Engaging with White Hat Hackers

Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council
Leader, I Am The Cavalry (.org)
Know your hacker
Survey

How many of you think you have adversaries actively targeting you?

What are some of the types of adversaries? Shout out names.
Nation State
Accident
Increasingly Willing
Professional
Increasingly capable
Hard to Distinguish
Ideological
Willingness
Capabilities
5kr1p7 K1dd13
Increasingly
I Am The Cavalry

Five Motivations of Security Researchers

https://iamthecavalry.org/motivations

Protect

Puzzle

Pride/Prestige

Profit/Payment

Protest/Patriot
Who engages hackers and why
“Security researchers... provide significant and measurable insight into the vulnerabilities associated with technology of all kinds.”

-Chris Wlaschin, ES&S
“Security researchers also assist government and businesses in protecting vital information and critical infrastructure assets important to our national security and democracy.”

-Chris Wlaschin, ES&S
“ES&S uses independent researchers to test its systems.”

-Chris Wlaschin, ES&S
800+ classes of technical cybersecurity failures

Each security researcher covers a subset
#We ♡ Hackers
Committed to working with researchers at the Biohacking Village at DEF CON

Launched January 29

Brands:
- FDA
- ThermoFisher Scientific
- GM
- Jeep
- Chrysler
- Dodge
- Ram
- Apple
- Great Seal of the State of Delaware
- Google
- Abbott
- Medtronic
- elektra labs
- Siemens
- United
DoD’s Vulnerability Disclosure Policy Results

- Total valid reports resolved: 2,837
- Participating hackers: 645+
- High or critical severity vulnerabilities: 100+

Hackers from 50 countries including: India, Great Britain, Pakistan, Philippines, Egypt, Russia, France, Australia and Canada
Dr. Marie Moe
Hacker
Pacemaker patient

https://www.youtube.com/watch?v=W1YWpVMpPi8
https://www.wired.com/2016/03/go-ahead-hackers-break-heart/
In 2018, Apple became the world’s first $1 Trillion company.
In 2019, Apple will spend around $1 Billion on security.
Last week, a 14-year-old reported a major security flaw in Apple’s products.
Vulnerabilities are inevitable.

Responses determine outcomes.
IT TAKES A VILLAGE: HOW HACKTIVITY CAN SAVE YOUR COMPANY

Atlantic Council

http://publications.atlanticcouncil.org/hacktivity/
Where/how to engage white hat hackers
An invaluable experience for understanding cybersecurity.

A lot friendlier than expected!

Huge perception gap. Hackers are a lot more friendly than we give them credit for.

Interested in learning and patient in teaching.

What Congressional and federal Agency visitors said about their trips to DEF CON
Engaging with White Hat Hackers

Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council
Leader, I Am The Cavalry (.org)
Additional Resources
Coordinated Vulnerability Disclosure
US Department of Commerce, NTIA Template

ISO/IEC 29147 Standard for Vulnerability Disclosure
https://www.iso.org/standard/45170.html

ISO/IEC 30111 Standard for Vulnerability Handling Processes
https://www.iso.org/standard/53231.html

National Governor’s Association

US Department of Justice
https://www.justice.gov/criminal-ccips/page/file/983996/download
### Procurement Guidance

<table>
<thead>
<tr>
<th><strong>4. System Information:</strong></th>
<th>Provides more granular information as to how the system is setup and managed within the Mayo Clinic environment.</th>
<th>Provide vendor documentation (i.e. Bill of Materials) for the bulletted items. Template provided.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- List of 3rd Party Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- List of Accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- List of Network Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- List of firewall rules (if applicable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Documentation of Security Capabilities/Configurations for System Hardening</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Scanning Requirements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>5. Vulnerability Assessment, including:</strong></th>
<th>Provides an in-depth vulnerability assessment, outstanding vulnerabilities and appropriate remediation plans and timelines to resolve the issues. This provides Mayo Clinic with appropriate information on risks that may be introduced into the patient care environment and allows for collaborative mitigation strategies to be detailed.</th>
<th>Complete a vulnerability assessment as detailed in the Vendor Assessment Book (pdf). Once testing is completed, complete the VA Statement of Methodology and document findings and remediation plans in a report. Example VA Statement of Methodology (pdf) and Vulnerability Assessment Template report provided.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Testing Results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Remediation Tracking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>6. Mayo Clinic Information Security Schedule</strong></th>
<th>Provides <strong>advanced copy</strong> of Mayo Clinic’s Information Security Schedule that Supply Chain Management will negotiate as part of the purchase contract or vendor agreements.</th>
<th>1. Ensure appropriate vendor internal staff receives Mayo’s Information Security Schedule for review. 2. Perform review and prepare any proposed redline items. 3. Provide a vendor contact to the Mayo proponent for the redlined ISS negotiation.</th>
</tr>
</thead>
</table>

[Link](https://www.mayoclinic.org/documents/medical-device-vendor-instructions/doc-20389647)
1. No default passwords
2. Coordinated vulnerability disclosure policy
3. Keep devices updated