Real-World Management of a Medical Device

Patrick Duncan
CBET
Integration Engineer, Clinical Engineering
Methodist Le Bonheur, Memphis

Shankar Somasundaram
CEO & Co-Founder
Asimily, Inc.

Webinar Overview

In this session, we will discuss the cybersecurity management of medical devices at Methodist Le Bonheur (MLH). We will outline the challenges faced in managing these devices, including vulnerability management, balancing costs and collaboration and coordination with Information Technology teams. Finally we will discuss future plans at MLH to improve medical device security posture and how organizations can remain current with industry trends.

About Asimily

- Asimily is a Venture backed company providing a connected device risk management solution focused on healthcare with provider customers across the nation

- Venture backed: lead investor is Engineering Capital, which is an influential investor in the Silicon Valley and co-invested by Plug and Play Ventures, ex-CEO of Symantec, ex-CEO of BlueCoat and others

- Asimily brings experts from healthcare technology management, cybersecurity, networking, and data analytics
  - Team members come with 5-20 years of experience each
  - Educational qualifications include Bachelors, Masters, and PhD from ivy leagues
  - Work experience from Symantec, RiskIQ, Spidercloud wireless, Tejas Networks, Qualcomm and others
  - Strong advisory council from experts like Steve Grimes, Axel Wirth, CISOs from provider organizations, ex-CEO of Symantec, Bluecoat, and others

- Asimily's solution solves for number of use cases around inventory, cyber-security and operational analytics and integrates with many systems like CMMS, SIEMs, Network Firewalls, NACs, Vulnerability Scanners and others

About Methodist Le Bonheur (MLH)

- 6 hospital system in the Memphis market with over 1600 licensed patient beds
- Providing both academic and community-based healthcare
- Methodist University Hospital is affiliated with the University of Tennessee Health Science Center as a teaching hospital
- Le Bonheur Hospital is a nationally recognized Children's Hospital
- Multiple Diagnostic Centers & Physician Practices

MLH Clinical Engineering Division

- General biomedical services (16 biomed technicians/engineers)
- Biomedical equipment specialist providing service on specialized biomedical equipment (7 biomed technicians/engineers)
- Imaging engineering department providing service on over 450 imaging devices in house, without service support contracts (15 imaging engineers)
- Surgical instrument service lab
- Clinical technology services - providing project management, medical device information technology services and medical device integration
- Capital equipment planning & acquisition department

Where MLH was at the beginning

- Had created a comprehensive list of their devices manually and had started the process of collecting IT parameters about the device
- Knew that vulnerabilities existed but didn’t have a good hold on what those vulnerabilities were and their priority
- Didn’t have much insight on whether something abnormal was happening in their network
- Had done a cost analysis on what it would take to collect the necessary data

Initial Cost Analysis – Manual Workload

Task	Equivalent Number of resources	Cost per resource	Total Cost
Collecting all the parameters, including Asset parameters	6	$90K/year	$540K/year
Collecting Vulnerabilities and Analytics of the collected Data And taking Action	Not clear how we would do it continuously	Expensive	High Cost but could not quantify
$540K + Analytics = Not Practical			

Above does not include other aspects like Vulnerability Exploit Analysis, Impact Analysis, Utilization tracking, Anomaly Detection, Policy Tracking, Remediation Actions based on Vulnerability Analysis
Considering the above, MLH decided that an automated way to solve many of the issues above was the right approach.

Challenges from the Manual Workload

- **Medical devices cannot be scanned like IT devices: Experimented with this in our labs**
  - Tested on four Draeger Physiological Monitors running on Simulators
  - Ran a series of Vulnerability scans , starting off from gentle to invasive
  - At some point, scan changed ECG gain on monitors, so they were all in asystole alarms

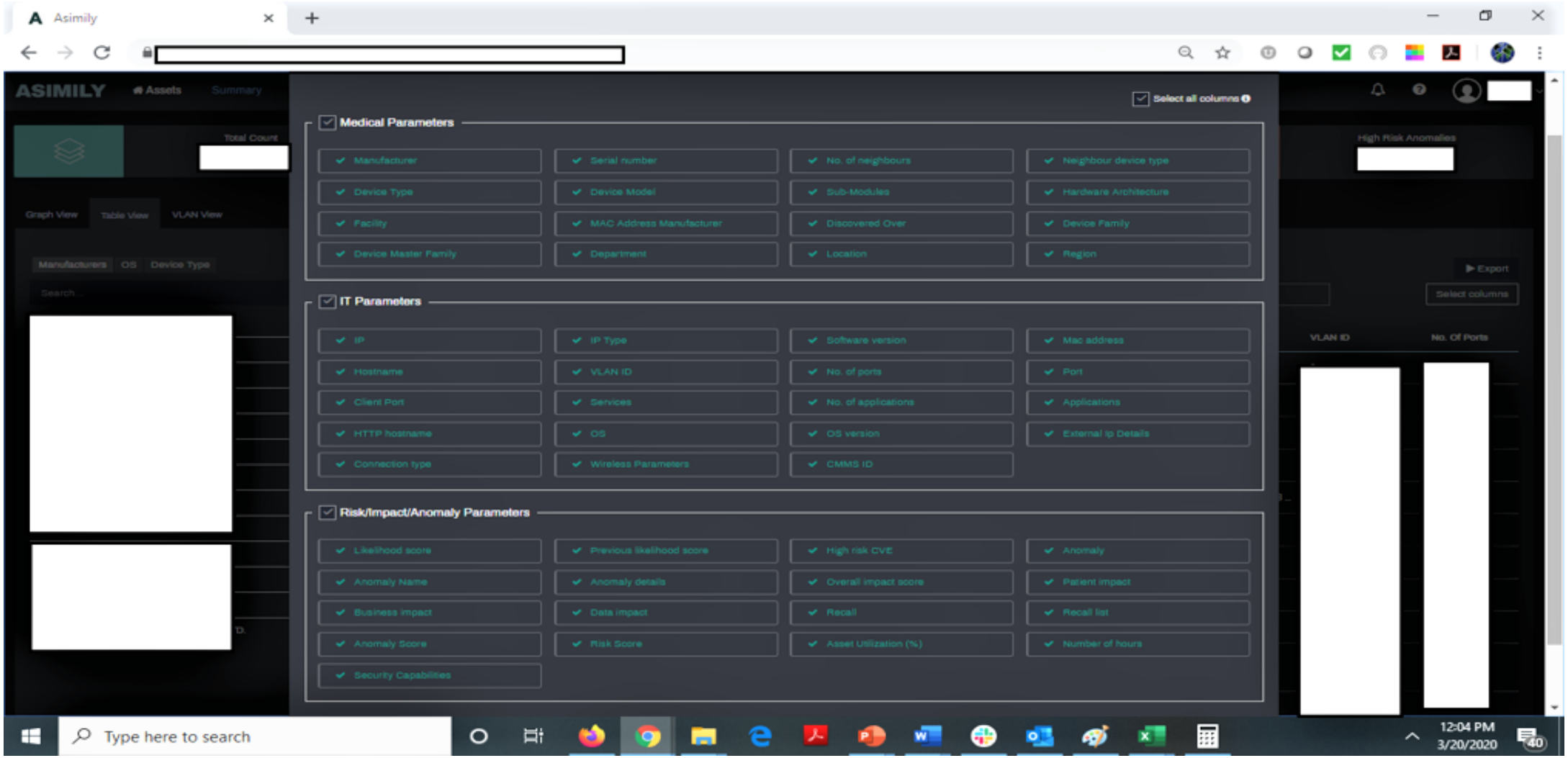
- **Medical devices are unique**
  - MLH looked at many solutions in the market and most of them looked like Network solutions that also happened to work with Medical devices
  - MLH wanted a solution that was specifically designed around medical devices

After evaluating many solutions, MLH chose Asimily for a variety of reasons (If you want more details on why we selected Asimily, please contact me offline)

Inventory Management

- MLH has deployed the Asimily appliance at each of its hospital sites
- All the data from different sites feed into the Asimily cloud where MLH has portal access
- Through this portal, MLH has a good measure of a variety of different inventory aspects:
  - *Number of network connected medical devices*
  - *Different parameters about the medical device like medical device parameters, IT parameters, cyber-security capabilities*
  - *How the devices are connected in the network*
  - *Where is the device transmitting data to, where they are reaching out*
  - *How vendors are accessing the devices*
- Inventory Management has also been offered to the IT team to track IoT devices as they also want to be familiar with the kind of device there might be on the network

Inventory Management

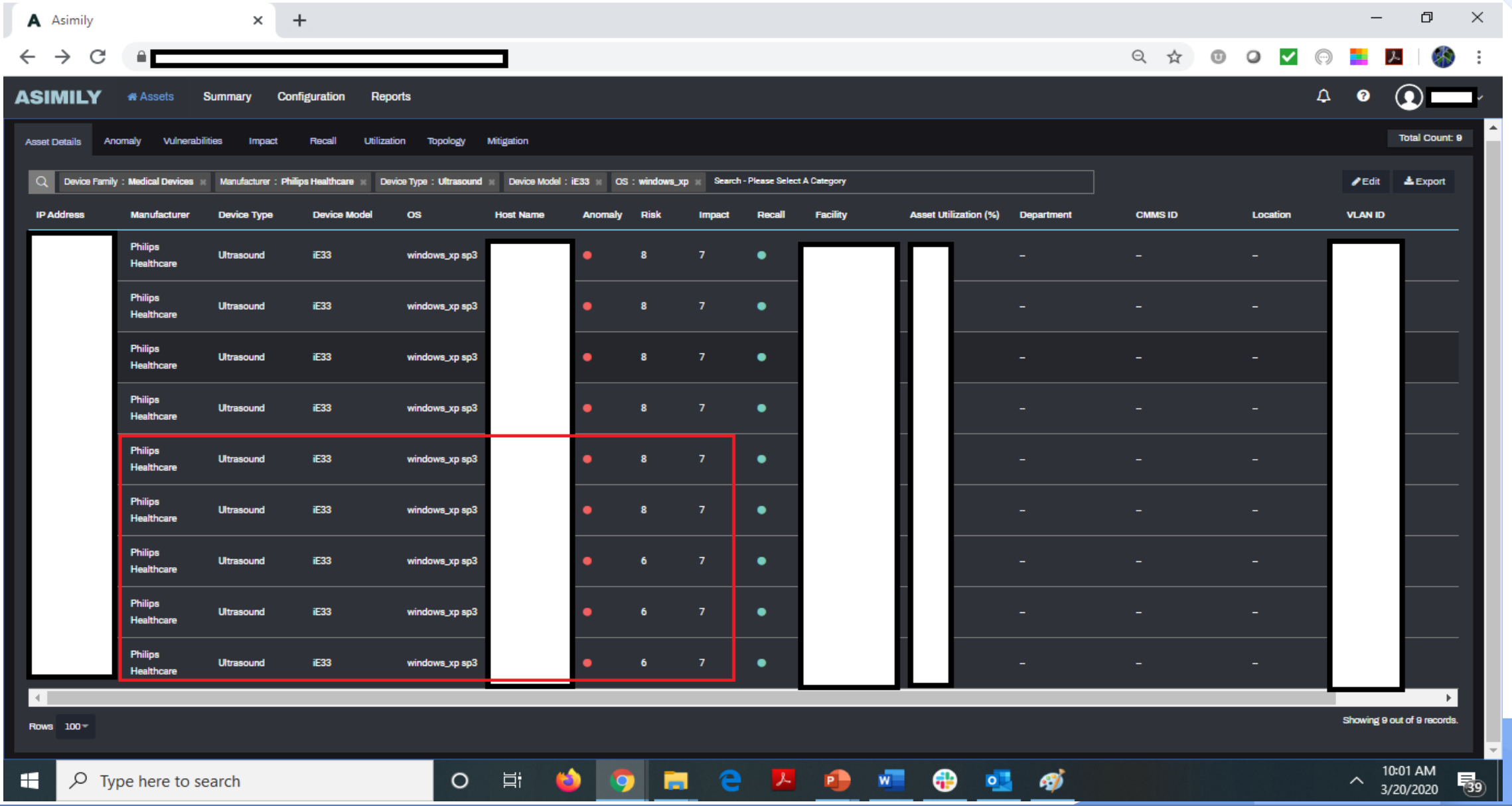


- Several parameters provided that is used to understand the device and track it

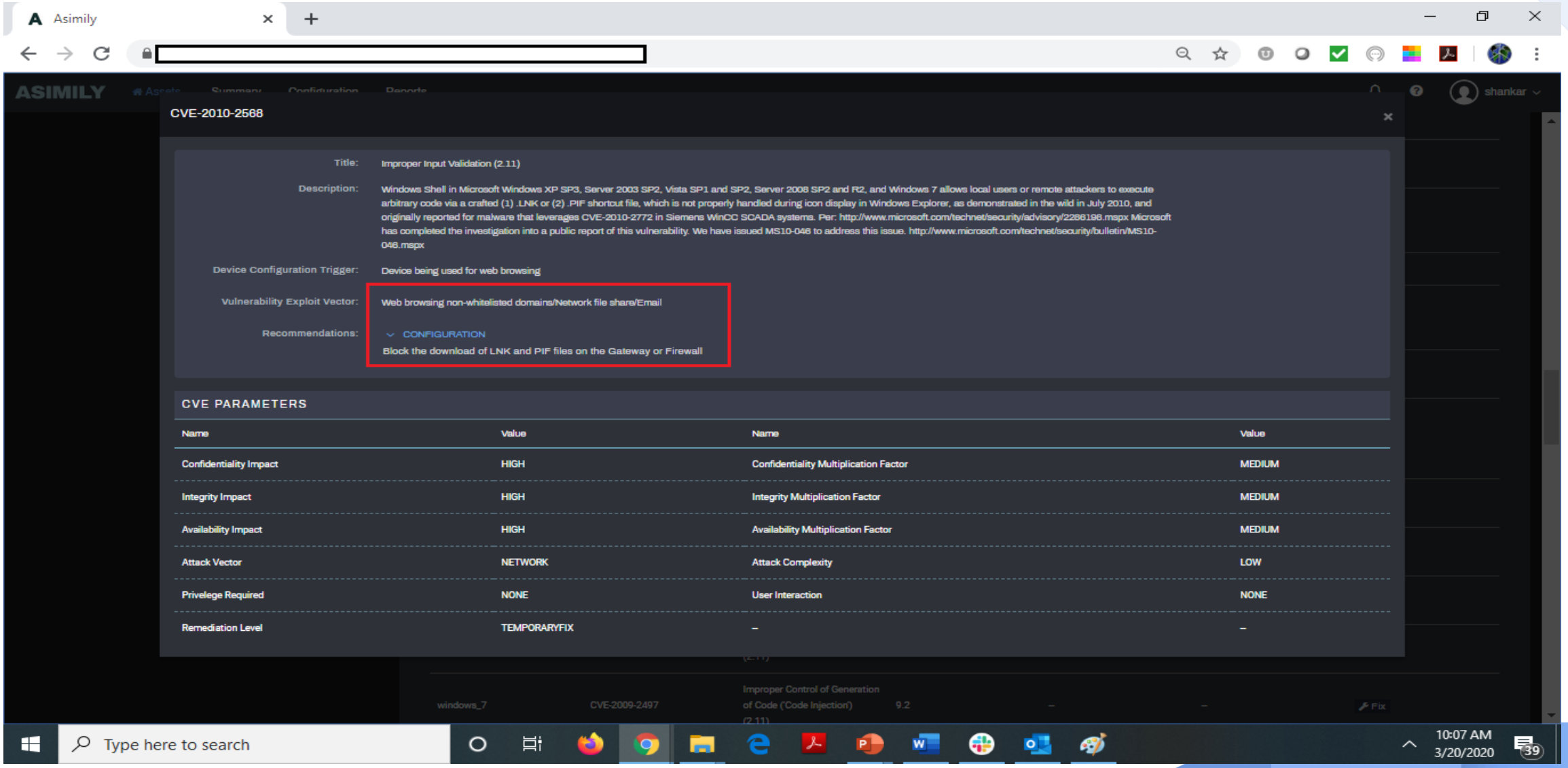
Vulnerability Management

- Not all devices have the same risk
- Even across devices with the same legacy operating system, risks could be different
- Whether an unpatched vulnerability affects a device is dependent on many factors:
  - *Exploitability of the vulnerability for that device in that environment*
  - *Impact of the vulnerability*
  - *How the device is connected*
  - *Security capabilities of the device*
  - *Any other mitigating security controls*
- Asimily takes all the other factors into account before deciding whether a vulnerability is exploitable and high impact and then if the vulnerability is high risk, high impact vulnerability, then provides a workaround

Same model, MFR., OS with different risk scores



Vulnerability Management – Workarounds



How MLH Address Vulnerabilities

- MLH is using a variety of techniques to address risks
  - **At Procurement**
    - Uses a process to address risk right at procurement. Currently driven by IT and will look to bring in more medical device context in the future
  - **Prioritization**
    - MLH is using the Asimily system to understand the priority for different vulnerabilities
  - **Patching**
    - Where possible, MLH is patching the device to ensure it has the latest software version and/or operating system
  - **Workarounds**
  - Where patches are not available, MLH is using workarounds to mitigate the risk
    - Some workarounds are widely known like turning on Network Level Authentication for RDP
    - In other cases, Asimily recommended workarounds are being used to mitigate the risks
    - Where workaround is not available, MLH has used One-Way firewalls

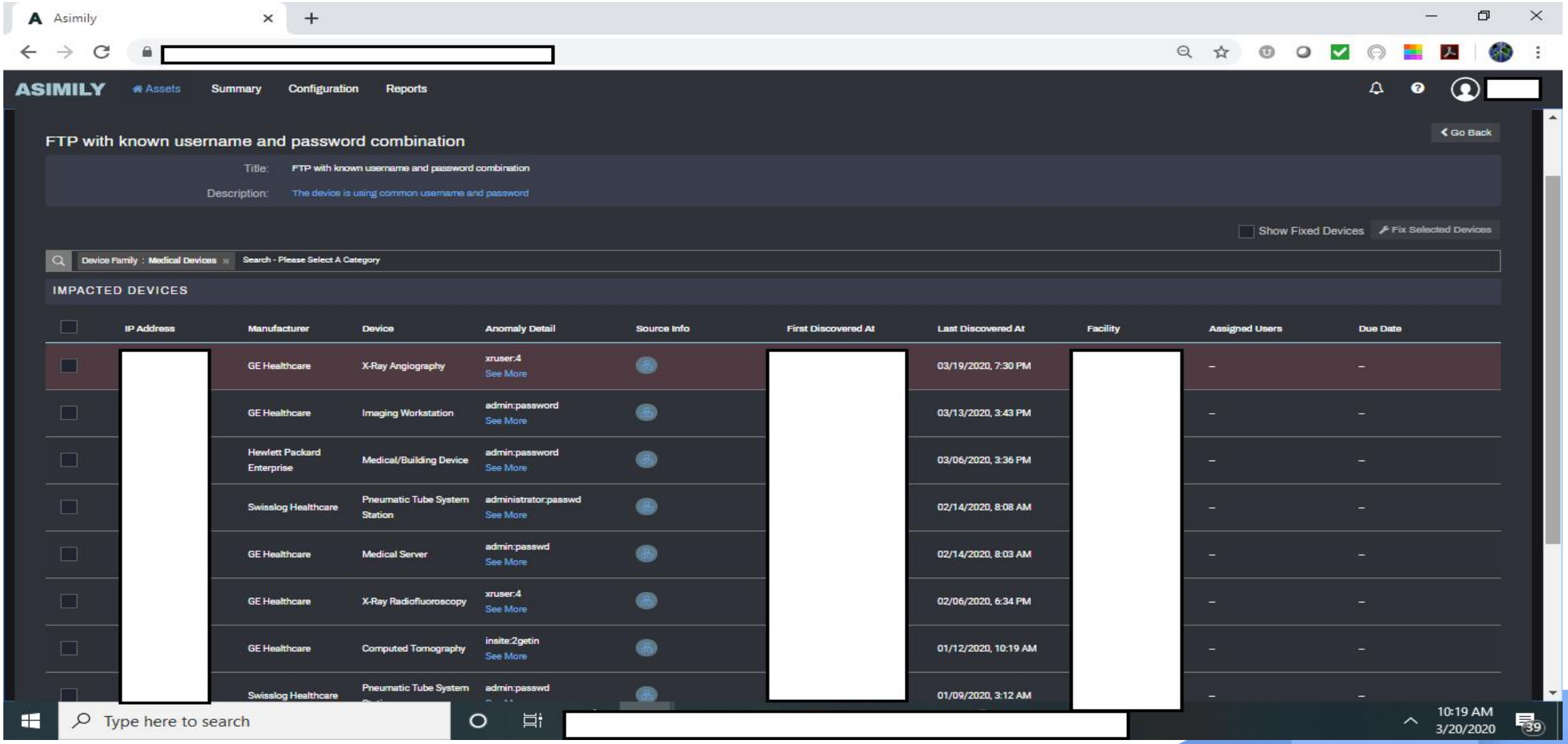
Anomaly and Forensic Analysis

- MLH monitors the sites periodically to determine what is happening on the network
  - Once an anomaly is determined or a potential misbehavior is seen, MLH makes changes to the device behavior directly on the device or network to take corrective action
  - MLH also determines the root cause and takes preventive action where required

- MLH also has several policies for what it determines as issues to be fixed
  - FTP, RDP, SMB, NFS connections – Why are they happening? Are they necessary?
  - Internet browsing – Discourage any kind of browsing from medical devices even to approved sites
  - Any external connections of any kind to be investigated and blocked if not required
  - Medical devices interact with IoT devices – Work with IT to ensure IoT, building and HVAC devices, etc. are secured.

- MLH has got Asimily to implement Forensic Analysis on top of Anomaly detection to understand the root cause so that it can understand the where to focus its resources
  - For example: Is a medical device being scanned? If so where is the scan coming from?

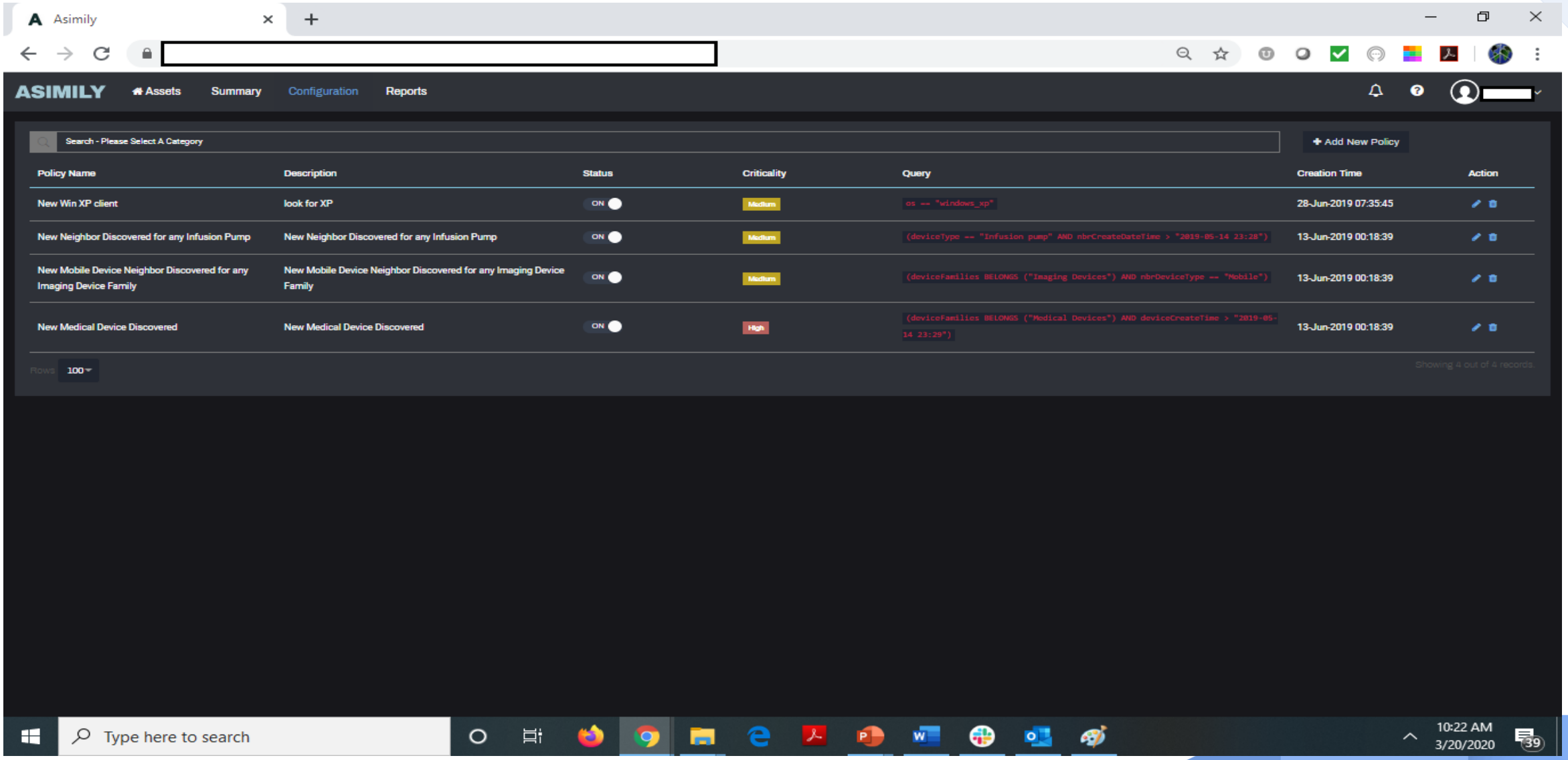
Anomaly and Forensic Analysis



Policy Management

- MLH has used the policy management module in Asimily to set policies to track events beyond anomaly or security events
- Some of the policies MLH has set up are:
  - Discovering when a new Windows XP device has been brought in
  - When a mobile device is connected to a new Imaging device
  - Tracking when a medical device leaves a given hospital
- Policies are easy to setup and can be done quickly. MLH will add more policies to add on

Policy Management



Overall MLH Approach for Managing Security

- Secure Wireless Medical Devices
- Avoid Bluetooth as much as you can
- Start with High Risk/Likelihood/Impact devices and modalities (MR, CT, etc.)
  - Where a device is high risk, high impact and work-around does not exist, put them behind firewalls which can “hide” the device
- Block off all exposed USB plugs to discourage unauthorized devices
- Consider using AD for logons – beware of inherited GPO, etc. Get you own AD location for medical devices and ask them to break all inheritances
- Use AV and malware protection if you can
  - MDS2s provide information on what can and cannot be done. Also remember to treat these as medical devices with special policies (e.g. : do not auto reboot, scan only when idle, etc.)
- Look at unusual activity and external connections and block them as required

Cost Analysis with the Automation

Task	Equivalent Number of resources	Cost per resource	Total people cost after automation	Manual costs (from slide 6)
Collecting all the Asset parameters	5% of a resource/month (review of data)	$90K/year	$5K/year	$540K/year
Collecting Vulnerabilities and Analytics of the collected Data And taking Action	19% of a resource (Take actions on the data)	$90K/year	$17K/year	Too high to quantify

Asimily provides other aspects like Vulnerability Exploit Analysis , Incorporation of MDS2 into Risk Prioritization, Impact Analysis, Remediation Actions, Utilization tracking, Anomaly Detection, Vendor tracking and others to help MLH with management of their medical devices

Future Developments at MLH

- MLH plans to leverage a lot more modules provided by Asimily and other systems in their network
  - Create a dossier of devices in CMMS system
    - Already been tested with a replica of the database
    - Use CMMS to Track/Remediate Anomalies and Vulnerabilities in Asimily.
  - Enforce Network segmentation through the Asimily integration with NAC and firewalls to better manage devices on the network
  - Using Asimily, Track utilization of devices on the network , Imaging Scans Monitoring And Dose Monitoring from Imaging Devices
  - Track how Vendors are accessing the devices
- MLH is working collaboratively with Asimily to use Asimily as a single view for all aspects of medical device management from procurement to operational management

Q & A
Thank You

Patrick Duncan
CBET
Integration Engineer, Clinical Engineering
Methodist Le Bonheur, Memphis

Shankar Somasundaram
CEO & Co-Founder
Asimily, Inc.