

# *Hack Dich doch einfach selbst!*



David Berger  
Regional Manager  
David@pentera.io

# The Pentera Approach

## Vulnerability Management? Exploit Management!!

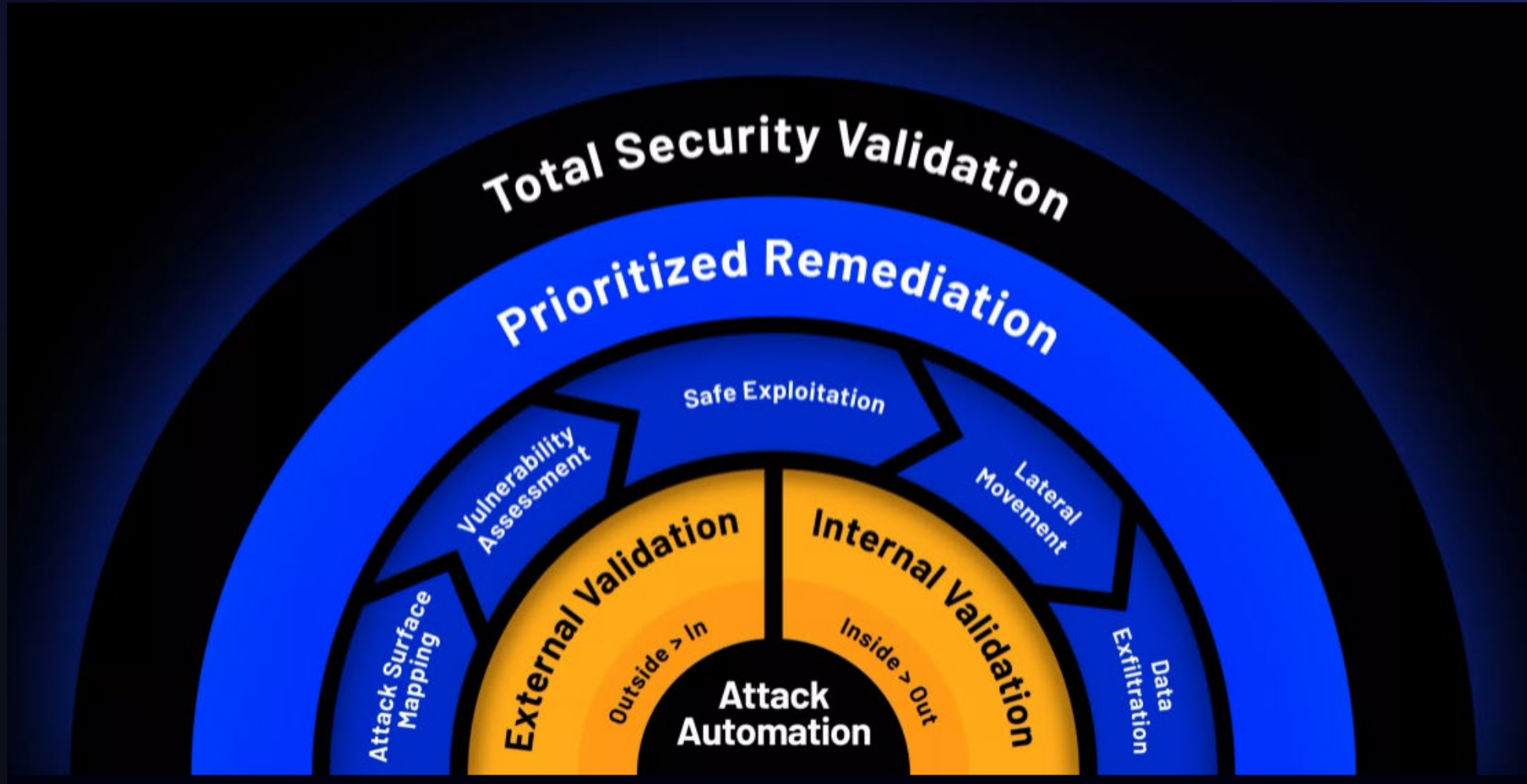


- Windows/Linux/MAC
- Microsoft Exchange
- CITRIX
- CISCO
- Office 365
- Azure/AWS
- Virtual Machine
- ....

- Remote Code Execution (RCE)
- Privilege Escalation (PE)
- Command & Control
- Lateral Movement
- Collection
- ...

- Common Vulnerabilities & Exposures (CVE)
- Misconfigurations
- Broken access control
- Injections
- Authentication bypass
- ...

# Die Sicht des Angreifers



Und nun... Use Cases

# MITRE ATT&CK™ Compliant

## Validation Attacks Mapped to the MITRE ATT&CK framework

**Pentera** | RansomwareReady

### Executive Summary

Type: REvil Ransomware Emulation | Time: Aug 25 2021 16:12 - Aug 25 2021 16:31

**Resilience Score**  
67%

Name: RansomwareReady  
Description: RansomwareReady

IP Ranges: 6 | Targeted Hosts / Candidates: 60% (3 of 5)

Based on AV/EDR bypass of all targeted hosts

**Resilience Score over Last 8 Runs**

Achievements: 4 Critical of 34 | AV / EDR Bypass: 1 Hosts | Targeted Hosts: 3 Hosts | Data Exfiltration to: Not configured

**Action Success Rate: 100% (276 of 276)**

Payload Launch	100%
File Enumeration	100%
Process Manipulation	0%
Encryption	100%
Data Exfiltration	0%
Host Modification	100%

**MITRE | ATT&CK** | Total Patterns: 861 | Most Common Technique: Defense Evasion / Indicator Removal on Host

Candidates - Live Hosts found to be suitable for reconnaissance emulation. May require user approval to execute the attack.  
Targeted Hosts - Hosts selected against the reconnaissance emulation but often following automatic user approval.

**Pentera** | Overview | Vulnerabilities | Attack Map | Hosts | Users | Actions Log | **MITRE** | Footprints | Report | Details & Input | Run

### MITRE ATT&CK Matrix for Enterprise

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning T1595	Valid Accounts T1078	Exploitation for Client Execution T1209			Indicator Removal on Host T1070	Unsecured Credentials T1552	Remote System Discovery T1018	Exploitation of Remote Services T1210	Data from Network Shared Drive T1039	Application Layer Protocol T1071	Automated Exfiltration T1020	
Scanning IP Blocks T1595.001	Cloud Accounts T1078.004	Command and Scripting Interpreter T1059			File Deletion T1070.004	Credentials In Files T1552.001	Network Service Scanning T1048	Remote Services T1021	Data from Local System T1005	Web Protocols T1071.001		
Vulnerability Scanning T1595.002	Domain Accounts T1078.002	Unix Shell T1059.004				Steal or Forge Kerberos Tickets T1558	Cloud Service Discovery T1026	Windows Remote Management T1021.006		File Transfer Protocols T1071.002		
Gather Victim Network Information T1590		Windows Management Instrumentation T1047				Kerberoasting T1558.003	System Information Discovery T1082	SMB/Windows Admin Shares T1021.002		Standard Non-Application Layer Protocol T1095		
DNS T1590.002		System Services T1569				AS-REP Roasting T1558.004	Network Share Discovery T1135	Remote Desktop Protocol T1021.001				
		Service Execution T1569.002				Brute Force T1110	File and Directory Discovery T1083	Distributed Component Object Model T1021.003				
						Password Guessing T1110.001	System Owner/User Discovery T1033	Taint Shared Content T1085				
						Forced Authentication T1187	Permission Groups Discovery T1069					
						Credential Dumping T1003	Domain Groups T1069.002					

# Watchdog



## Top # Vulnerabilities

Pentera handpicked the most significant vulnerabilities. See which vulnerabilities were discovered and exploited in your environment.

Severity	Vulnerability	Found on Targets	Exploited	Result
10	Confiker (MS08-067)(CVE-2008-4250)	10 of 200 (5%)	5 of 10 (50%)	Found
10	ZeroLogon (CVE-2020-1472)	0 of 200 (0%)	0 of 0 (0%)	Not Found
9.8	Citrix ADC (CVE-2019-19781)	0 of 200 (0%)	0 of 0 (0%)	Not Found
9.8	Citrix ADC directory traversal (CVE-2019-19781)	10 of 200 (5%)	5 of 10 (50%)	Found
9.8	Fortinet auth bypass (CVE-2022-40684)	10 of 200 (5%)	5 of 10 (50%)	Found
9.8	Fortinet VPN (CVE-2018-13379)	0 of 200 (0%)	0 of 0 (0%)	Not Found
9.8	Oracle WebLogic RCE (CVE-2020-14882)	10 of 200 (5%)	5 of 10 (50%)	Found
9.8	Proxylogon Post-auth arbitrary file write RCE (CVE-2021-27065)	0 of 200 (0%)	0 of 0 (0%)	Not Found
9.8	Spring4Shell (CVE-2022-22965)	10 of 200 (5%)	5 of 10 (50%)	Found
9.8	PulseSecure (CVE-2019-11510)	10 of 200 (5%)	5 of 10 (50%)	Found
9.8	VMWare vCenter - File Upload Vulnerability - RCE (CVE-2021-22005)	0 of 200 (0%)	0 of 0 (0%)	Not Found
9.3	EternalBlue (MS17-010) (CVE-2017-0144)	1 of 200 (<1%)	0 of 1 (0%)	Found
9.9	Bits Service PE (CVE-2020-0787)	10 of 200 (5%)	5 of 10 (50%)	Found
8.8	PrintNightmare (CVE-2021-34527)	0 of 200 (0%)	0 of 0 (0%)	Not Found
8.8	ProxyNotShell Microsoft Exchange SSRF (CVE-2022-41040)	10 of 200 (5%)	5 of 10 (50%)	Found
8.8	SAM name impersonation (CVE-2021-42278)	0 of 200 (0%)	0 of 0 (0%)	Not Found
8.2	Windows Win32k PE (CVE-2018-8120)	10 of 200 (5%)	5 of 10 (50%)	Found
8	ProxyNotShell Microsoft Exchange RCE (CVE-2022-41082)	10 of 200 (5%)	5 of 10 (50%)	Found
7.8	Bits Service PE (CVE-2020-0787)	0 of 200 (0%)	0 of 0 (0%)	Not Found
7.8	Dirty Pipe LPE (CVE-2022-0847)	0 of 200 (0%)	0 of 0 (0%)	Not Found

# SecVal Standardization



# Security Stack Bake Off

EDR | NDR | EPP | SIEM | WAF | FW | SOAR | ...

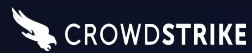


Carbon Black.

SOPHOS



KASPERSKY<sup>®</sup>



FORTINET<sup>®</sup>

Forcepoint



# Red Teamer's best friend



# Audits, Due Diligence and M&A



# SOC Detection / SLA Testing



# Ransomware Resilience



# User Credential Strength

PASSWORD:  
123456

# Vulnerability Prioritization In the era of Talent Shortage



# Pentera 1-day Proof-of-Value

*Wer hat schon mehr Zeit als einen Tag?*

## Security Validation POV

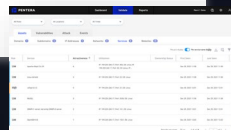
Agreement on POV & scheduling.

Only domain name required

## Know your security readiness

### Learn about your total attack surface

- Internal & External
- Known & Unknown
- Exploitable Vulnerabilities & Exposures



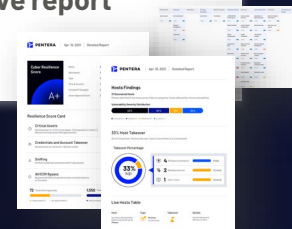
### Validate your security program

- Controls efficacy insights
- Testing scope
- Safe TTP Exploitation



### Analyze and report

- Remediation prioritization
- Root vulnerabilities
- Possible breach impact
- **Executive report**



Demo time!



Thank You.

June 2024

David Berger – Enterprise Account Manager

0151 – 221 22 22 0

David@Pentera.io