Dr. Allen Harper, CISSP, Executive Vice President of Cybersecurity Allen.Harper@trexsolutionsllc.com

Dr. Allen Harper has more than 30 years of experience in IT and cybersecurity. After retiring from the U.S. Marine Corps, Dr. Harper started a successful cybersecurity consultancy, which was acquired in just six years. Having performed hundreds of security assessments for public and private sectors, he is a best-selling author and the lead author of the Gray Hat Hacking series. Dr. Harper specializes in ethical hacking, offensive security, penetration testing, and reverse engineering. He most recently served as department chair and cyber program director at Liberty University. Dr. Harper holds a bachelor's degree in computer engineering from North Carolina State University, a master's degree in computer science and information assurance from the Naval Post Graduate School, and earned his Ph.D. in business and IT from Capella University.

HOW THE CLOUD SAVED THE 2020 CENSUS

Presented To: AFCEA Mid-America Conference

RELENTLESSLY DRIVING INNOVATION

Dr. Allen Harper

November 4, 2020

T-REX

The U.S. Census Continues To Advance America's Computing Industry

1880

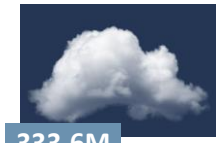
1st Commercial Calculator in 1850

1890

1st Tabulating Machine

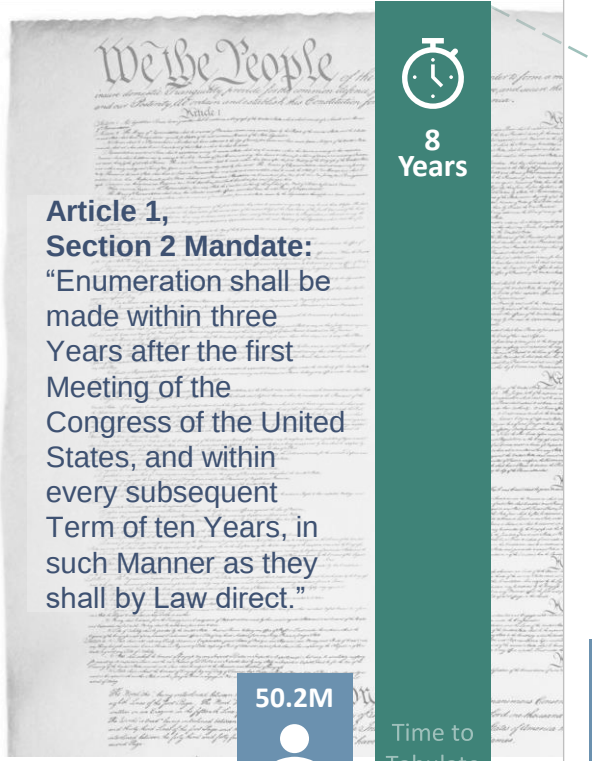
1960

1st General Purpose Electronic Digital Computer in 1951



2020

1st Census to use "Public Cloud" Technology



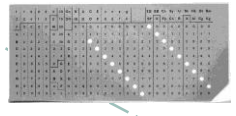
Article 1, Section 2 Mandate: "Enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct."

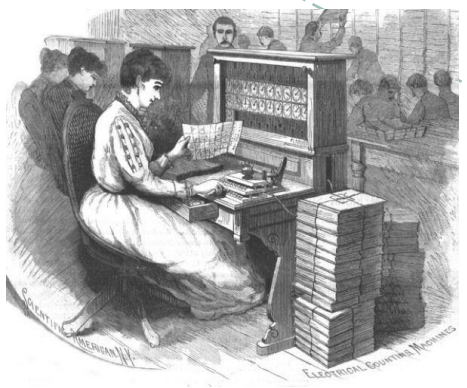
8 Years

Time to Tabulate

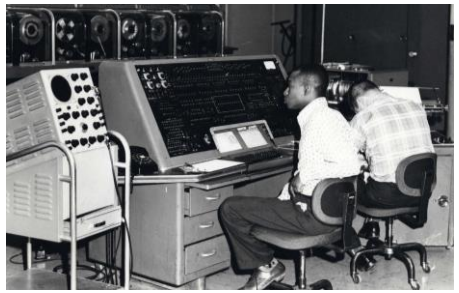
50.2M

Herman Hollerith created an electronic tabulating machine for use on the 1890 Census.





62.9M

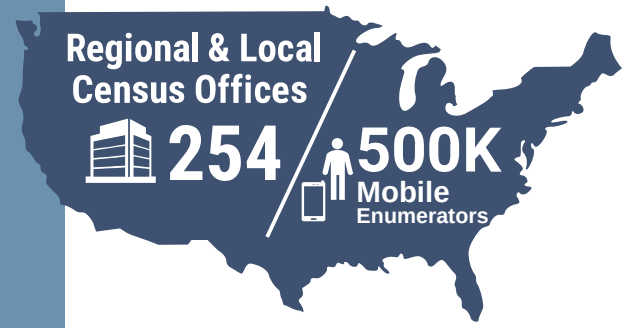


189.3M

UNIVAC I:

- 1st UNIVAC computer delivered to the U.S. Census Bureau in 1951
- 1ST used to process and tabulate data for 1960 Decennial Census

333.6M



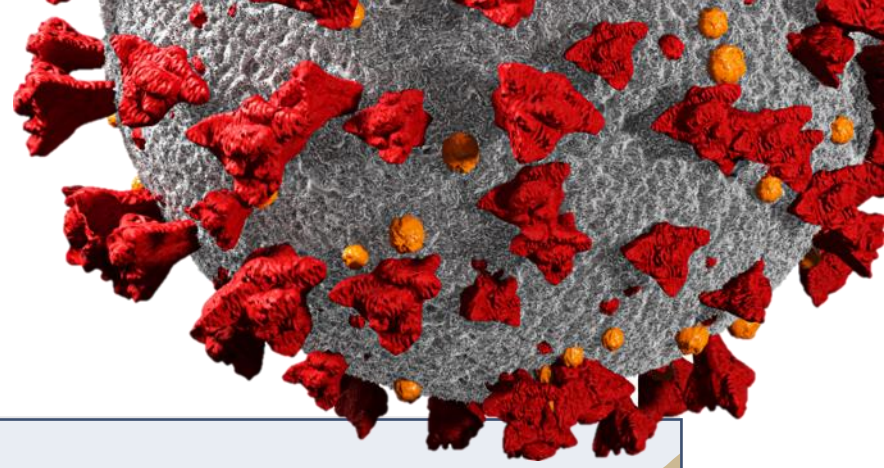
143M Households

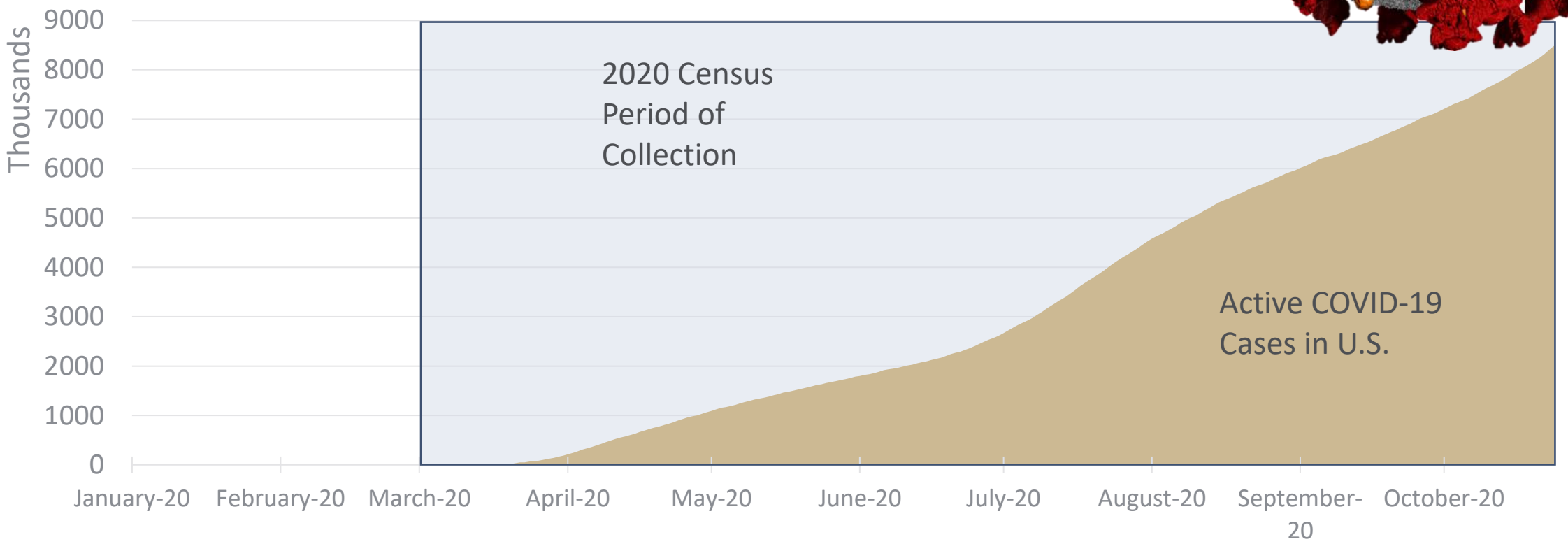
600K Peak, Concurrent, Internet Self-Respondents (ISR)

Months

https://www.census.gov/history/www/innovations/technology/tabulation_and_processing.html

The Impact of Cloud ISR on Census during COVID



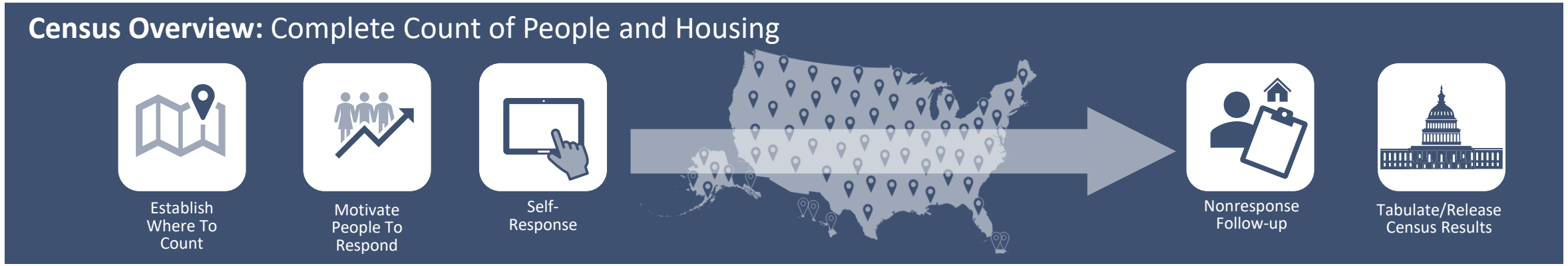


Cumulative US Covid-19 Cases

World Health Organization as of 10/26/20

https://covid19.who.int/?gclid=Cj0KCQjwit_8BRCoARIsAIx3Rj7BR7bl1NCvcM_NMQMXZDEMQMhVvSdi-AOxRF85YWOw8mkFC55G1U8aAl3REALw_wcB

How Technology Is Being Used For The 2020 U.S. Census



Size, Scale & Complexity

Cost Savings Achieved $2.4B

Mission Critical Systems 52 | 18

100% Availability

Integrated 32 Network & Security Tools with 285+ Apps

600K Peak Concurrent Respondents load tested to 1.2M

Regional & Local Census Offices 254

20K Office Workers

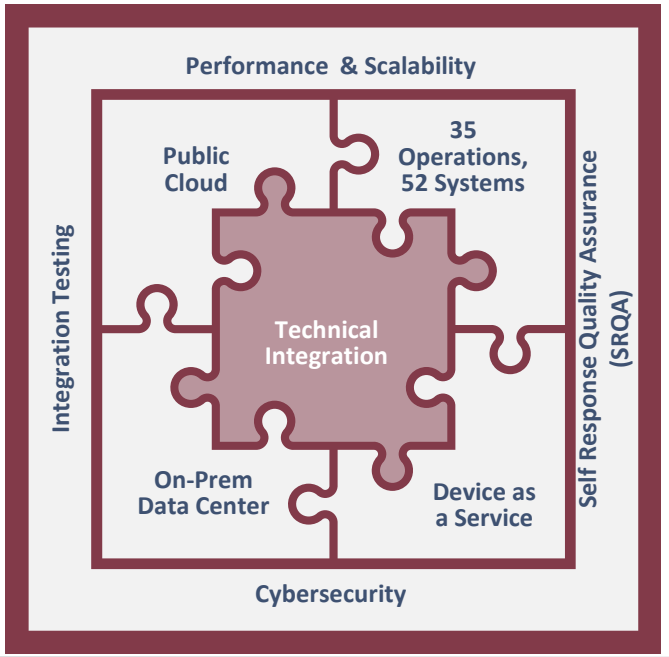
45 concurrent scrum teams

16 release trains

Decennial Systems Collect Information From:
- 325M Residents
- 148M Households
- 450+K Mobile Enumerators

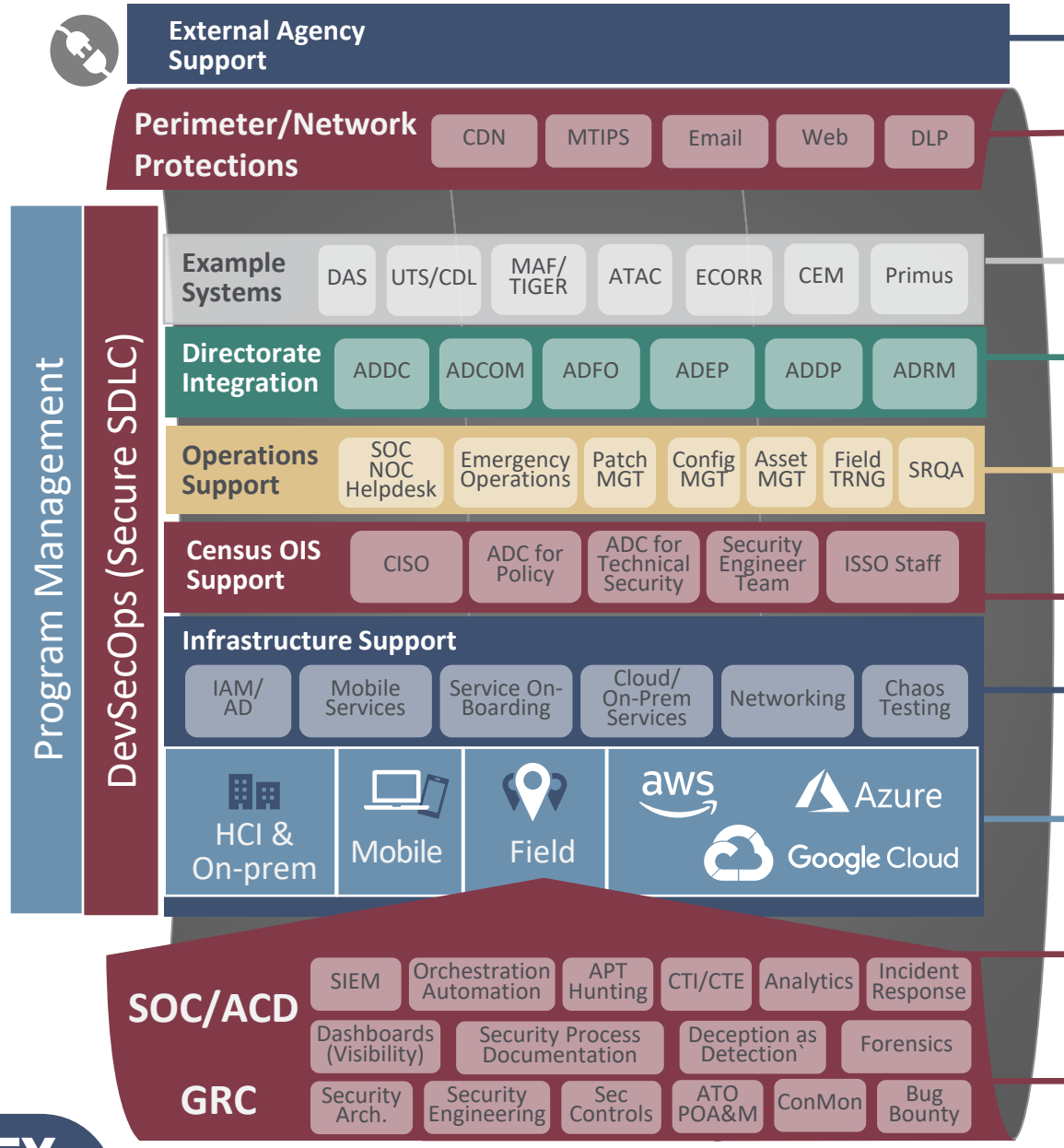
500,000+ Endpoints Monitored

Bringing the Technology Pieces Together



Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this presentation

Technical Integrator (TI) and Leader of USCB Large and Small Vendors



Flexible External Support
- **Worked with External Agencies**

Data-Threat Centric Approach
- **Deep Packet Inspection Services:** 7.5 PB of data protected by 20+ cyber tools + external CDN, Cloud, and MTIPS Services

Integration of 52 Business Systems
- **Internet Self-Response (ISR):** representative directorate systems shown

Collaborative & Organizational Integration
- **Horizontal Integration across all 6 Census Directorates**

Operationally-Focused Organization
- **Integrated Support to Census Operations, developed and operated SRQA, documented 500+ operational KBAs**

Security Support to Census OIS
- **Responded to up to** RFIs, PIAs, ATOs, ISCMs

Responsive Infrastructure Support
- **Integrated Support to Census Infrastructure,** resolution of hundreds of remedy tickets

Hybrid Cloud & On-Premise Services Environment
- **Built and integrated** Azure, AWS GovCloud, GCP, mobile, remote office and multi-SaaS environment with over 500,000 endpoints

Proactive SOC with Active Cyber Defense (ACD)
- **Targeted Data Protection Services:** 7.5 PB of data protected by 24x7x365 SOC, with 20+ cyber tools and proactive, threat-focused posture

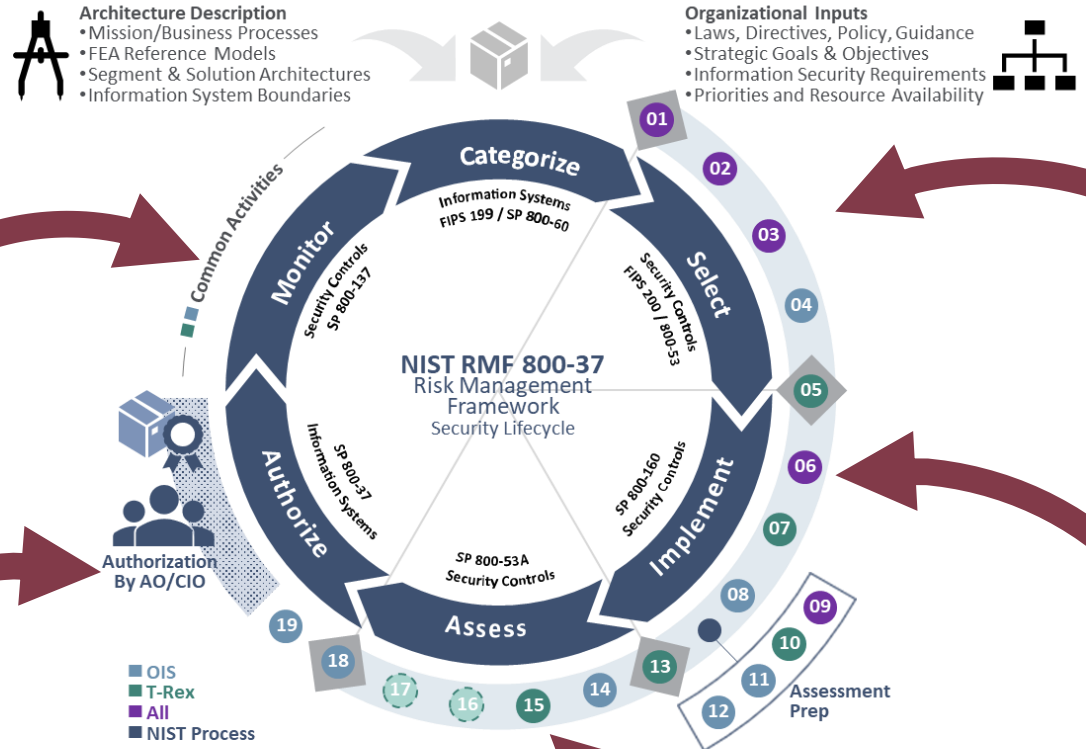
Governance, Risk Management Compliance (GRC)
- **Foundational Security** through Architecture, Engineering, Security Controls, Assessment, Authorization, Remediation, Monitoring, External Reviews

Note: Compliance ≠ Security

TI ATO Lifecycle Process and Automation Steps

Single Security Visibility/Agility

- **T-Rex ATO Dashboard:** full stakeholder visibility through every ATO step
- **Real-time status of ATOs in process:** inclusive of duration in each process step to enable pinpointing of issues for quick resolution and identification of regular occurring bottlenecks for process improvement



Inheritable Components

- **ATO Inheritance:** by using components already authorized, only the newly developed pieces need to seek new ATO. Reused aspects can be signed off based on existing ATO
- **Prioritizing ATO of Security Components:** enables expediting of issue resolution to minimize ATO cycle time

ATO Services and Automation

- **Every Endpoint Enabled** ensures readily available, ATO-automation data
- **Holistic DevSecOps approach** ensures built-in endpoint solutions (implement phase and continuous assessment phase)

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this presentation

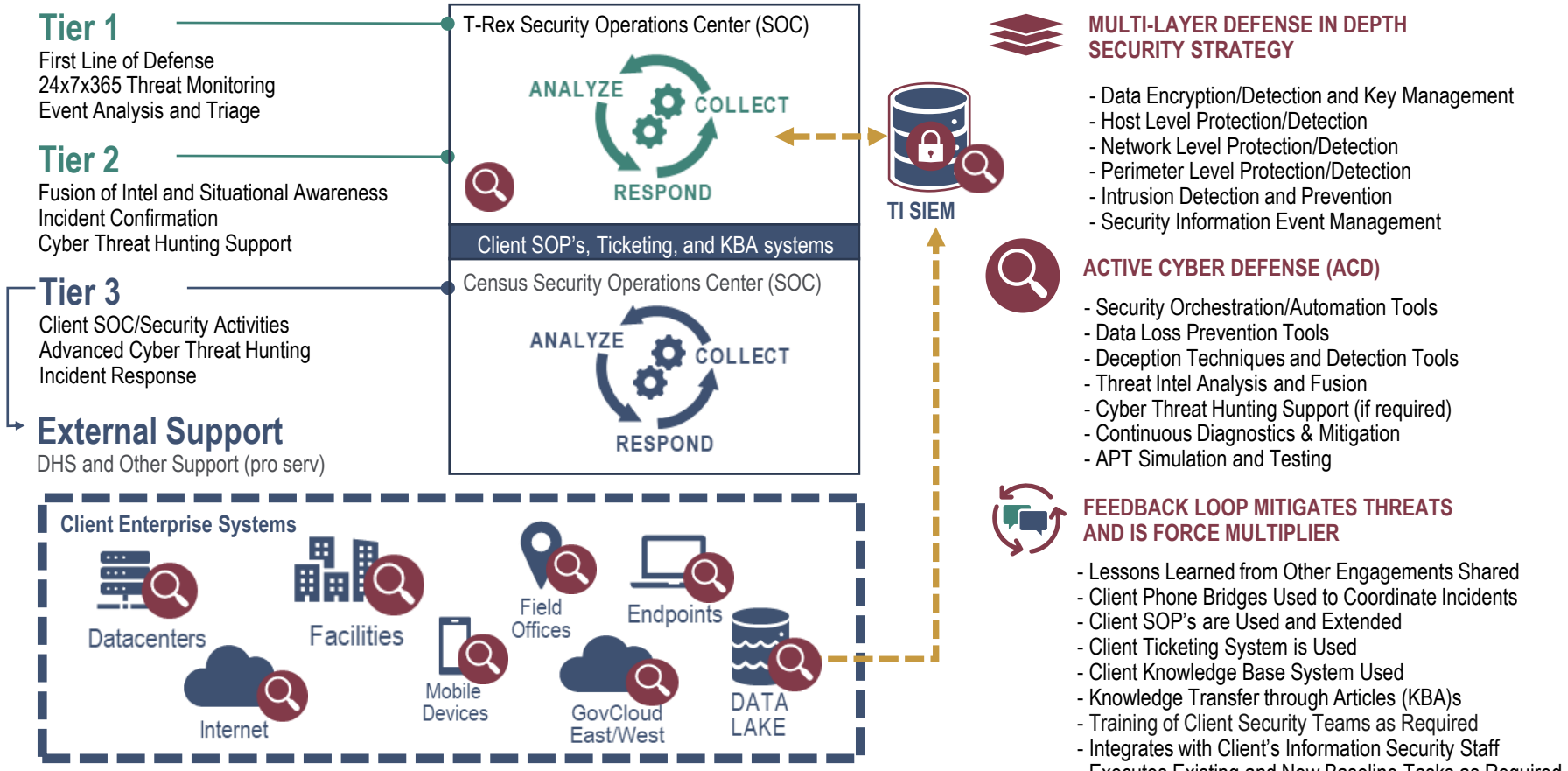
Integrated SOC: Extension Of Census SOC

Note: Due to COVID-19, we transitioned to Remote SOC in 1 week, using VPN/VDI

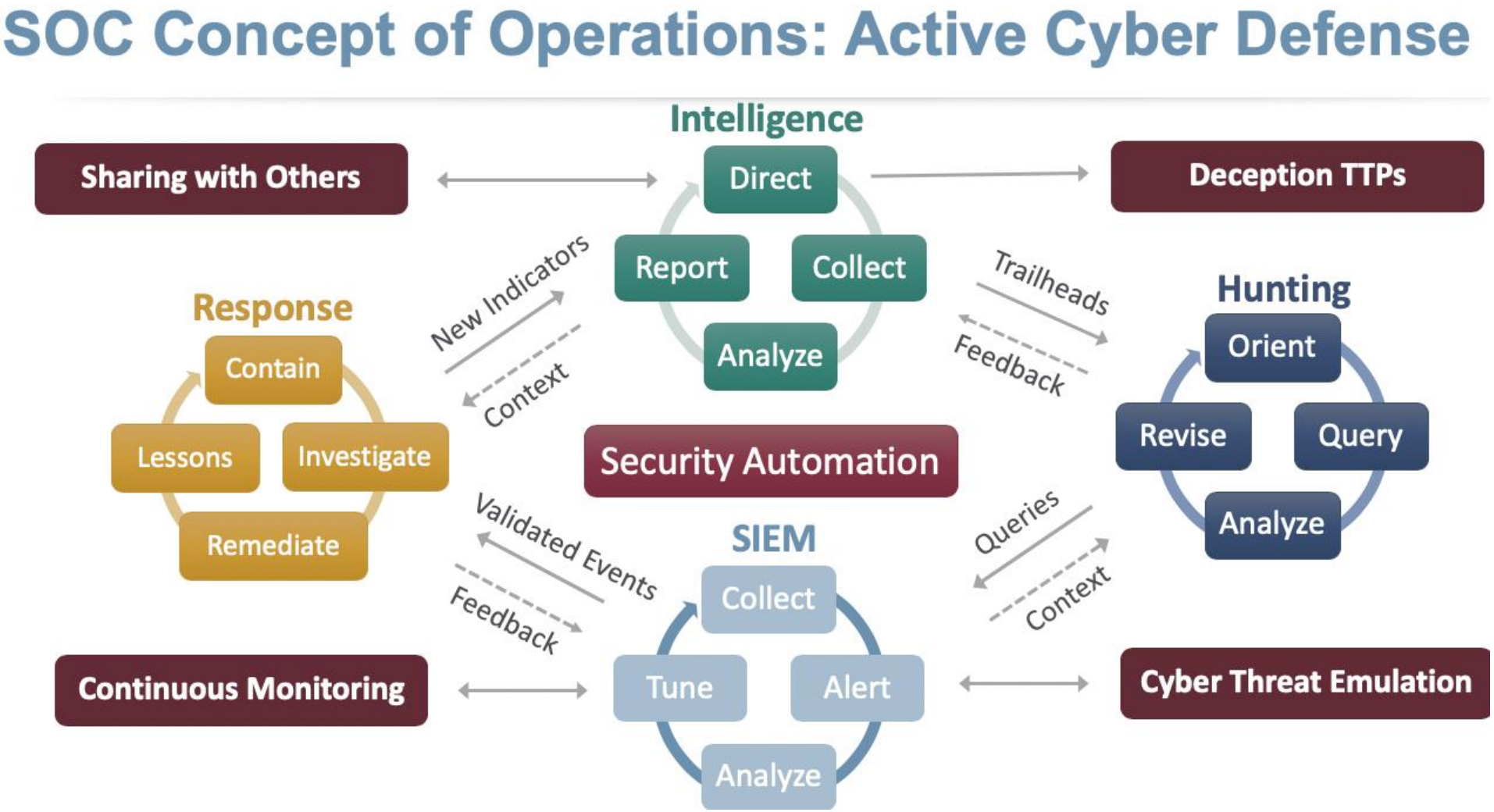
Many Lessons Learned:

- People
- Process
- Technology

Where We Fit – The Role of T-Rex Security Operations Center (SOC)



Nation State Threat Requires a Proactive Security Posture



BACK-UP

T-REX

OUR DEEP TECHNICAL EXPERTISE

Cloud Adoption & Infrastructure Optimization

- Migration of Legacy Apps
- Multi-Cloud
- IaaS/SaaS/PaaS
- Containers/Serverless/N-Tier
- Event Driven Automation
- Modeling for Cost Optimization
- DevSecOps
- Agile Infrastructure Development
- Infrastructure Virtualization/HCI
- Disaster Recovery Planning/HA
- Network Infrastructure
- ITIL Implementation and Automation
- O365/Active Directory
- Virtual Desktop Infrastructure
- Monitoring Automation and Visualization

Cybersecurity

- Data Loss Prevention
- Intrusion Prevention & Detection
- Risk & Threat Profiling
- Cyber Threat Hunting
- Adv. Persistent Threat Testing
- Static & Dynamic Code Analysis
- Key Management
- Access & ID Management
- Continuous Diagnostics & Mitigation
- Network Visibility / SSL Decrypt Processing
- Database Security Enforcement; Database Configuration, Access Control Policy Enforcement
- SOC Operations & Management
- Security Orchestration, Automation and Response
- Zero Trust
- Security Application Design/Implementation

Data Engineering & Analytics

- Data Architecture, Design & Governance
- Big Data Storage/Big Data Processing
- Fraud Data Analysis
- High Performance Computing
- Performance and Data Modeling
- Dashboards & Visualization
- Data Web/Mobile Interface
- Self-Service Business Intelligence
- Augmented Analytics
- Machine Learning
- Robotic Processing Automation

Systems Integration & Development

- Agile Application Development
- UI/UX Design
- SAFe Transformation/Execution
- Enterprise & System of Systems Architecture (FEA and TOGAF)
- Application Rationalization
- Modernization Roadmapping
- Agency Horizontal Integration for Modernization
- System of System Design
- Strategic Planning & Policy Development
- Model Based System Engineering
- Interface Design
- Technology Evaluation
- Gap Analysis
- Automated Functional, Performance and Integration Testing

Mission Critical Services

- Program Management
- Earned Value Management
- Quality Management
- Knowledge Management
- Facilities Management
- Change Management
- Metrics Management
- Incident & Ticket Management
- ITIL Service Processes
- Help Desk Functions
- ITIL Training
- Intelligence Analysis
- Operational Coordination