EMR Security

Presented by
Mike Pinch

November, 2019
Table of Contents

1 Industry Threats

2 Assessing Your EMR Security Program

3 Recommendations
My Background

- **Director at Security Risk Advisors**
- **Other Experience**
  - Chief Information Security Officer – URMC 2012-2018
  - Chief Technology Officer – UR, Palladian Health
  - Medical Device Manufacturer CISO
  - PricewaterhouseCoopers
The Current State

• EMRs are the crown jewels of HDOs today, and often don’t receive dedicated, special attention from cyber security

• Penetration testing often shows not just access to the EMR, but it is often the easiest way to tunnel into the organization and go much deeper

• Basic controls, low hanging fruit, not often implemented
Industry Threats
Threats - Ransomware

- **Significant healthcare uptick again in 2019**
  - Predominantly Windows based systems
  - Workstations, Windows Servers, Windows Databases, Medical Databases

- **First-Ever Statistics on Data Breach Effects on Clinical Care**
  - 2019 Vanderbilt Study Showed the Following:
    - Hospitals that had data breaches showed 36 additional deaths per 10,000 heart attacks
Trends in EMR Security

- Citrix/Virtualization isn’t patched
- Citrix/Virtualization breakout attack preventions aren’t implemented
- Rudimentary alerting of session breakout or tool misuse isn’t in place or integrated into SIEM
- Incident response workflows are not mature to handle clinical and patient safety incidents
Trends in EMR Security

- Privileged access management is weak or absent
- Data warehousing and reporting is over provisioned and under monitored
- Many organizations still aren’t running AV/EDR tools on the EMR
- Multi-Factor Authentication is still inconsistently in place
Quantifying Your Security Readiness
Metrics

• **Hygiene Metrics**
  • How well are your processes and protections configured to protect against compromise? Patches, Vulnerabilities, AV Coverage, Firewalling, etc.

• **Hyperbole Metrics (bad)**
  • Noise that says nothing about your real world efficacy
    • Ex: We blocked 3 million attacks last month!

• **Defense Success Metrics (New!)**
  • How well will your system stand up to and respond to actual attacks
Metrics Takeaways

- **Hyperbole Metrics Bad**
  - At best drown out meaningful metrics, at worst unintentionally misleading

- **Hygiene Good**
  - Preparation against attack

- **Defense Success Metrics Good**
  - Resiliency against attack

Let's Dive Into the Good!
EMR Security Hygiene
The EMR Security Program Controls, “Honeycomb”, diagram is a collection of processes and technical controls that should be implemented to enhance the security of the EMR application. This diagram was created to represent a mature EMR security program for organizations seeking to improve the maturity level of their program.

Each of the controls in this diagram will be evaluated against objective criteria and scored accordingly in subsequent slides. Additional honeycomb visuals will be presented to indicate the current state of each of these tiles with the goal of enabling management to prioritize investments to further protect the EMR environment.
Requiring multifactor authentication (MFA) to access EMR and perform privileged activity within the application will prevent an individual from performing unauthorized activity using compromised credentials.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Controls Required</th>
<th>Meets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Initial</td>
<td>Multifactor authentication is required for e-prescribing of controlled substances within EMR.</td>
<td>✓</td>
</tr>
<tr>
<td>2 - Baseline</td>
<td>Multifactor authentication required for all remote system access to EMR.</td>
<td>✓</td>
</tr>
<tr>
<td>3 - Par</td>
<td>Multifactor authentication required for all third-party connections into the network.</td>
<td>✓</td>
</tr>
<tr>
<td>4 - Leader</td>
<td>Multifactor authentication is used for privileged access and administrative functions within hyperspace.</td>
<td></td>
</tr>
<tr>
<td>5 - Innovator</td>
<td>Risk-based authentication is used for all system access.</td>
<td></td>
</tr>
</tbody>
</table>

Observed Strengths & Recommendations

**Observed Strengths**
- MFA is required for remote VPN access, Hypervisor’s EPCS function, and the MDM platform

**Recommendations**
- Information Security should leverage MFA capabilities in the upcoming EMR upgrade for related applications and systems such as MyChart, Haiku and Canto
- Information Security should implement MFA for systems that impact the security of the EMR application such as Active Directory
Effective Hyperspace breakout protections are critical to preventing misuse of the application and reduce the likelihood of an attacker being able to access underlying Epic infrastructure.

### Observed Strengths & Recommendations

#### Observed Strengths

<table>
<thead>
<tr>
<th>Rating</th>
<th>Controls Required</th>
<th>Meets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Initial</td>
<td>The organization is unaware of hyperspace breakout attacks and the possible root risks associated with them.</td>
<td>✔</td>
</tr>
<tr>
<td>2 - Baseline</td>
<td>The organization has attempted to reduce the likelihood of hyperspace breakouts by setting certain configurations such as sticky keys / accessibility mode to restrict breakouts.</td>
<td>☐</td>
</tr>
<tr>
<td>3 - Par</td>
<td>The hyperspace environment has been assessed to eliminate unnecessary underlying software that could provide an attacker the ability to move laterally inside the organization, such as PowerShell, RDP, F12 Developer Tools etc.</td>
<td>☐</td>
</tr>
<tr>
<td>4 - Leader</td>
<td>The hyperspace environment has been configured to alert upon a successful hyperspace breakout or use of unauthorized software.</td>
<td>☐</td>
</tr>
<tr>
<td>5 - Innovator</td>
<td>A formal incident response playbook has been defined and tested to identify a successful hyperspace breakout and respond by ending the user session, locking their account, and preserving forensic information from the image to aid in the investigation. Notifications should include a review by clinical leadership to determine if there was any patient risk by the actions of the attacker.</td>
<td>☐</td>
</tr>
</tbody>
</table>
How to Design

• Combine
  • Common Security Frameworks (NIST, CIS etc)
  • EMR Infrastructure Inventory
  • Threat Modeling (STRIDE / DREAD)
  • Your technology stack
  • Business Outcomes
  • A maturity framework
    • CMMI
    • Bad, Good, Best
Examining the Full Infrastructure

• Most testers see EMRs as just the clinicians app... but as you know, its so much more than that:
  • Financials
  • Patient Portal
  • Patient Mobile App
  • FHIR Interface
  • API Server
  • Printers
  • Database

• Data Warehouse
• Business Intelligence
• Share Drives
• Domain Administrator Access
• Host OS
• Downtime PCs
• Workstations on Wheels
EMR Security Resiliency
Why EMR Pen Testing?

- We already have a penetration test performed almost every year.... What’s the difference?
  - Focus – In a traditional penetration test, you have thousands of assets, typically all with their own vulnerabilities. Penetration testing typically finds one (or a couple) ways in, but rarely has the time to focus on specific systems.
  - Knowledge – Penetration testing an EMR typically requires deeper knowledge and experience with specific tools, as well as better understanding of clinical workflows to demonstrate effects of compromise.
  - Risk – Quite simply, your EMR is likely the center of your clinical Universe. Organizations spend 8, 9, and even 10 figures to implement them, The **impact** factor of risk is extremely **high**
  - Weakness – EMR manufacturers off the shelf security configurations are often very weak and trivially easy to bypass, combined with the fact that they are often exposed on the internet. The **likelihood** factor of risk is extremely **high**
Establishing Safeguards

- Safe penetration testing is mandatory
- Ask about fragile and weak assets
  - Interface engines, for example, can often create performance or integrity issues if under hard scans or attacks
  - This inquiry phase may actually create your first ‘tabletop’ findings
- Identify methods for safely testing a production system
  - Identify and get provisioned access for both production and a non-production system
  - Non-prod needs to be most recent mirror of production and have common security controls employed in application and supporting infrastructure wherever possible
  - Testing performed in production until application access is obtained
  - Shift to non-production instance to demonstrate further attacks; when successful attacks are made, review with management before doing in production
Introducing Purple Teams

• Purple Teams is an open-book-exam process that prioritizes and shows quantifiable improvements in defenses over time.

- Vulnerability Assessment
- Reconnaissance
- Penetration Testing
- Social Engineering
- Data Exfiltration

- Threat Intelligence
- Incident Response
- Forensics
- Active Monitoring
- Process Improvement
How we make Purple
What is Purple Team Testing?

Live, cooperative attack and defense events that focus on collaborative improvement and optimization of prevention, detection, and response

Red team plans an attack that exercises different phases of the kill chain

Red team executes attack while announcing / sharing their activities with blue team

Blue team must prevent / detect / respond

▶ Inability to meet expected outcome creates an action or task to remediate
Aligning with MITRE ATT&CK

- The MITRE ATT&CK Framework is a collection of granular attacker tactics, catalogued in a variety of useful fashions

Enterprise Tactics

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA001</td>
<td>Initial Access</td>
<td>The adversary is trying to get into your network.</td>
</tr>
<tr>
<td>TA002</td>
<td>Execution</td>
<td>The adversary is trying to run malicious code.</td>
</tr>
<tr>
<td>TA003</td>
<td>Persistence</td>
<td>The adversary is trying to maintain their foothold.</td>
</tr>
<tr>
<td>TA004</td>
<td>Privilege Escalation</td>
<td>The adversary is trying to gain higher-level permissions.</td>
</tr>
<tr>
<td>TA005</td>
<td>Defense Evasion</td>
<td>The adversary is trying to avoid being detected.</td>
</tr>
<tr>
<td>TA006</td>
<td>Credential Access</td>
<td>The adversary is trying to steal account names and passwords.</td>
</tr>
<tr>
<td>TA007</td>
<td>Discovery</td>
<td>The adversary is trying to figure out your environment.</td>
</tr>
<tr>
<td>TA008</td>
<td>Lateral Movement</td>
<td>The adversary is trying to move through your environment.</td>
</tr>
<tr>
<td>TA009</td>
<td>Collection</td>
<td>The adversary is trying to gather data of interest to their goal.</td>
</tr>
<tr>
<td>TA011</td>
<td>Command and Control</td>
<td>The adversary is trying to communicate with compromised systems to control them.</td>
</tr>
<tr>
<td>TA010</td>
<td>Exfiltration</td>
<td>The adversary is trying to steal data.</td>
</tr>
<tr>
<td>TA040</td>
<td>Impact</td>
<td>The adversary is trying to manipulate, interrupt, or destroy your systems and data.</td>
</tr>
</tbody>
</table>

ID: T1003
Tactic: Credential Access
Platform: Windows, Linux, macOS
Permissions Required: Administrator, SYSTEM, root
Data Sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters
Contributors: Vincent Le Tou, Ed Williams, Trustwave, SpiderLabs
Version: 1.1

Credential Dumping

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
MITRE Usage

- ATT&CK Framework provides 100s of technical tactics that can be tested to show your overall resilience to attacks
- Tactics can be sorted a number of different ways, including the actual bad guys....

Deep Panda

Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. The intrusion into healthcare company Anthem has been attributed to Deep Panda. This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. Some analysts track Deep Panda and APT11 as the same group, but it is unclear if open source information is the same.

Associated Group Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shell Crew</td>
<td></td>
</tr>
<tr>
<td>WebMasters</td>
<td></td>
</tr>
<tr>
<td>KungFu Kittens</td>
<td></td>
</tr>
<tr>
<td>PinkPanther</td>
<td></td>
</tr>
<tr>
<td>Black Vine</td>
<td></td>
</tr>
</tbody>
</table>

Techniques Used

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1015</td>
<td>Availability Features</td>
<td>Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1143</td>
<td>Hidden Window</td>
<td>Deep Panda has used the &quot;UbiDuck&quot; technique to remain PowerShell windows by setting the WindowsStyle parameter to hidden.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1066</td>
<td>Indicator Removal from Tools</td>
<td>Deep Panda has updated and modified its malware, resulting in different hash values that evade detection.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1066</td>
<td>PowerShell</td>
<td>Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.</td>
</tr>
</tbody>
</table>
Running Purple Teams

• **Start small, simple**
  - ICS Cert Advisory
  - Email Phish
  - Wireless Attack
  - Data Exfiltration – cloud storage
  - Data Loss – Email
  - Virtual Currency Mining
  - Password Spray Attack
  - Permissions Change
  - Excessive Internal Logins

• **VECTR Purple Team Platform for Growth and Metrics**
Recommendations
Tabletop Exercises

- Tabletop exercises (TTX) are some of the best exercises to simulate events and get better at soft skills.
- Focus on small, relevant scenarios.
- Start “left of boom”, early stages of attack to think through communication and escalation.
- Take notes, make improvements.
Backup Security

- Your most critical security control for ransomware

- If your backup systems run on Windows and are bound to your domain; be very afraid!

- Conduct dedicated hardening projects; multi-factor auth, configuration change alerts, consider removing remote logons

- Don’t disregard the value of tape/offline backups
HIPAA Risk Analysis

- You NEED to do this every year

- Don’t just focus on assessing controls

- Include
  - ePHI Inventory
  - Mapping your controls to HIPAA
  - How you address “addressable” controls
  - Risk quantification (impact * likelihood)
  - Current Industry Threats
  - Risk Management Plan
Multi-Factor Authentication

- You NEED this everywhere....

- EVERY external facing authentication source
  - VPN
  - EMR
  - Email

- For everyone, no exceptions
Privileged Access Management

- Nearly every successful attack campaign compromises domain administrator credentials
- Make local administrator password one-time use & strong with MS LAPS (free)
- Make one time use passwords for domain admin accounts, use privileged account management tools ($)
- 2 Factor Authentication on servers is a red-herring – there are other ways in!
Summary

• We’ve turned a corner and can now correlate patient safety and security
• Consider a dedicated focus to customize markers and metrics around your EMR program
  • Communicate at the board level, show progress and growth
• Dedicated Pen Testing is great, Purple is better
  • DIY can be highly effective to get started
• Drop metrics that don’t matter
• Focus on the most critical items
  • Multifactor Authentication
  • Privileged Access Management
  • Tabletop Exercises
Questions?

Mike.Pinch@SecurityRiskAdvisors.com
Resources

• Purple Team Platform – https://vectr.io
• DIY Red Teaming - https://atomicredteam.io/