Background

- Over 28 years of experience in device security, IT, data analytics
- Served as the chairman and board director for Trusted Computing Group.
- Vast industry expertise spans life sciences, manufacturing, government, healthcare, financial services
- Holds 7 patents in cryptographic technology & 5 pending patents

Brian Berger, President of Cytellix Corporation

CYTELLIX®

The Cybersecurity Division of IMRI

Cytellix – Trusted Leader in Managed Cybersecurity

- Cytellix Corporation is the wholly owned Cybersecurity subsidiary of IMRI
- IMRI, Delivering comprehensive Cybersecurity, IT Infrastructure and Program Management solutions since 1992
- Successfully delivered over $220+ million in technology contracts

Cybersecurity Operations:

Over 1500 networks, 7 million devices; Engaged with U.S Army Network Enterprise Technology Command; Missile Defense Agency; U.S Army Corps of Engineers; DISA

Cyber Security Compliance Readiness:

Assisting over 150 Small to Medium Size Businesses with NIST 800-171 Compliance Readiness

Cyber Security Supply Chain:

Assisting large integrators supply chain vendors with NIST 800-171 Cyber Security Readiness

Program Management:

Assisting U.S Army Corps of Engineers and multiple regions of GSA with Acquisition and Contract Management

Computer Operations:

Supports Army DOD Supercomputing Resource Center (DSRC) with various 7/24 HPC Program and Operations over $300 million.

Data Center/Cloud Computing:

Since 1996, provided onsite and remote technical, operations support, network monitoring, help desk and system administration support for DISA, U. S. Army Corps of Engineering, and NRL.

Cytellix provides a simplified, easy to use, cost effective complete visibility platform

Affordable
Measurable

Flexible
Frictionless

Capabilities to consider for: NIST and CMMC

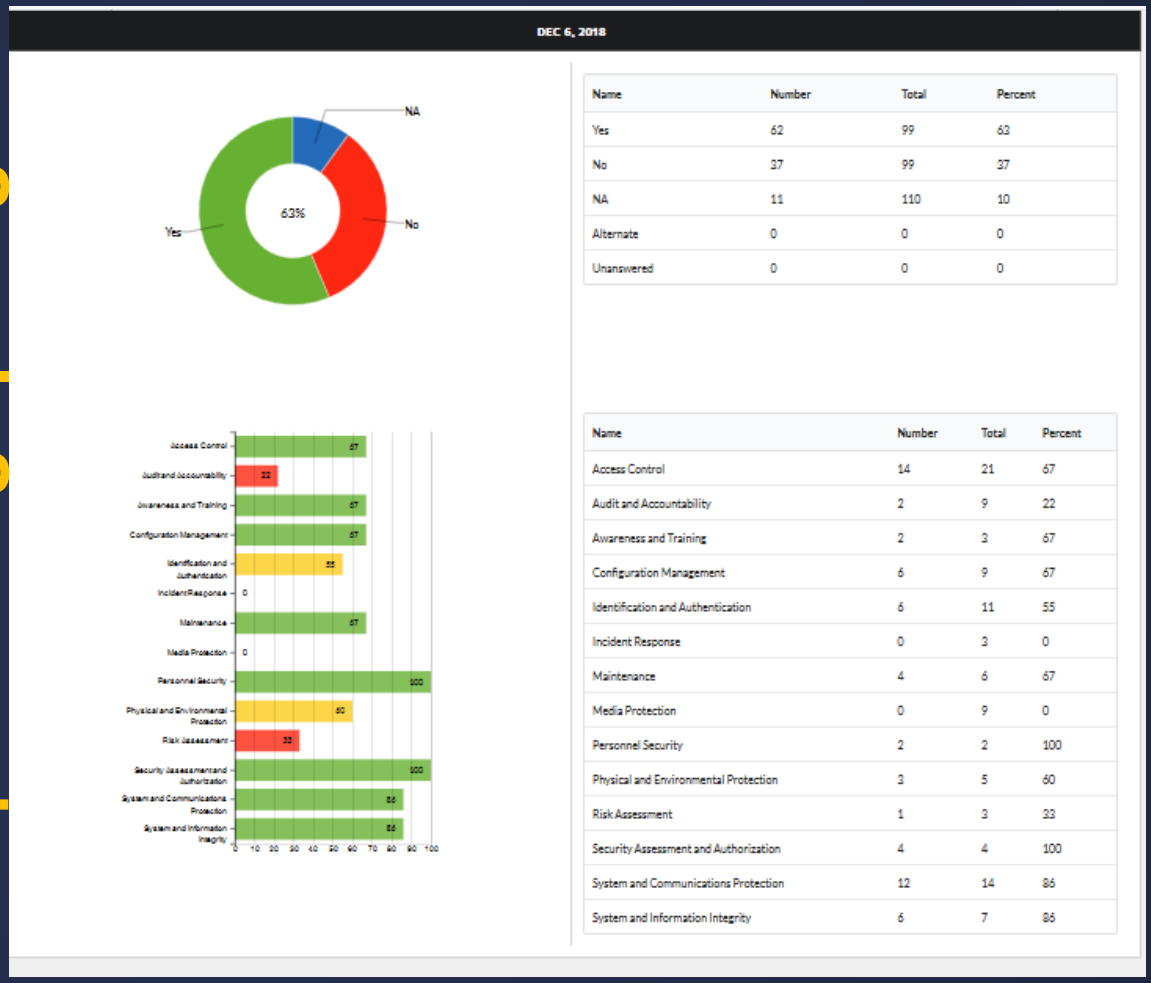
- Cyber Assessments by Framework (NIST, ISO, *CMMC)
  - Compliance – highly automated
    - *Assessments - Gap Analysis*
    - *Plan of Action for Remediation*
    - *Pre-written Cyber Policies*
    - *Artifact collection (assessing compliance)*
- Real-time 24x7 Cyber Monitoring
  - Profiling, Leak Detection, Bad Actor Connections, Network Discovery
- Vulnerability Testing & Monitoring
- Security Information and Event Management as a Service (SIEM)
  - Log management, use cases by framework
- Incident Management / SOC
- Threat Hunting
- Cyber event correlation and filtering
- Real-time cyber event notifications - Alerting

**Planning for C3PAO Accreditation*

Cyber Controls

- NIST
- CMMC
- ISO
- RMF
- Customer Specific Measures

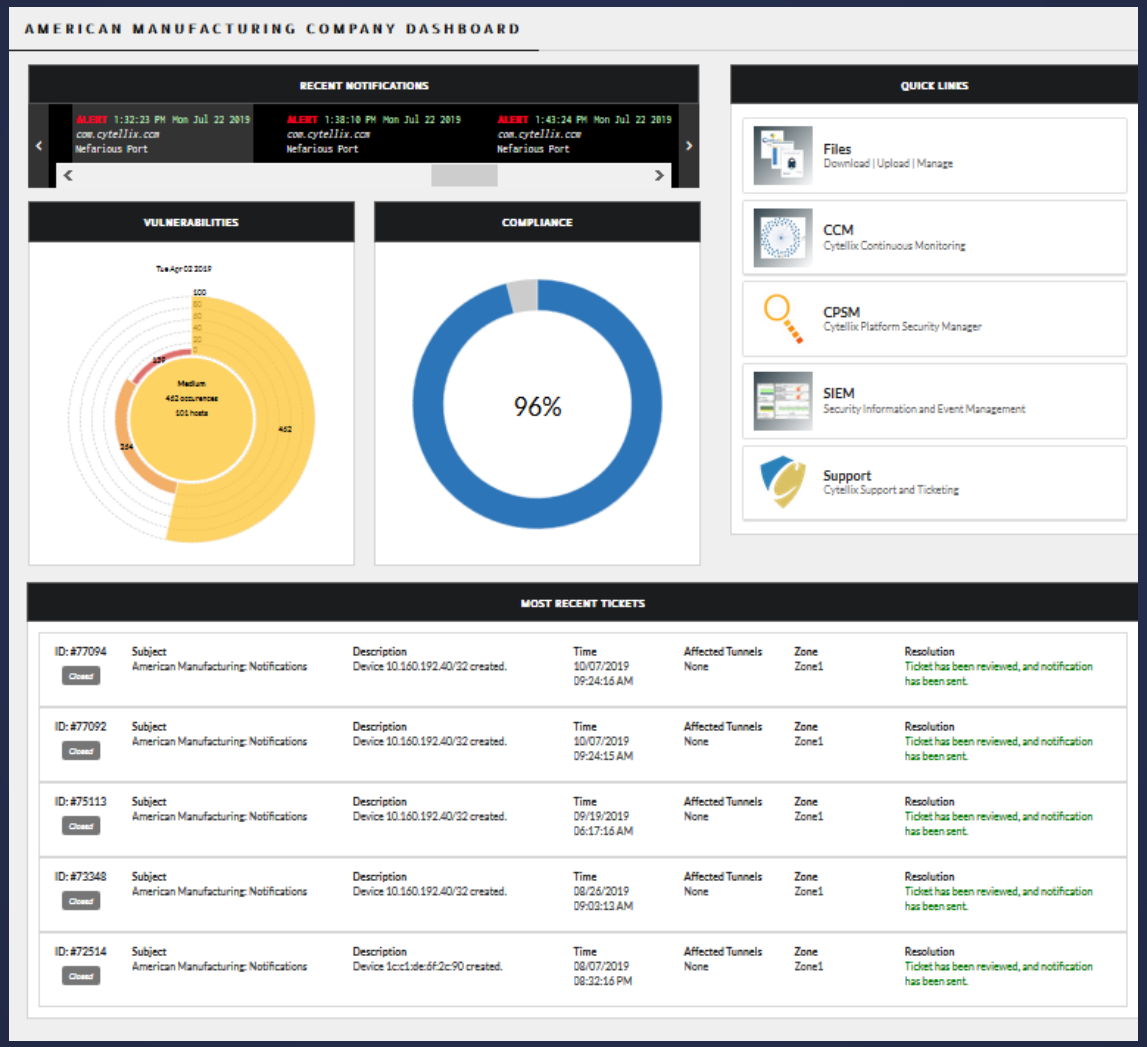
Sample Scorecard



Name	Number	Total	Percent
Yes	62	99	63
No	37	99	37
NA	11	110	10
Alternate	0	0	0
Unanswered	0	0	0

Name	Number	Total	Percent
Access Control	14	21	67
Audit and Accountability	2	9	22
Awareness and Training	2	3	67
Configuration Management	6	9	67
Identification and Authentication	6	11	55
Incident Response	0	3	0
Maintenance	4	6	67
Media Protection	0	9	0
Personnel Security	2	2	100
Physical and Environmental Protection	3	5	60
Risk Assessment	1	3	33
Security Assessment and Authorization	4	4	100
System and Communications Protection	12	14	86
System and Information Integrity	6	7	86

Complete Cyber Posture & Visibility



Single Pane of Glass

1. **Complete NIST SP 800-171**
    - Work your POAM's
    - Remediate vulnerabilities
    - Develop your Incident Response Plan

2. **Compliance and Cybersecurity Preparedness**
    - Conduct internal reviews with your security team
    - Prepare evidence of compliance
    - Complete policies and procedures
    - Technology enablement
    - Monitor for threats
    - Respond to Incidents
    - Remediate proactively
    - Training
    - Have a active cyber program

Actions to take – NIST is still a requirement

Protect your business and the USA

Key Points to CMMC Preparation

1. Implement NIST SP 800-171, 110 controls and 320 objectives
   - Use NIST SP 800-171 as guidance
   - Conduct internal reviews with security team to ensure they are aware of relevant CMMC 1.0 details
   - Review when contracts are up for renewal and plan to for CMMC in advance of new contract awards.
   - Collect artifacts (evidence) of compliance for each control (NIST currently)
   - There is no "throw away work" as CMMC leverages NIST SP 800-171 framework
2. Network discovery and data protection
   - Complete a network diagram showing all segmentation
   - Identify all assets on the network
   - Test for leaks, bad actor connections, unknown IP's, vulnerable ports
   - Protect IP and CUI from insider and outsider threats
3. Remediate gaps and vulnerabilities
   - Discover and remediate vulnerabilities as a practice
   - Manage and remediate cyber events efficiently
4. Monitor cyber activity
   - Develop use cases that correlate NIST requirements
   - Identify legitimate threats and cyber events – near real-time preferred
   - Capture logs and remediation steps for cyber events

Connect with Us

CYTELLIX®

The Cybersecurity Division of IMRI