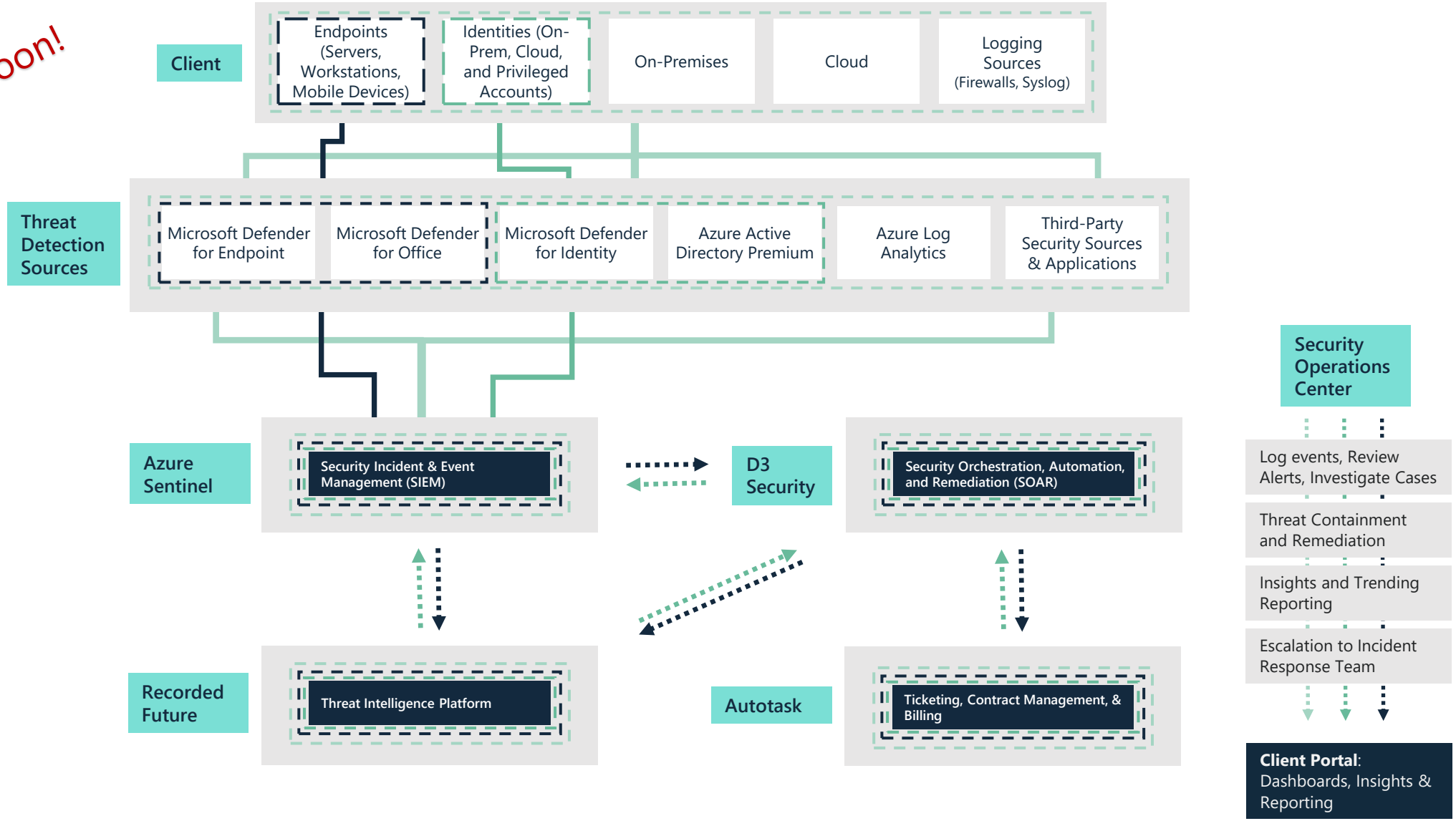
The ProArch SOC team analyzes cases and performs a thorough threat investigation to confirm indicator of compromise or false positive—24 hours a day.

Transition to ProArch Incident Response in the event of compromise.



How MDR Works

Coming Soon!



D3 Security SOAR Platform Highlights

Integrations

Integrates with 300+ products

- SOC, InfoSec, IT tools
- Forensics
- DevOps
- Cloud operations
- Physical security
- Vulnerability Scanner
- Identity Management

Case Management

Extends case management to digital forensics use-cases, with evidence tracking and chain-of-custody capabilities for digital and physical artifacts.

Playbooks

Fully customizable workflows that automate tasks and coordinate actions across tools and workforce.

Alert Enrichment

By the time an analyst sees an event in D3, it has already been enriched with:

- contextual data from threat intelligence platforms
- past incidents
- MITRE ATT&CK matrix

MITRE ATT&CK

D3 uses the MITRE ATT&CK Matrix, the largest information set of adversary tactics, techniques, and procedures, to make sense of threats and vulnerabilities.

D3 Security SOAR Key Benefits

- Holistic Visibility & Correlation
- MITRE ATT&CK Kill Chain Mapping & Monitoring
- Threat Intelligence Integration
- Noise Reduction & Alert Prioritization
- Faster Alert Triage & Response (MTD & MTR)
- Enhanced Communication & Reporting
- Automation!

Review **50%** more alerts

Identify threats **10x** faster

Resolve threats **63%** quicker

Identify **22%** more threats before impact

Boost analyst efficiency by **32%**

Recorded Future Threat Intelligence Platform Highlights

Intelligence Graph

Delivers the right intelligence at the right time.

Automatically connects the dots in a massive data set to tell an end-to-end story of an attack, including

- the victim
- the attacker
- the infrastructure used to carry out the attack

Intelligence Cards

Single view of essential investigation information dramatically increases the speed and efficiency of threat analysis and allows for confident decision making quickly.

Intelligence Modules

ProArch subscribes to 5 modules:

- Brand
- Threat
- SecOps
- Vulnerability
- Third-Party

Threat Views and Hunting

Real-time collection of intelligence from dark web sources to understand the adversary.

Includes YARA, Snort, and Sigma rules to hunt for adversaries, malware, or traffic of interest.

proarch

Demo of New Capabilities

proarch

What This Means for Our Clients

Business Impact: Primary Loss

Productivity: Inability to generate value.

Wages of idle workers, lost sales in an outage.

Response: Managing and responding to the loss event.

Incident response, disaster recovery, external counsel/forensics fees, breach notification.

Replacement: Capital expenditure to repair/replace tangible/depreciable assets.

Replacing IT hardware, repairing facilities.

Business Impact: Secondary Loss

Competitive Advantage: Value of lost market share if competitor obtained and exploited information.

Loss from compromise of trade secrets, IP.

Fines/Judgements: Legal, regulatory, or contractual penalties.

Reputation Damage: Loss from negative perceptions.

Uncaptured future revenue, increased cost of capital.

Improve Return on Security Investment (ROSI)

$$\text{ROSI (\%)} = \frac{(\text{Risk Exposure} \times \text{Mitigation Ratio}) - \text{MDR Cost}}{\text{MDR Cost}}$$

XYZ Corp. Example

$50,000: losses from a breach

4 attacks per year

$60,000: MDR cost

90%: MDR risk mitigation

Risk Exposure: $50,000 x 4 attacks per year **= $200,000**

$$\frac{(\$200{,}000 \times 90\%) - \$60{,}000}{\$60{,}000} = 200\% \text{ ROSI}$$

Business Benefits

Boost Cyber Resilience

- Have confidence you're prepared for an attack

Speed Threat Detection and Response

Improve Return on Security Investment

Eliminate Alert Overload

Meet KPIs for Compliance

SOC Advanced Threat Hunting and Investigation

- Focus on priority alerts and recommendations
- Less time on reports and repetitive alerts

ProArch Client Security Portal - 2023

THANK YOU FOR JOINING US | WWW.PROARCH.COM