cyberange

DATA SHEET

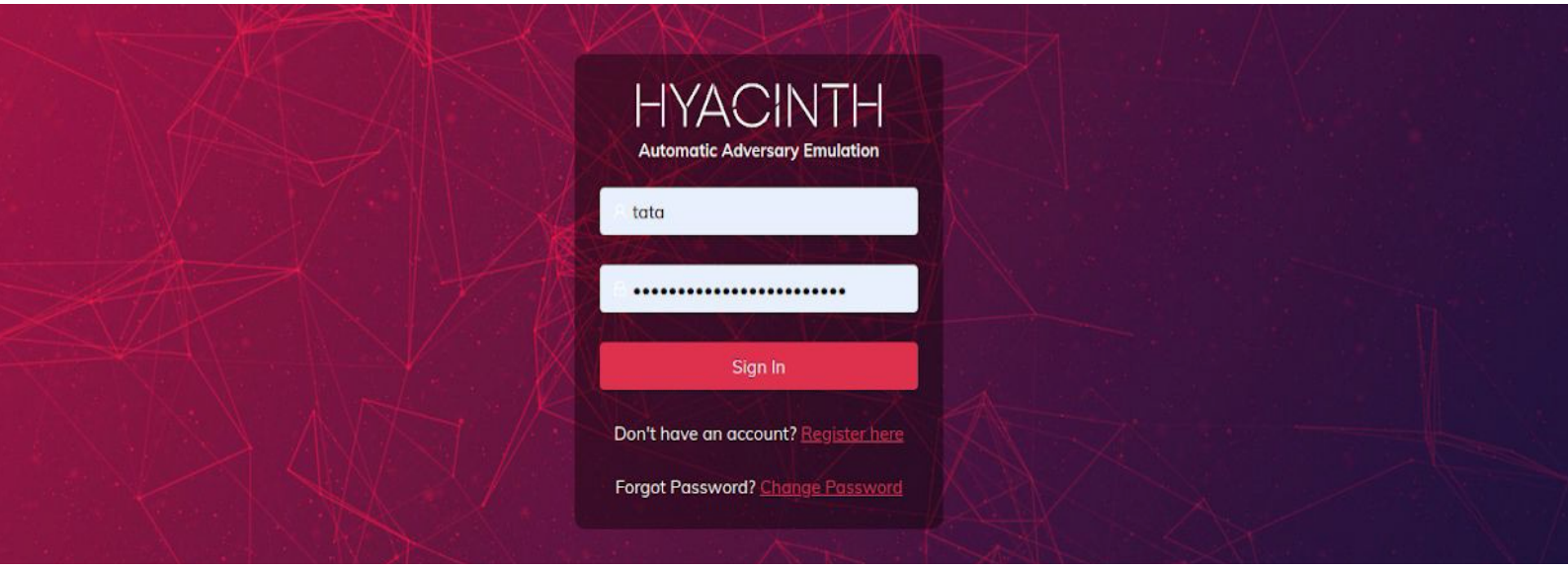
Cyberange ® Hyacinth Adversary Attack Emulation

Evaluate the maturity of your security operations center

Emulate sophisticated real-world cyberattacks and test the readiness and maturity of your Security Operations Center without side effects.

Hyacinth solves the challenges faced by organizations in detecting new and advanced cyberattacks from various threat actors. From Ransomware Attack Simulation, advanced persistent threat (APT) groups, and malicious behavior of employees, Hyacinth can emulate complex cyberattacks, making it genuinely robust and an advanced tool to test the maturity of your SOC environment during a cyber crisis.

120+ Advanced Attack Emulation Based on MITRE ATT&CK
Cloud based, Get started instantly!



Key Features:

- Completely automatic
- Decision Engine to choose exploits
- Cross-Platform
- Modern exploits as seen in the wild
- Run-on single or multiple machines
- Customizable to setup your scenarios
- Ability to upload custom exploit scripts
- Seamless updates and support
- Detailed logs and reports

Compared to traditional Adversary Emulation tools, Hyacinth doesn't complicate what you need to run and how. Instead, it's a ***fire-and-check the logs*** tool. Hyacinth's modular architecture allows it to support any platform and can run customizable attack simulations efficiently. Choose your exploits, Run and watch how Hyacinth quickly runs the exploits leaving traces which your SIEM system should detect.

Benefits:

- Audit and Improve your technologies deployed for Cyber Threat Detection and Response Capabilities.
- Improve SOPs and Response Times against real-time sophisticated cyber-attacks.
- Conduct cyber security drills in your organization.
- Conduct SOC Maturity Assessments

Capabilities:

Emulate attacks that can test the security effectiveness of various devices:

- Desktops
- Servers
- Supported Embedded devices
- Routers
- Switches
- Firewall
- UTM
- IDS
- SIEM / Log Analysis tools
- IoT / SCADA

Use Cases:

Ransomware attack Emulation and Protection

Hyacinth will emulate real-life ransomware attacks with advanced features such as polymorphism and AV detection and bypass without actually causing any harm to the system files. The emulation executes by targeting a single directory or group of files explicitly created for this exercise. Unlike other traditional traffic-based simulations, hyacinth deploys actual malware without any side effects, ensuring that the technologies and processes implemented are up to the mark and gaps are identified immediately and improved.

Detecting Insider Fraud or Lateral Movement Attacks

Suppose a malicious insider or an attacker is already inside and is trying to perform a lateral movement attack or gain privileges maliciously; he will have to perform specific actions and run some commands or payloads to achieve this. Traditional logging mechanisms and detection tools may not be able to detect these kinds of attacks. Hyacinth can emulate such attacks to check if the security tools are sufficient to detect and respond to such attacks.

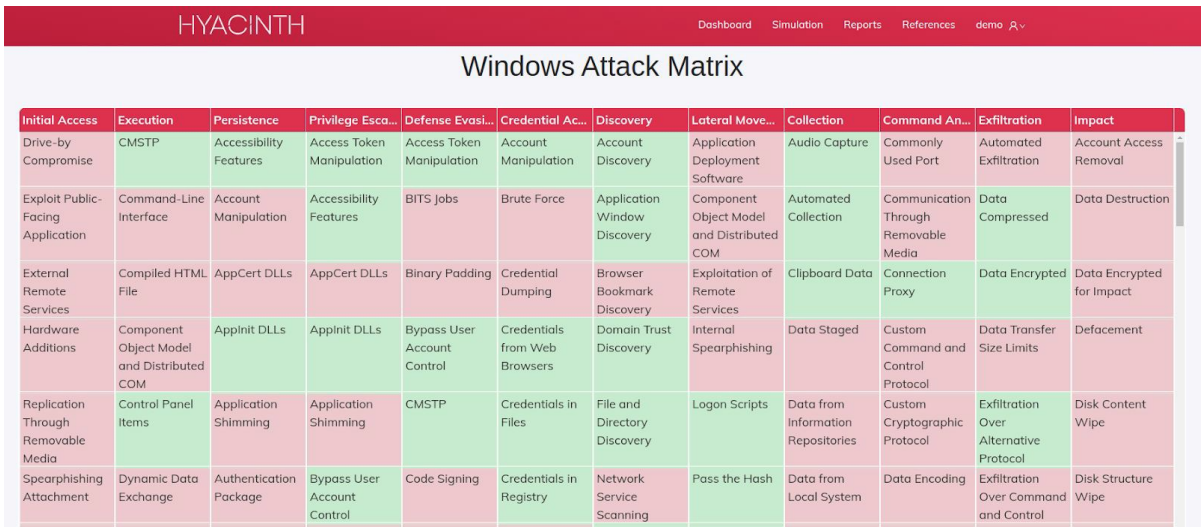
Malicious bots or C&C

Hyacinth can emulate malicious communication to known and unknown C&C networks. A good Threat intel and SIEM alerting mechanism should be able to detect such communication and report it.

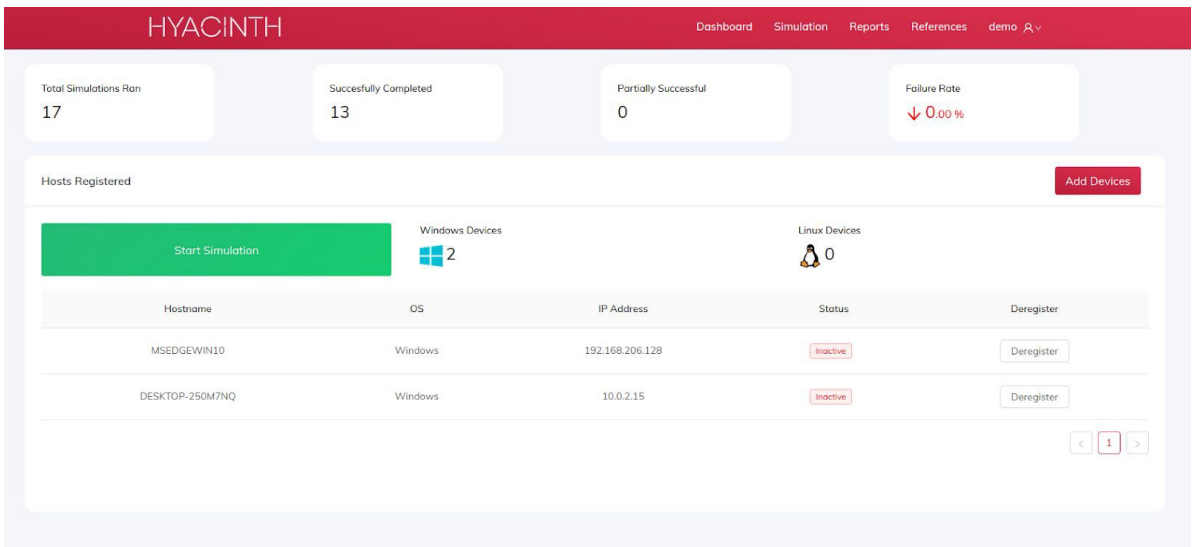
cyberange

Multiple Tactics and Techniques supported:

Initial Access	Execution	Persistence	Privilege Esca...	Defense Evasi...	Credential Ac...	Discovery	Lateral Move...	Collection	Command An...	Exfiltration	Impact
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data Staged	Custom Command and Control	Data Transfer Size Limits	Defacement
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Share Discovery	Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative	Disk Content Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Network Sniffing	SSH Hijacking	Data from Local System	Data Encoding	Exfiltration Over Command and Control	Disk Structure Wipe
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network	Endpoint Denial of Service



Initial Access	Execution	Persistence	Privilege Esca...	Defense Evasi...	Credential Ac...	Discovery	Lateral Move...	Collection	Command An...	Exfiltration	Impact
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control	Disk Structure Wipe



cyberange

Technical Features - Supported Attack Techniques:

Execution (13 Techniques)

1. Local Job Scheduling
2. Trap
3. CMSTP
4. Control Panel Items
5. Execution through Module Load
6. MS-HTA
7. PowerShell
8. Rundll32
9. Scheduled Task
10. Service Execution
11. Signed Binary Proxy Execution
12. Windows Management Instrumentation
13. Windows Remote Management

Persistence (22 Techniques)

1. .bash_profile and .bashrc
2. Create Account
3. Hidden Files and Directories
4. Kernel Modules and Extensions
5. Local Job Scheduling
6. Trap
7. Accessibility Features
8. Account Manipulation
9. AppInit DLLs
10. Change Default File Association
11. Component Object Model Hijacking
12. Create Account
13. File System Permission Weakness
14. Hidden Files and Directories
15. Logon Scripts
16. Modify Existing Service
17. Netsh Helper DLL
18. New Service
19. Powershell Profile
20. Scheduled Task
21. Service Registry Permissions Weakness
22. Windows Management Instrumentation

Privilege Escalation (13 Techniques)

1. Exploitation for Privilege Escalation
2. Sudo
3. Sudo Caching
4. Access Token Manipulation
5. Accessibility Features
6. AppInit DLLs
7. Bypass User Account Control
8. File System Permissions Weakness
9. New Service
10. Parent PID Spoofing
11. Powershell Profile
12. Scheduled Task
13. Service Registry Permissions Weakness

Defense Evasion (34 Techniques)

1. Binary Padding
2. Clear Command History
3. Compile After Delivery
4. Connection Proxy
5. File and Directory Permission Modification
6. HISTCONTROL
7. Hidden Files and Directories
8. Indicator Removal on Host
9. Install Root Certificate
10. Masquerading
11. Obfuscated Files or Information
12. Timestomp
13. Access Token Manipulation
14. Bypass User Account Control
15. CMSTP
16. Component Object Model Hijacking
17. Connection Proxy
18. Control Panel Items
19. DLL Side-Loading

20. Disabling Security Tools
21. File and Directory Permission Modification
22. Hidden Files and Directories
23. Hidden Window
24. Indicator Removal on Host
25. Indirect Command Execution
26. Masquerading
27. Modify Registry
28. MS-HTA
29. Network Share Connection Removal
30. Obfuscated Files or Information
31. Parent PID Spoofing
32. Process Hollowing
33. Rootkit
34. Rundll32

Credential Access (11 Techniques)

1. Bash History
2. Credentials from Web Browsers
3. Credentials in Files
4. Input Capture
5. Private Keys
6. Account Manipulation
7. Brute Force
8. Credentials in Registry
9. Input Prompt
10. Kerberoasting
11. Private Keys

Discovery (19 Techniques)

1. Account Discovery
2. Browser Bookmark Discovery
3. File and Directory Discovery
4. Network Service Scanning
5. Remote System Discovery
6. System Information Discovery
7. System Network Configuration Discovery
8. System Network Connections Discovery
9. System Owner/User Discovery
10. Application Window Discovery
11. Domain Trust Discovery
12. Network Share Discovery
13. Permission Group Discovery
14. Query Registry
15. Remote System Discovery
16. Security Software Discovery
17. Software Discovery
18. System Service Discovery
19. System Time Discovery

Lateral Movement (4 Techniques)

1. Remote File Copy
2. Logon Scripts
3. Pass the Hash
4. Windows Remote Management

Collection (7 Techniques)

1. Data from Information Repositories
2. Input Capture
3. Screen Capture
4. Audio Capture
5. Automated Collection
6. Clipboard Data
7. Email Collection

Command And Control (5 Techniques)

1. Connection Proxy
2. Remote Access Tools
3. Remote File Copy
4. Uncommonly Used Port
5. Web Service

Exfiltration (4 Techniques)

1. Data Compressed
2. Data Encrypted
3. Data Transfer Size Limits
4. Execution Over Alternative Protocol

SPECIFICATIONS | ON-PREMISE & PRIVATE CLOUD

Component	On-Prem/Private Cloud	Cyberange Cloud
Virtual Cyberange Labs Server	6 Core, 64 GB RAM, 1TB RAID 10, 2 NIC 10gbps cards	Auto-scalable
Attack Simulations	Unlimited	Unlimited
Attack Techniques Supported	32	32
Fully Automated attacks	Yes	Yes
Custom scenario development	Yes	Yes
Custom attack scripts	Yes	No
Supported End Points	Windows, Linux, MacOS	Windows, Linux, MacOS
Detailed Reports	Yes	Yes
White-label	Yes	No
Scenario Updates under AMC	Quarterly	No AMC Required, updates provided real-time

www.cyberange.io