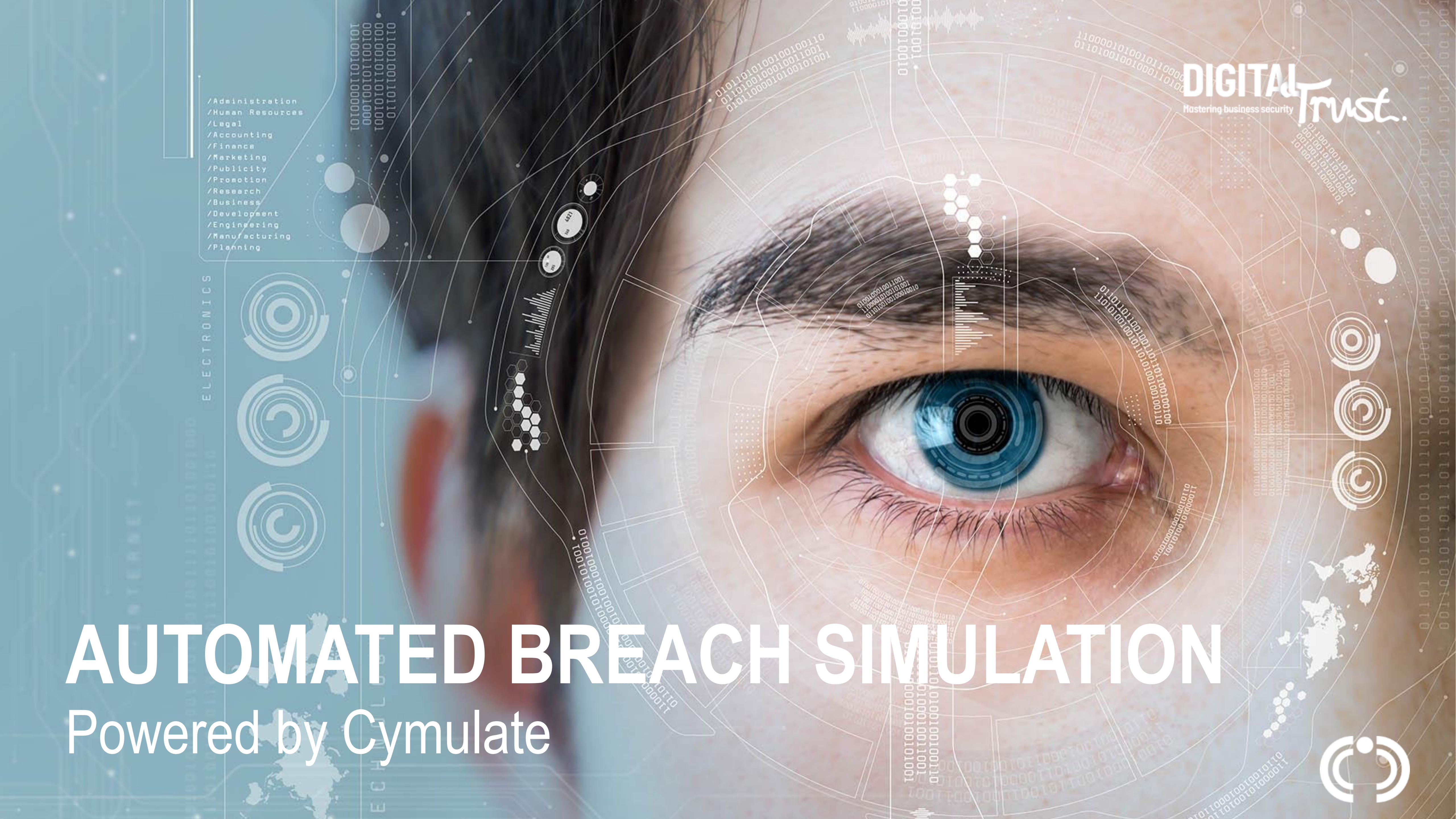
DIGITAL Trust
Mastering business security



AUTOMATED BREACH SIMULATION

Powered by Cymulate

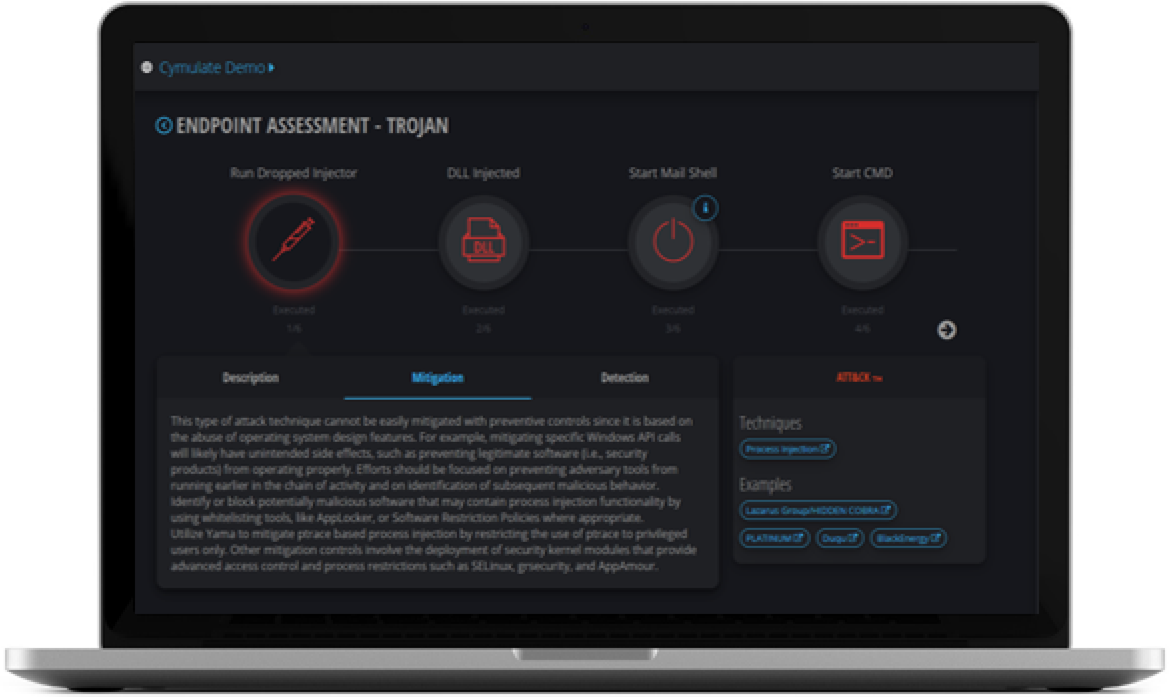
CYMULATE INTRODUCTION

A Breach & Attack simulation platform

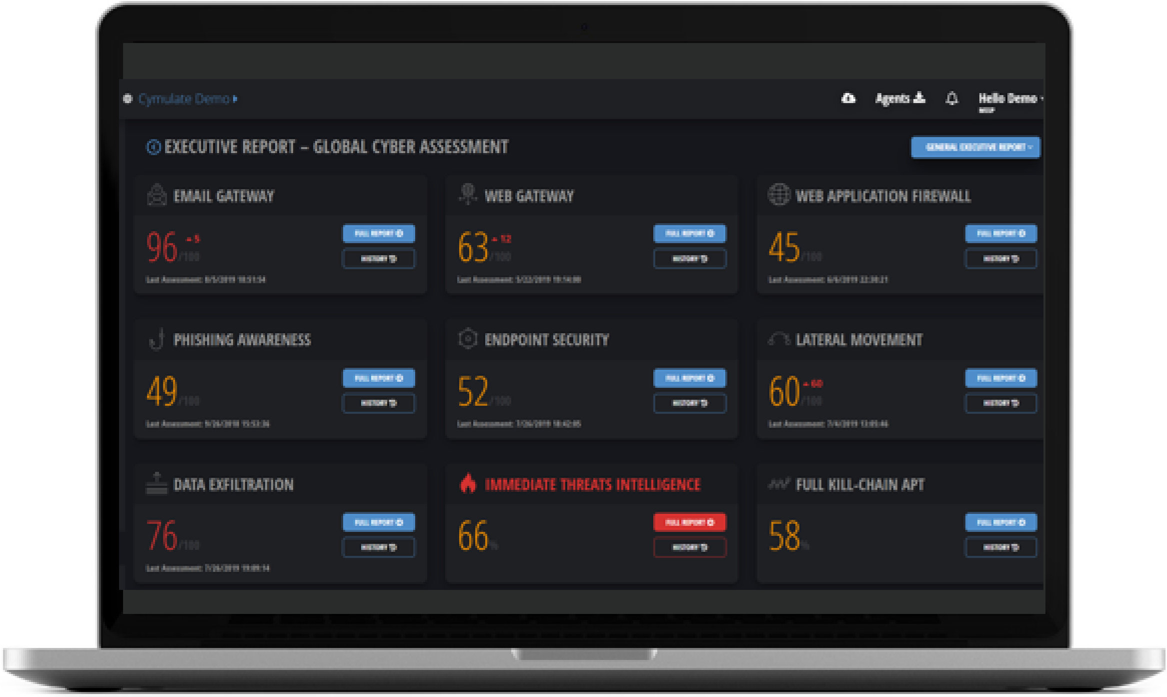
Test security assumptions, identify possible security gaps and receive immediate actionable insights

Can simulate multiple attack vectors

Test against latest vulnerabilities and threats derived from Cymulate's research department



This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.
Identify or block potentially malicious software that may contain process injection functionality by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.
Utilize Yama to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced access control and process restrictions such as SELinux, grsecurity, and AppAmour.



BREACH ATTACK AND SIMULATION

"The premise of Breach Attack and Simulation tools is to launch reverse engineered threats, as you see them in the wild, on your own network, with the detonation code removed. All the pathways and methodologies of an APT, without the damage".

01 How safe is my company right now? How good is your security posture?

02 Where am I most vulnerable?

03 Are we protected against the latest threats?

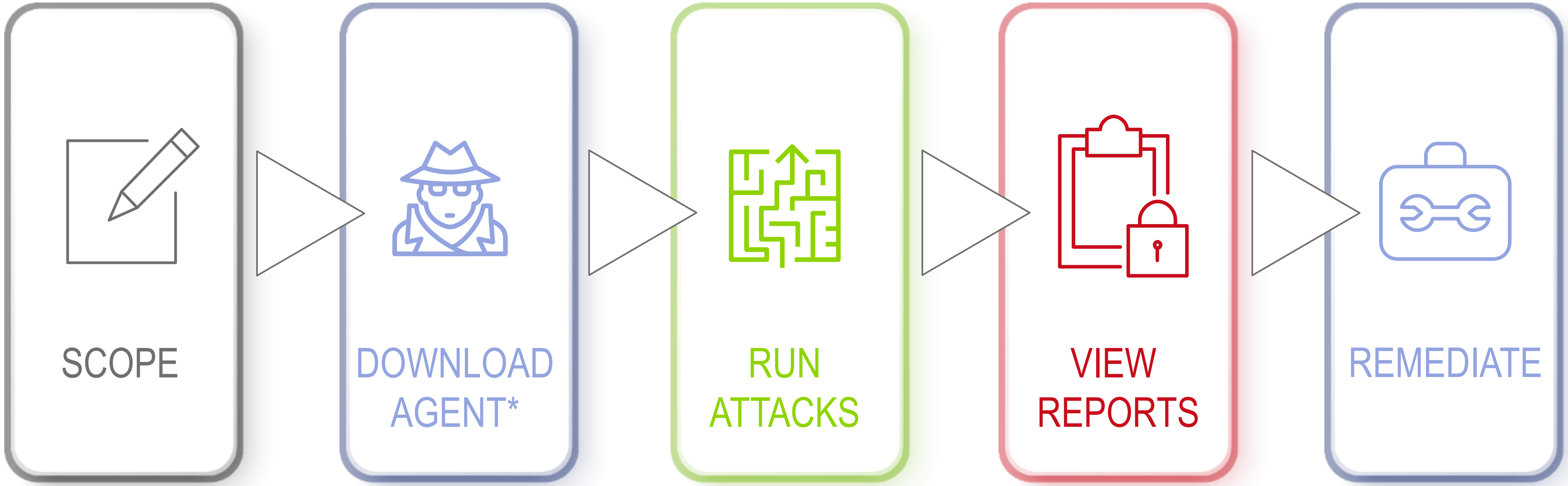
04 How can I continuously validate compliance?

05 How do I select the best product for my company

06 I need a way to convey risk to the board

07 What do you need to spend money, time, resources on? How do you justify the spend?

HOW CYMULATE WORKS



Machine with Agent installed can be:

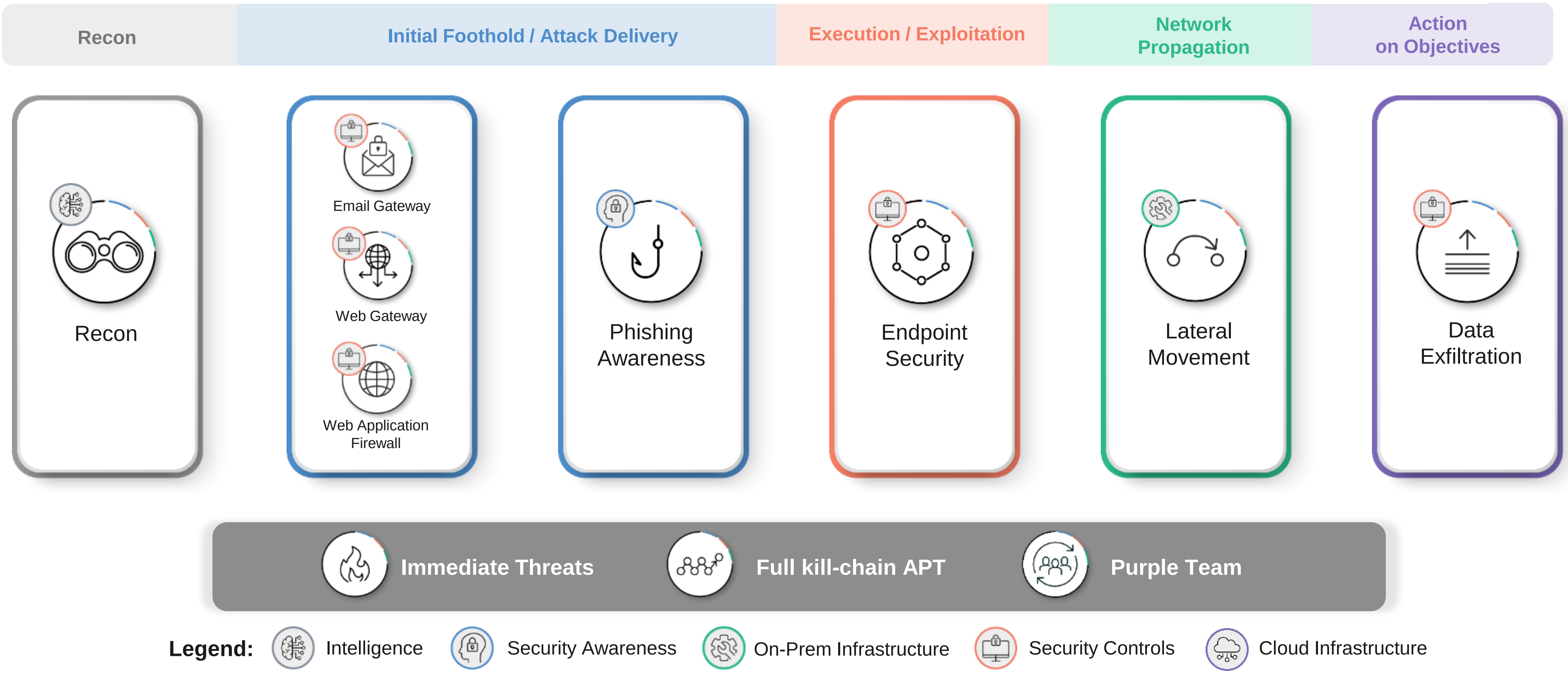
- A standard build employee laptop or desktop
- A VM with an e-mail client and web gateway aligned, behind the perimeter Firewalls

Pre-Reqs

- Clear Pre-requirements documents available to ensure smooth transition

* A minimum of one **TARGET** endpoint with **ONE** agent deployed per e-mail and web gateway

VECTORS OVERVIEW



Recon | Initial Foothold / Attack Delivery | Execution / Exploitation | Network Propagation | Action on Objectives

Recon

Email Gateway

Web Gateway

Web Application Firewall

Phishing Awareness

Endpoint Security

Lateral Movement

Data Exfiltration

Immediate Threats

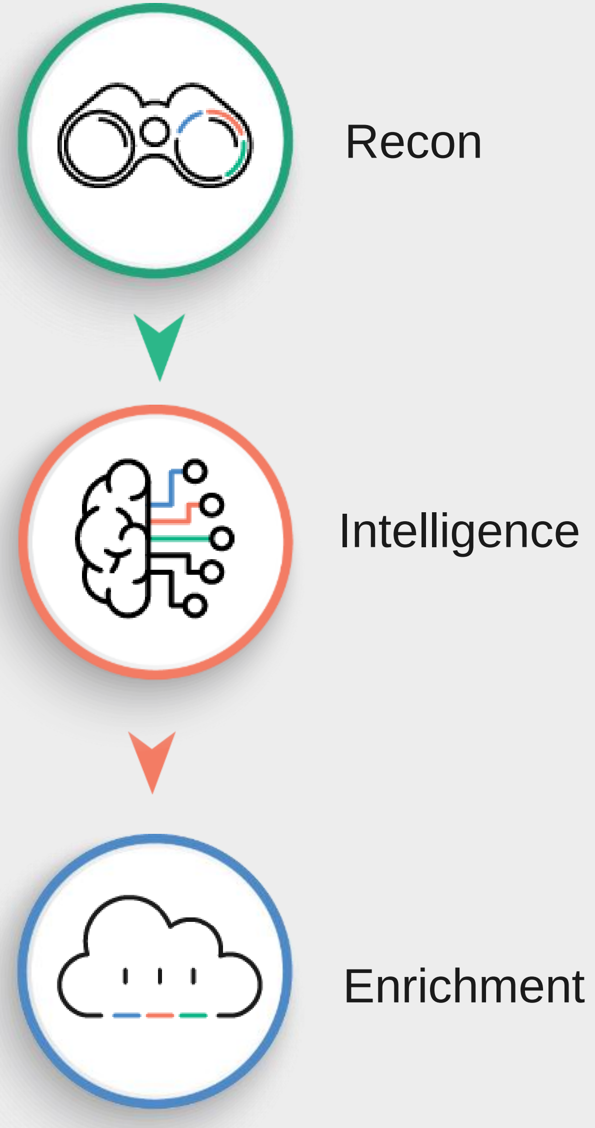
Full kill-chain APT

Purple Team

Legend: Intelligence · Security Awareness · On-Prem Infrastructure · Security Controls · Cloud Infrastructure

RECON

- Know what your attackers know…
  - Gathers intelligence and identifies internet facing weaknesses and vulnerabilities
  - Findings mapped to the MITRE ATT&CK™ Pre-Attack phase
  - Types of Intelligence:
    - Leaked credentials
    - Infrastructure weaknesses
    - Domain mimicking
  - Enriches security testing with Intelligence
  - Detect website which are not protected by a WAF



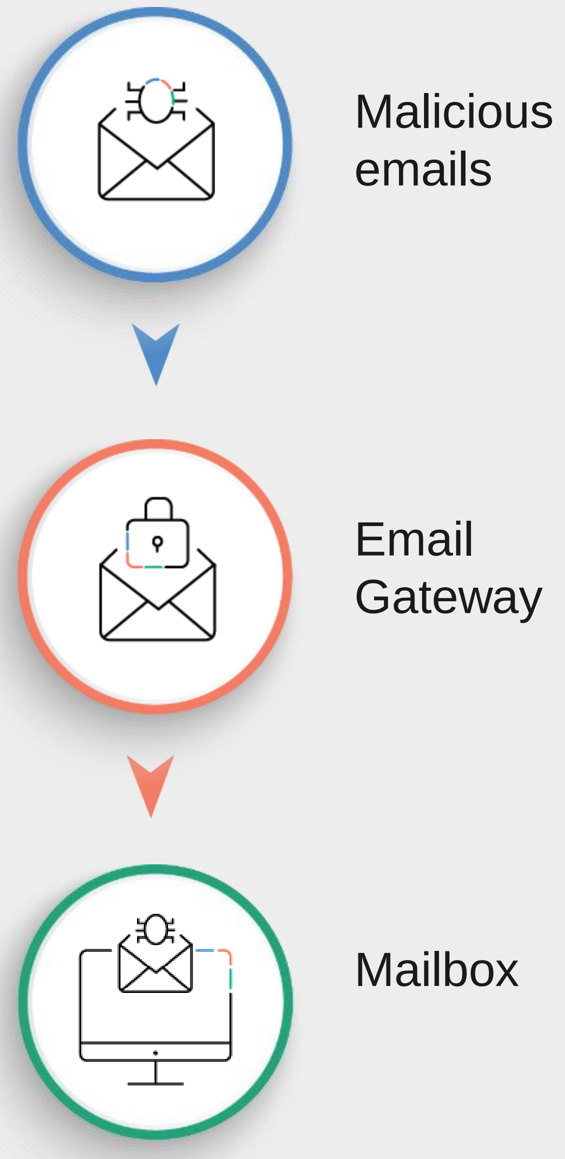
Recon

Intelligence

Enrichment

EMAIL GATEWAY

- Test your email security controls against a comprehensive combination of crafted test emails:
  - Email headers – spoofing
  - Email body – malicious links
  - Attachments - many file types with embedding
  - Attachments - malicious payloads
- Extensively tests the effectiveness of email security controls, e.g., email G/W, Sandbox and Network A/V
- Provides clear remediation guidance to fix misconfigurations and close security gaps



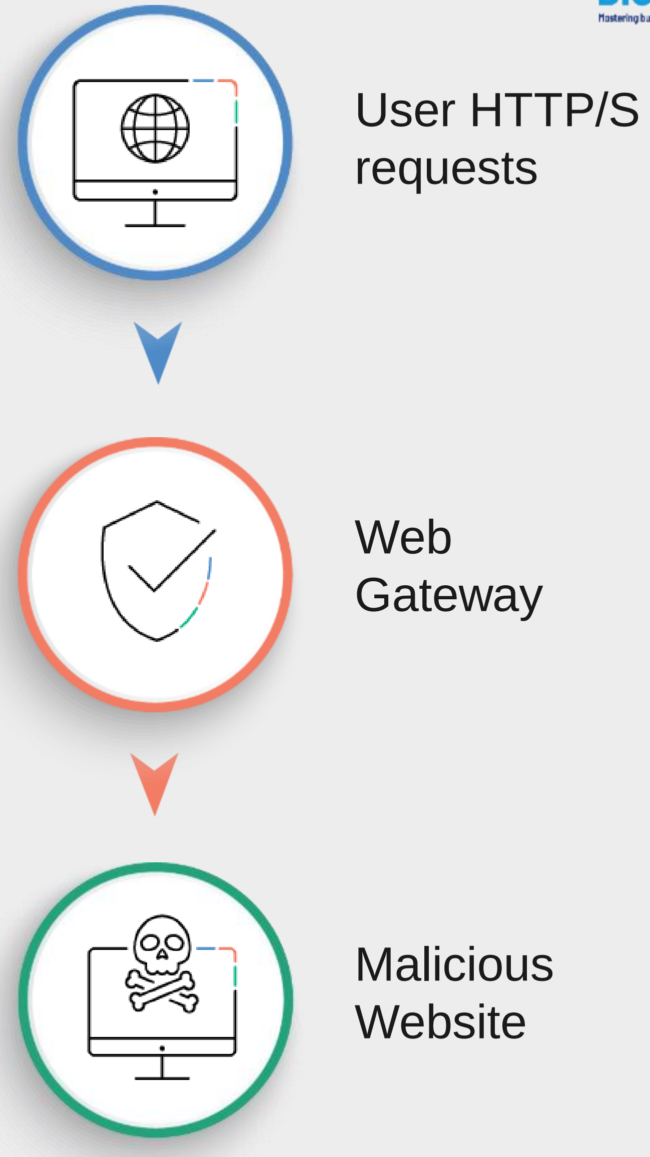
Malicious emails

Email Gateway

Mailbox

WEB GATEWAY

- Test your web security controls against a comprehensive combination of web activity:
  - Access to malicious web sites
  - Downloads from malicious web sites
  - Command & control communications
  - Inappropriate content
- Extensively tests the effectiveness of web security controls
- Test URLs and objects updated daily
- Provides clear remediation guidance to fix misconfigurations and close security gaps



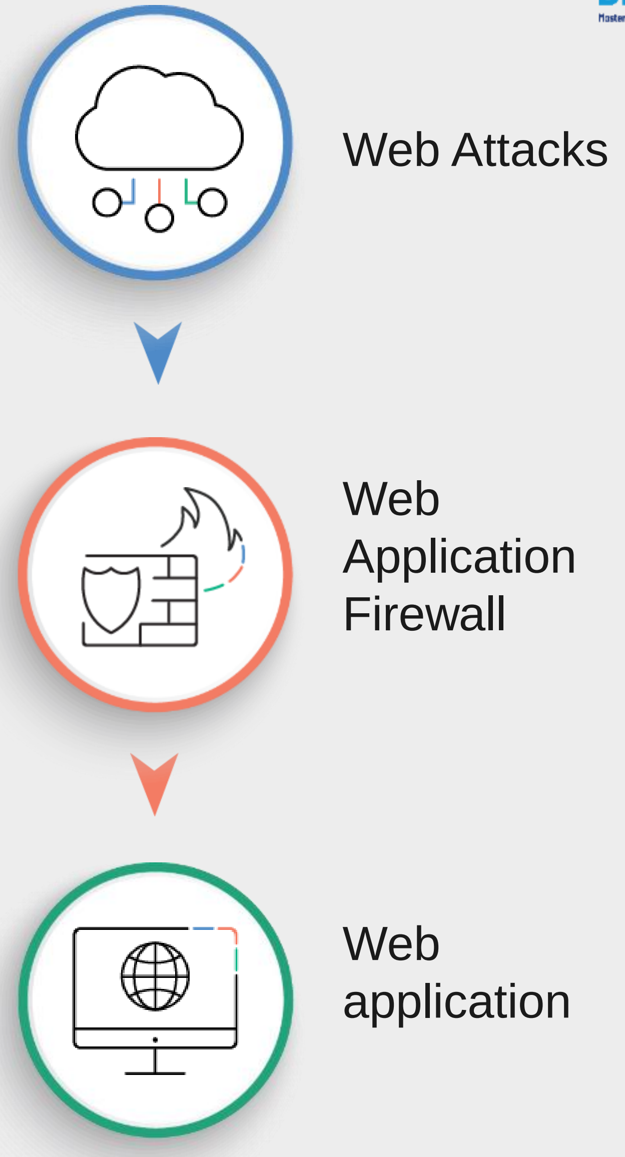
User HTTP/S requests

Web Gateway

Malicious Website

WEB APPLICATION FIREWALL

- Test that your WAF protects web application vulnerabilities and threats, including:
  - SQL Injections
  - Cross Site Scripting
  - File Inclusion
  - Command Injections
  - Vulnerabilities
- Extensively tests the effectiveness of the web application firewall
- Provides clear remediation guidance to fix misconfigurations and close security gaps



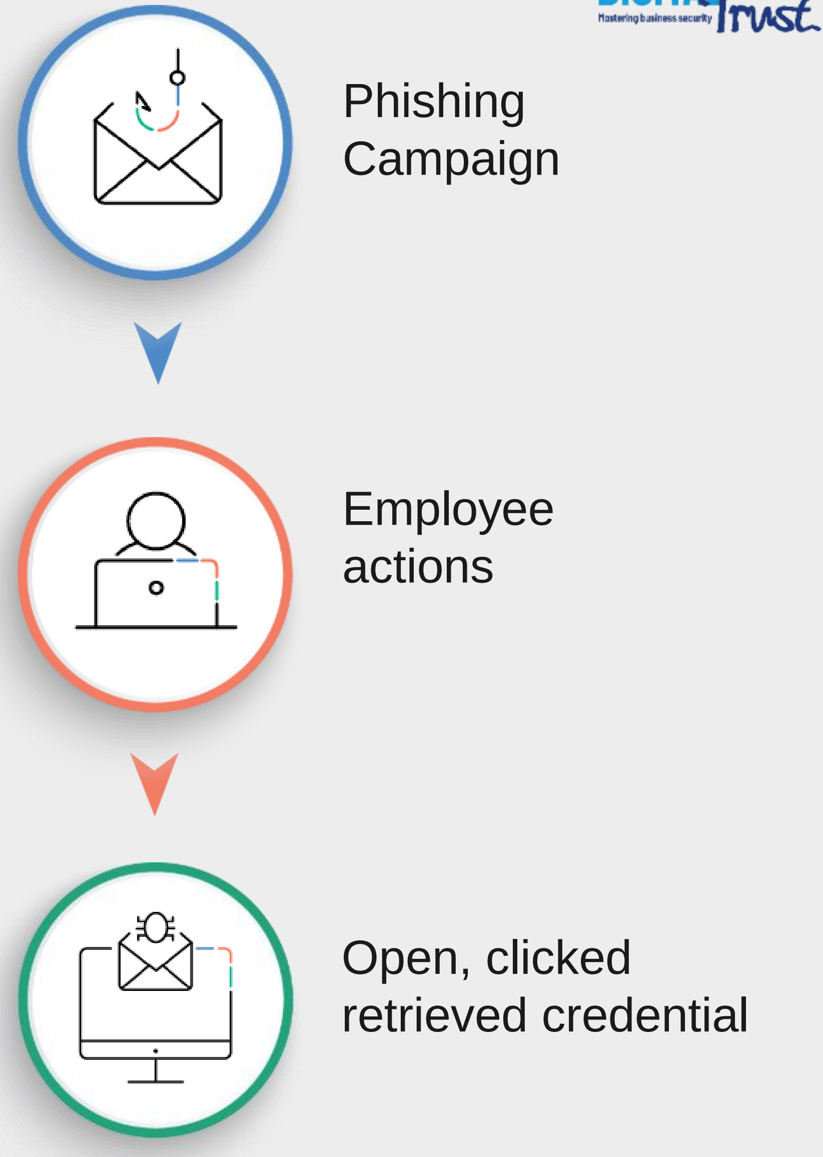
Web Attacks

Web Application Firewall

Web application

PHISHING AWARENESS

- All the resources available to run and manage a phishing campaign:
  - Types of phishing campaigns - Link to landing page or login Page, attachment etc.
  - Craft email from template
    Office, Social, File Sharing, Work Related etc.
  - Malicious attachments are synthetic - Do Not cause damage
- Find out who opened the email, clicked on the links or entered credentials
- Assess employee security awareness to focus on employees that require more education and monitoring than others



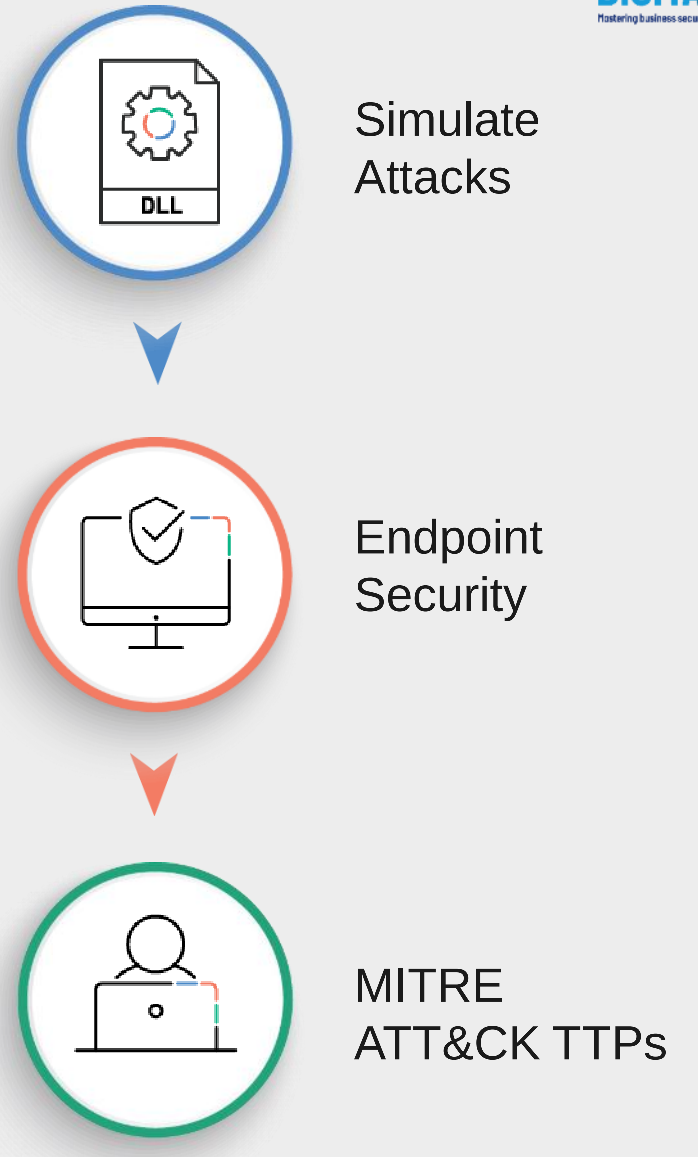
Phishing Campaign

Employee actions

Open, clicked retrieved credential

ENDPOINT SECURITY

- Validate your endpoint security against a comprehensive set of out-of-the-box tests and create your own
  - Behavior based: Trojan, Ransomware, Worm (lateral movement) and other techniques
  - Signature based (Drop to disk)
  - Red-team function to create and run custom commands mapped to the MITRE ATT&CK framework: Credential access, C&C, lateral movement, privilege escalation, execution, exfiltration, discovery and defense evasion
- Extensively tests the effectiveness of endpoint security and provides clear remediation guidance to fix misconfigurations and close security gaps



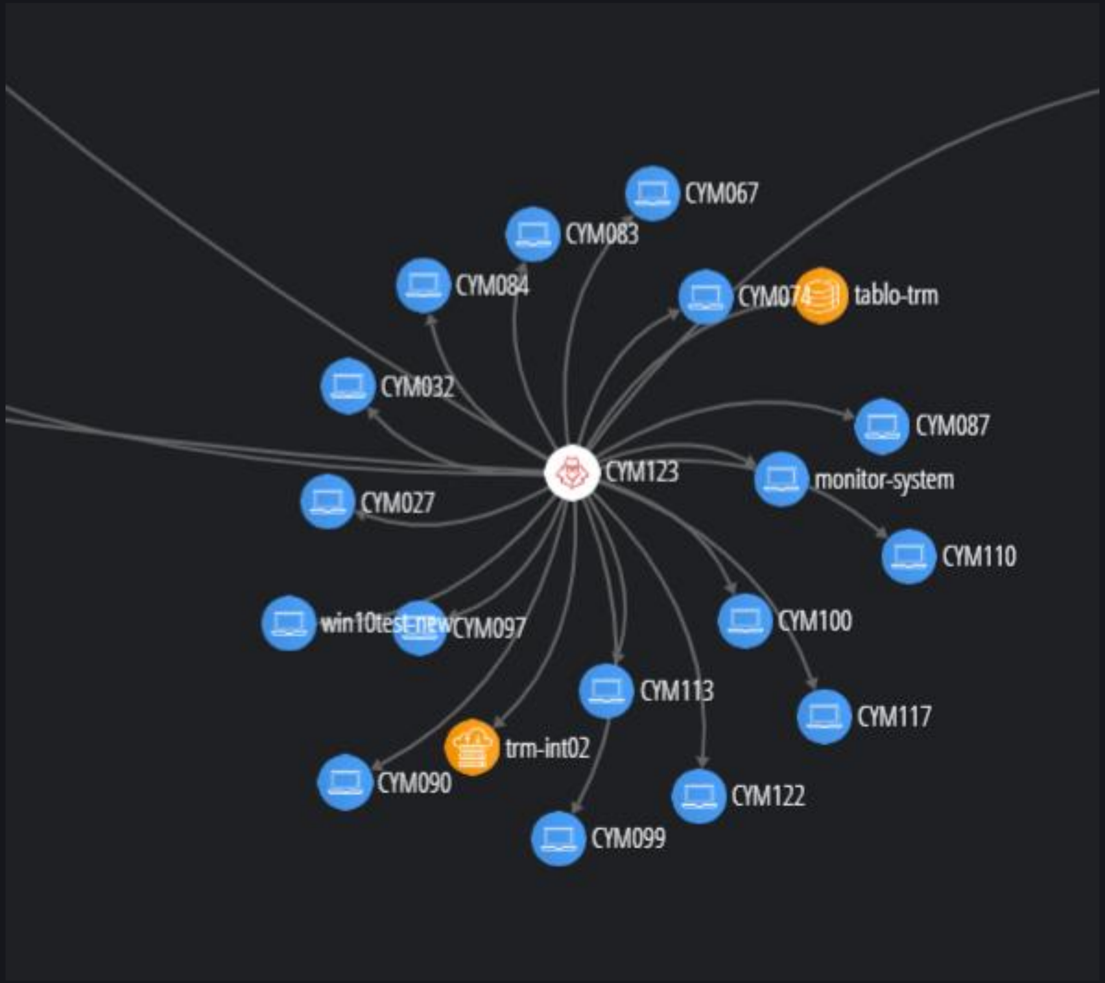
Simulate Attacks

Endpoint Security

MITRE ATT&CK TTPs

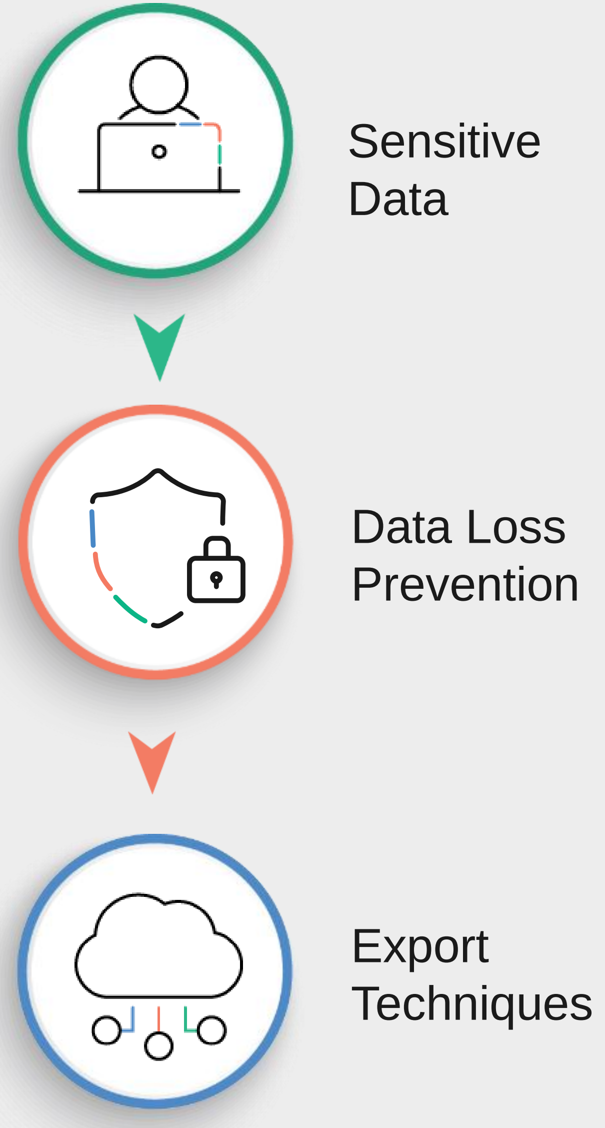
LATERAL MOVEMENT

- Network infrastructure configuration
  - Launched from a single agent
  - Employs “living of the land” techniques. for example, credentials and token harvesting
  - Propagates using network and system services such as WMI, SMB and file shares
  - Safe to use in production environments, does not exploit vulnerabilities
  - Visualize network propagation and discovered assets
  - Analysis to describe and guide you to remediate infrastructure misconfigurations and weaknesses



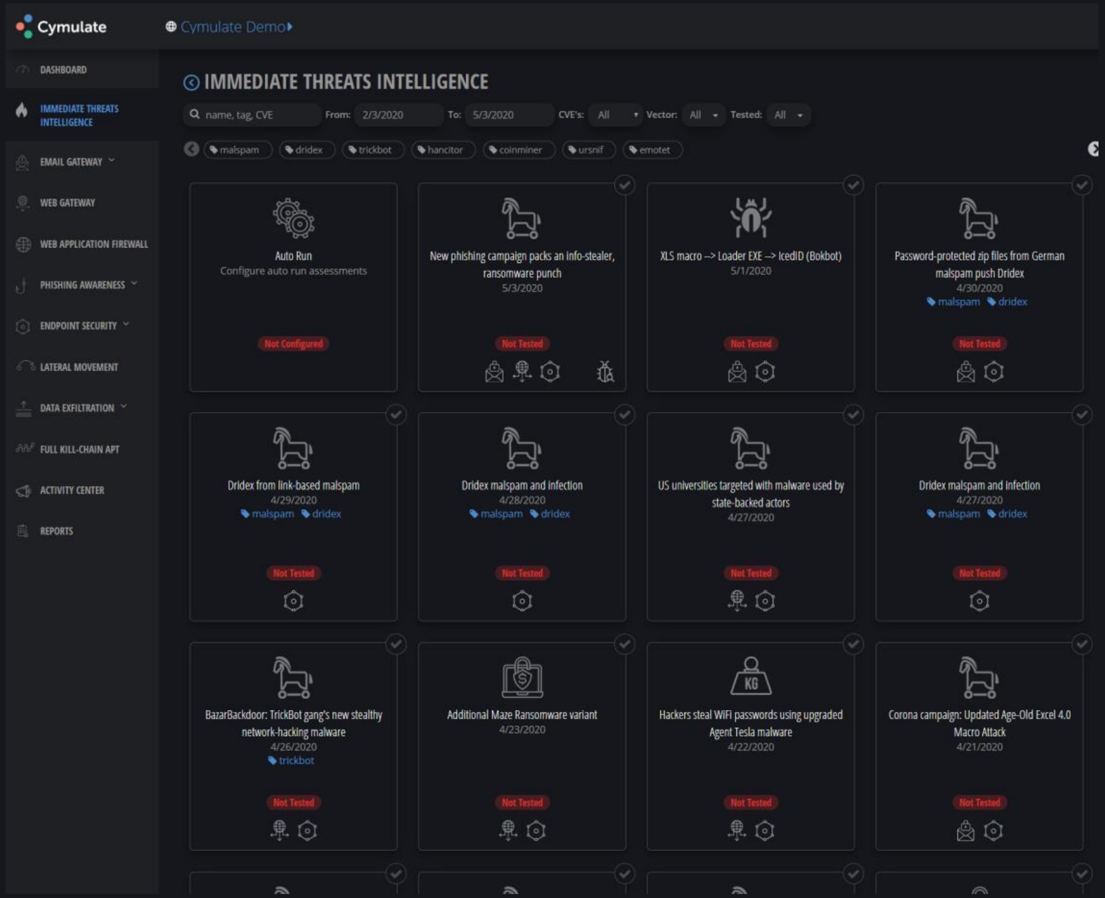
DATA EXFILTRATION

- Test security controls that prevent data loss against an extensive test scenarios based on:
  - Synthetic sensitive data:-
    - Regulatory
    - Company confidential
    - Create & import your own
  - Packaged in different file types: e.g., Rich media and office
  - Exported using different techniques: e.g., cloud services, email and network protocols
- Provides clear remediation guidance to fix misconfigurations and close security gaps



IMMEDIATE THREATS

- Cymulate security researchers explore for new threats 24X7
- Newly discovered threats updated daily to the platform
- Enables you to replay attacks in one click or automatically upon availability
- Provides immediate assessment of your protection against new threats found in the wild: email, web and endpoint security controls
- Provides threat related CVE’s and mitigation guidelines within minutes



IMMEDIATE THREATS INTELLIGENCE

name, tag, CVE From: 2/3/2020 To: 5/3/2020 CVE's: All Vector: All Tested: All

Auto Run
Configure auto run assessments
Not Configured

New phishing campaign packs an info-stealer, ransomware punch
5/3/2020
Not Tested

XLS macro --> Loader EXE --> IcedID (Bokbot)
5/1/2020
Not Tested

Password-protected zip files from German malspam push Dridex
4/30/2020
malspam dridex
Not Tested

Dridex from link-based malspam
4/29/2020
malspam dridex
Not Tested

Dridex malspam and infection
4/28/2020
malspam dridex
Not Tested

US universities targeted with malware used by state-backed actors
4/27/2020
Not Tested

Dridex malspam and infection
4/27/2020
malspam dridex
Not Tested

BazarBackdoor: TrickBot gang's new stealthy network-hacking malware
4/26/2020
trickbot
Not Tested

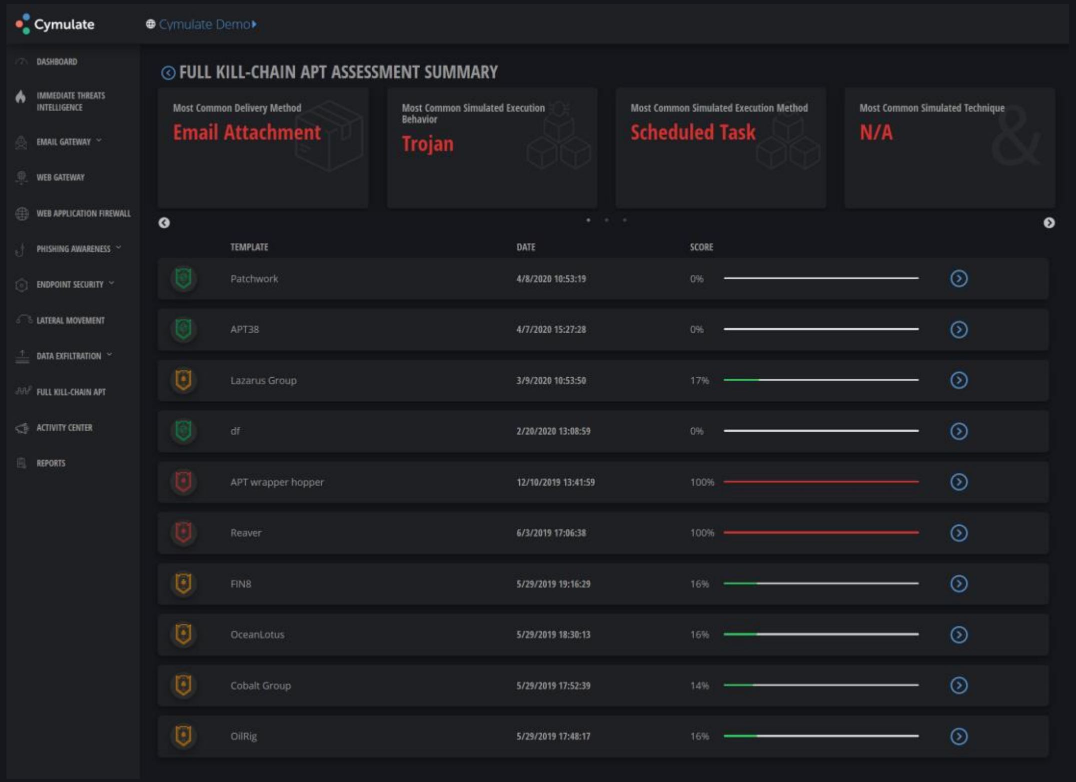
Additional Maze Ransomware variant
4/23/2020
Not Tested

Hackers steal WiFi passwords using upgraded Agent Tesla malware
4/22/2020
Not Tested

Corona campaign: Updated Age-Old Excel 4.0 Macro Attack
4/21/2020
Not Tested

FULL KILL CHAIN APT

- Simulates the entire flow of an APT in one go
- Choice of Agent and Agentless Mode
- Agentless mode starts with phishing email for a true-to-life simulation
- Offers selection of APT attack templates based on high-profile APT groups: Lazarus, APT38, FIN8, Cobalt etc.
- Customise your own APT based on MITRE ATT&CK techniques
- Provides clear remediation guidance to fix misconfigurations and close security gaps



FULL KILL-CHAIN APT ASSESSMENT SUMMARY

Most Common Delivery Method
Email Attachment

Most Common Simulated Execution Behavior
Trojan

Most Common Simulated Execution Method
Scheduled Task

Most Common Simulated Technique
N/A

TEMPLATE	DATE	SCORE
Patchwork	4/8/2020 10:53:19	0%
APT38	4/7/2020 15:27:28	0%
Lazarus Group	3/9/2020 10:53:50	17%
df	2/20/2020 13:08:59	0%
APT wrapper hopper	12/10/2019 13:41:59	100%
Reaver	6/3/2019 17:06:38	100%
FIN8	5/29/2019 19:16:29	16%
OceanLotus	5/29/2019 18:30:13	16%
Cobalt Group	5/29/2019 17:52:39	14%
OilRig	5/29/2019 17:48:17	16%

PURPLE TEAMING

- For organisations with in-house PT/RT skills:
  - Leverage and scale expert resources
  - Create custom policy and compliance assessments
  - Automate and expand security assurance activities and regression testing
- Additional benefits for security service providers
  - Create, automate and operationalize customer-specific testing scenarios
  - Differentiate service offerings with own brand of automated assessments
  - Address mid-market price sensitivity
  - Assess SIEM Detection and SOC Response inline with NIST 800-53 / MITRE ATT&CK

MITRE ATT&CK FRAMEWORK

01 Cymulate threat modelling uses the building blocks of the MITRE ATT&CK™ framework

02 Simulations of the latest techniques utilized by current cyberthreats, updated daily

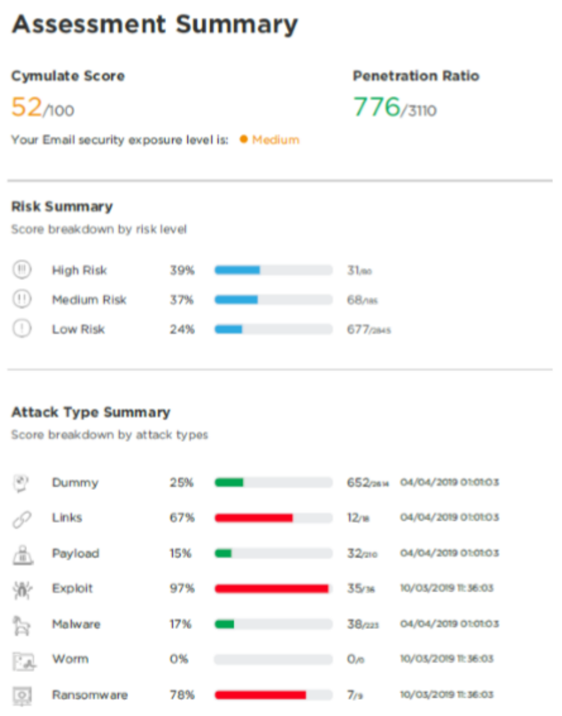
03 Full attack kill chain coverage, emulating the flow of events of a multi-vector attack

04 Create scenarios from the library of commands, create your own commands and upload your own samples

05 Automation of ATT&CK™ based simulations, so you can run them daily, weekly, or whenever

06 Remediation and mitigation guidelines mapped to ATT&CK™ for additional context

REPORTING



Assessment Summary

Cymulate Score

52/100

Your Email security exposure level is: ● Medium

Penetration Ratio

776/3110

Risk Summary

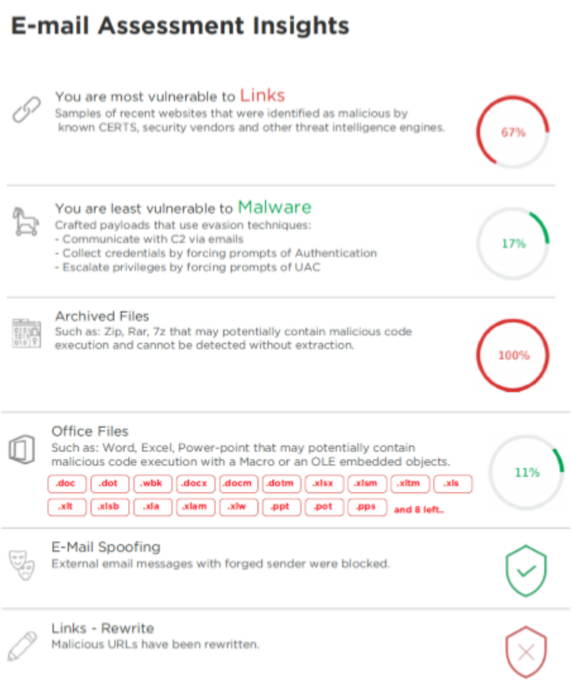
Score breakdown by risk level

High Risk	39%		31/80
Medium Risk	37%		68/185
Low Risk	24%		677/2845

Attack Type Summary

Score breakdown by attack types

Dummy	25%		652/2614	04/04/2019 01:01:03
Links	67%		12/18	04/04/2019 01:01:03
Payload	15%		32/210	04/04/2019 01:01:03
Exploit	97%		35/36	10/03/2019 11:36:03
Malware	17%		38/223	04/04/2019 01:01:03
Worm	0%		0/0	10/03/2019 11:36:03
Ransomware	78%		7/9	10/03/2019 11:36:03



E-mail Assessment Insights

You are most vulnerable to Links
Samples of recent websites that were identified as malicious by known CERTS, security vendors and other threat intelligence engines.
67%

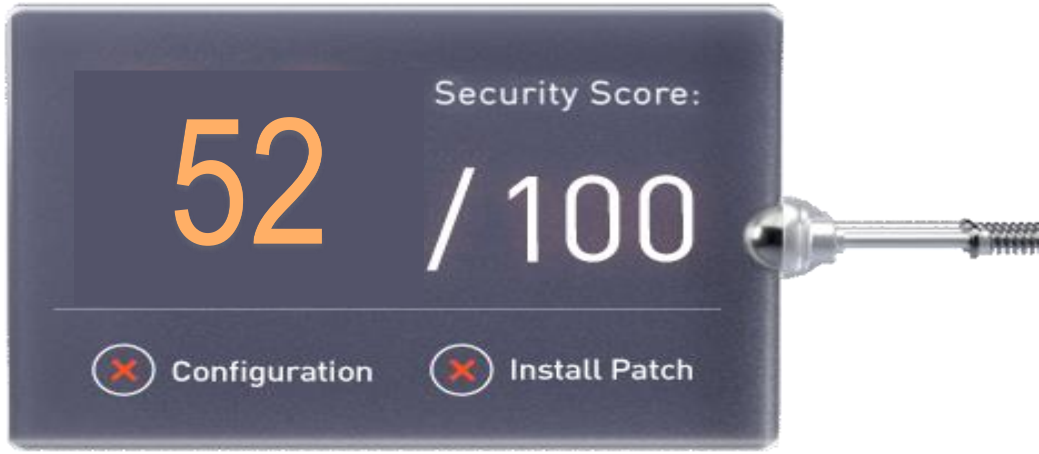
You are least vulnerable to Malware
Crafted payloads that use evasion techniques:
- Communicate with C2 via emails
- Collect credentials by forcing prompts of Authentication
- Escalate privileges by forcing prompts of UAC
17%

Archived Files
Such as: Zip, Rar, 7z that may potentially contain malicious code execution and cannot be detected without extraction.
100%

Office Files
Such as: Word, Excel, Power-point that may potentially contain malicious code execution with a Macro or an OLE embedded objects.
.doc .dot .wbk .docx .docm .dotm .xlsx .xlsm .xltm .xls .xlt .xlsb .xla .xlam .xlw .ppt .pot .pps and 8 left..
11%

E-Mail Spoofing
External email messages with forged sender were blocked.
✓

Links - Rewrite
Malicious URLs have been rewritten.
✗



Variables

- Impact of attack
- Probability of encounter
- Infection success rate

BENEFITS

FOR CUSTOMERS TAKING THE AUTOMATED BREACH SIMULATION ASSESSMENTS

Better understand risk: Simulate attacks to understand security resiliency with no impact on the IT environment

Validate controls: Ensure that changes and updates to the Network don’t create security gaps

Enhance Security: Multiply ROI and Cyber Defence investment by understanding how to maximise the value of existing security products

Derive insight: Understand how and where to invest to optimise security spend

Commercial flexibility: Computacenter’s Breach Simulation service is quick and easy to enable with flexible pricing options to meet different customer requirements.

WHY COMPUTACENTER

Better understand risk: Simulate attacks to understand your security resiliency with no impact on your environment

Validate controls: Ensure that changes and updates to your Network don't create security gaps

Enhance Security: Multiply ROI and Cyber Defence by understanding how to maximise the value of your existing security products

Derive insight: Understand how and where to invest to optimise your security spend

Commercial flexibility: Computacenter's Breach Simulation service is quick and easy to enable with pricing options that work best for your business.

DIGITAL Trust.

Mastering business security

PROTECTING DATA & INFORMATION

ACHIEVING IT COMPLIANCE & MANAGING IT RISK

SECURING WORKPLACES & PEOPLE

DEFENDING TECHNOLOGY PLATFORMS