CYBER RECOVERY: ALLOTROPE USE CASE

ALLOTROPE USER MEETING, BOSTON (5-9 NOVEMBER 2018)

MERCK

INVENTING FOR LIFE

6-Nov-2018

Allan Ferguson, Josh Bishop

Cyber Incident Summary

Incident Background

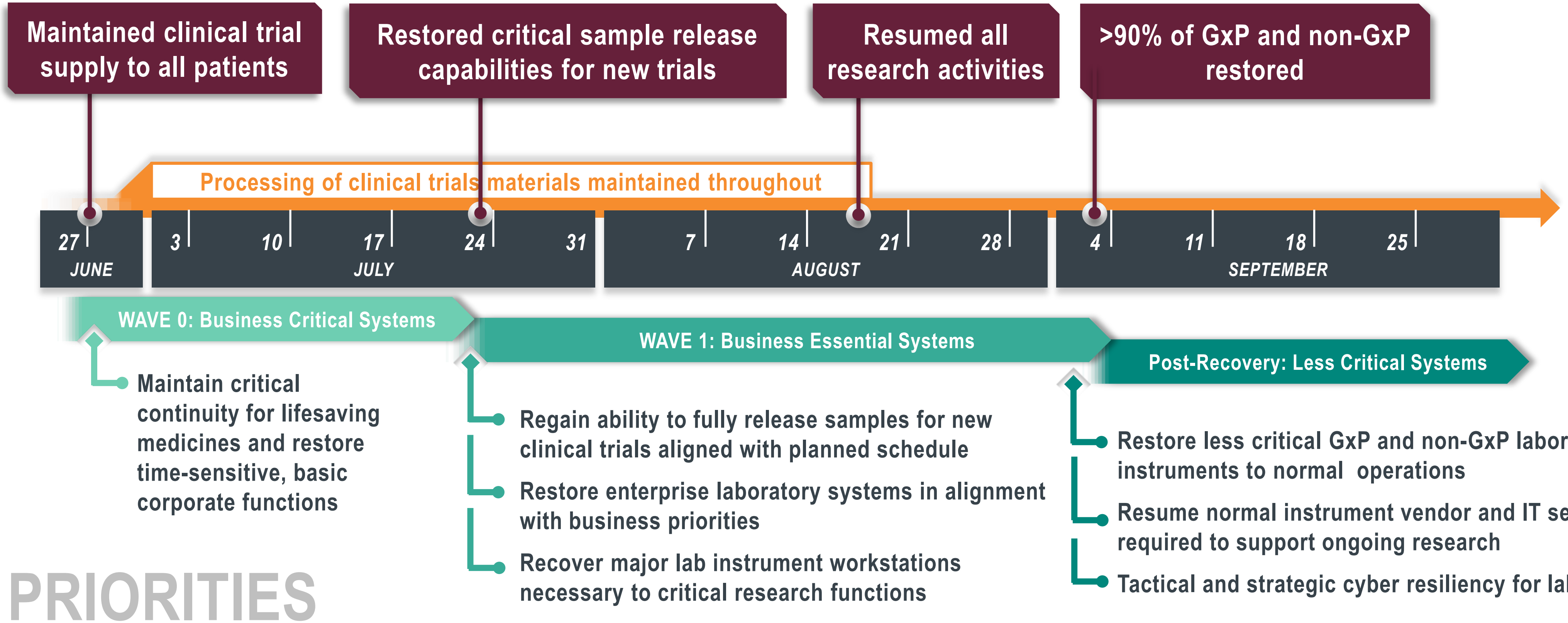
- Threat actors conducted a large scale cyber incident using the **NotPetya** malware
- Merck, along with **many other large organizations** across **numerous industries**, was a victim of the attack

Incident Anatomy

- Threat actors exploited a third-party software application used by Merck and other organizations in the Ukraine
- Threat actors gained unauthorized access to the software vendor's system to deliver the NotPetya malware
- The malware stole credentials from infected Windows systems, propagated across the networks and **encrypted the data on impacted systems**

Research Priorities Translated Into Integrated, Operational Recovery Program

MILESTONES



Maintained clinical trial supply to all patients

Restored critical sample release capabilities for new trials

Resumed all research activities

>90% of GxP and non-GxP restored

Processing of clinical trials materials maintained throughout

WAVE 0: Business Critical Systems

- Maintain critical continuity for lifesaving medicines and restore time-sensitive, basic corporate functions

WAVE 1: Business Essential Systems

- Regain ability to fully release samples for new clinical trials aligned with planned schedule
- Restore enterprise laboratory systems in alignment with business priorities
- Recover major lab instrument workstations necessary to critical research functions

Post-Recovery: Less Critical Systems

- Restore less critical GxP and non-GxP laboratory instruments to normal operations
- Resume normal instrument vendor and IT services required to support ongoing research
- Tactical and strategic cyber resiliency for labs

PRIORITIES

MERCK INVENTING FOR LIFE

Key Considerations for Lab Recovery

- Implement recovery process
  - Engage key partners (IT, instrument vendors, operations, sciences)
  - Proceed based on prioritized systems
  - Determine what is needed where

- Continue experimentation
  - Bring instrument online
  - Generate new data
  - Perform analysis & reporting

- Restore access to existing data
  - Access to data sources
  - Perform analysis & reporting

Cyber Resiliency Near Term Actions

Back Up of Lab Instrument Workstation Images

- Capture Lab Workstation images for business prioritized systems.
- Begin planning for longer term lab OS management

Revised Plan to align enterprise lab solutions with enterprise resiliency

- Rapid adherence to Enterprise Resiliency plans

Update Lab Inventory Data and Processes

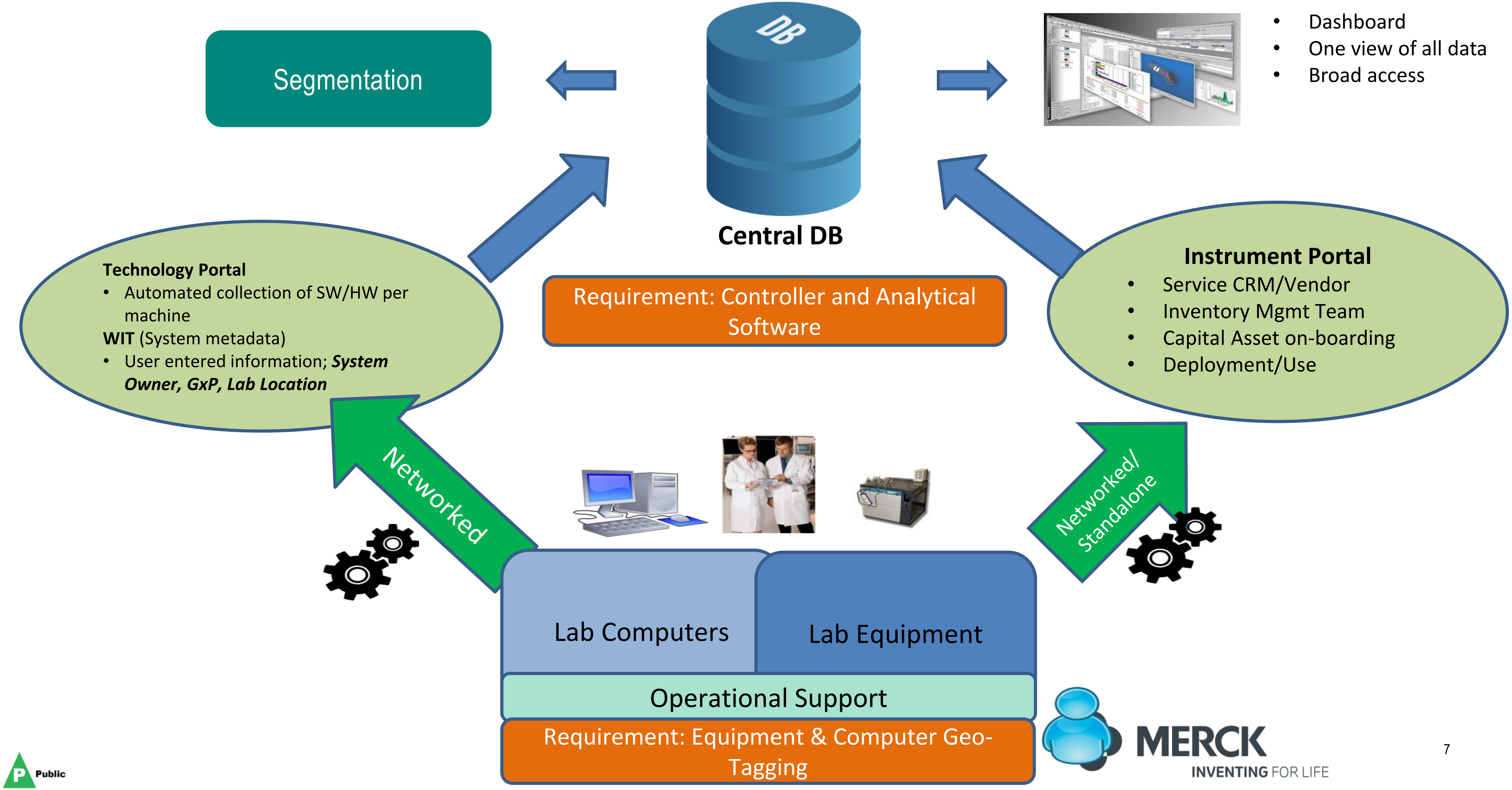
- Accessibility and accuracy of lab equipment and IT dependencies

Post-Cyber Recovery: Enhancing Lab Operations

Digital Lab Strategy

- Efficient and effective lab instrument access
- Consideration of major use scenarios: science, IT, engineering, ops
- Comprehensive and accurate lab asset repository
- Better visibility into lab equipment maintenance and validation status
- Access to instrument data (even when instrument software unavailable)
- Better availability of methods/protocols
- Disentangling data creation from data analysis

Lab Instrument Opportunities: Real-time monitoring of systems



Segmentation

Central DB

- Dashboard
- One view of all data
- Broad access

Technology Portal

- Automated collection of SW/HW per machine

WIT (System metadata)

- User entered information; ***System Owner, GxP, Lab Location***

Requirement: Controller and Analytical Software

Instrument Portal

- Service CRM/Vendor
- Inventory Mgmt Team
- Capital Asset on-boarding
- Deployment/Use

Lab Computers

Lab Equipment

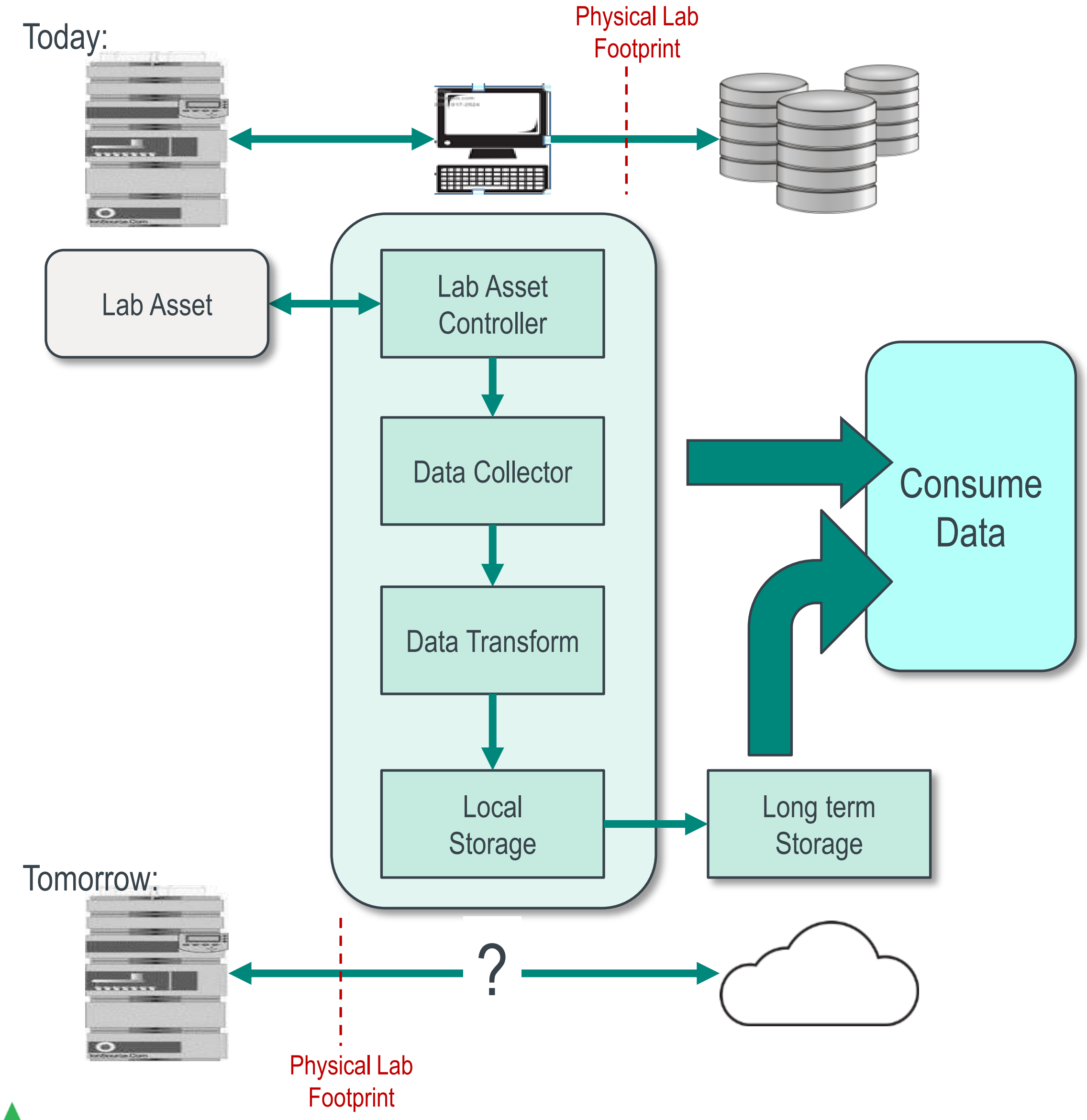
Operational Support

Requirement: Equipment & Computer Geo-Tagging

MERCK
INVENTING FOR LIFE

P Public

Lab Instrument Opportunities: Changing how we solve lab workflows



Key Messaging:

- today **functionality** exists on local PCs
- tomorrow we have a better opportunity to distribute

- current focus builds on top of what already exists
- future focus should **redefine** how silicon accelerates science

- current configuration is overwhelmingly one scientist to one instrument
- future configuration should support a **many-to-many relationship**

- current silicon enables high value assets
- future silicon should focus on **digitization of all lab assets**

- Today apply security measures to be compatible with lab equipment
- Future apply **all security measures** to labs regardless

What are the Use Cases for Allotrope

Business continuity

- Instrument data in standardized form accessible by more than single application
- Means to rapidly restore instruments to current state
- Availability of instrument calibration info/data to reduce/eliminate restart time

Lab Productivity

- Comprehensive Methods/Protocol repository for lab instruments
- Manage instrument utilization, dependencies and metadata
- Proactive monitoring/diagnostics for instrument components to sustain uptime

Roadmap In Brief

Beyond

- **Full adoption** across Research / Target Outcomes Fully Realized
- **Legacy systems retired**
- Sustainable **operating model** and adoption of platform technologies facilitate future advancement

2020

- **Digital Lab** becomes a reality – secure operating system and infrastructure, automated workflows, exposed human-machine interfaces (voice and visual cues)
- Life Science Cloud for Research benefits become a reality

2019

- **End to end** data capture, integration, and analysis for selected groups
- **Teams working jointly**: data standards/governance and records mgt.
- Implement **Io(L)T** for lab instrument **command and control**, **inventory, utilization** and **data collection**

H2 2018

- New molecular registration capabilities
- Request workflow simplification
- **Collaborative** planning of IT portfolio and scientific support

H1 2018

- Establish and release technology to interrogate **trusted, integrated datasets**
- Examine IT/Science hurdles to success

Backup Slides

Public

MERCK
INVENTING FOR LIFE

Restore research functions critical for business continuity

- Most research operations were interrupted by the initial cyber attack
- For employee safety, all research operations were brought to a safe position in a controlled manner using existing procedures.
- Health authority notifications began immediately domestically and internationally.
- Quality Alerts and guidance were initiated for the event, for the compliant restoration of systems in a controlled manner and to evaluate for disruption to key quality and compliance systems.
- Documentation was initiated and controlled for the GxP system outage to provide guidance for Windows system restoration and guidance for non-Windows system restoration.
- Research operations were then restored according to the priority for product-to-patient supply and after IT system hardening and GMP documentation needs were met.

Additional Benefits and Opportunities

- Elevation of the Allotrope Data Format
  - Modular Methods Database
    - Improved security of methods by removing from local storage
    - Improved ability to share methods across functional areas and divisions
    - Improved usability of methods across multiple instrument vendors

- Potential to reduce surface area for cyber attack in the future

- Reduced technological burden of support on lab computing resources