# AMPLIFY

# Medtech

AMPLIFY
Medtech

# Fehmida Kapadia

AMPLIFY
Medtech

# Mission

*Our goal is to establish a unified MedTech ecosystem by promoting collaboration, networking, and the sharing of resources among startups, investors, service providers, entrepreneurial service organizations (ESOs), economic development agencies, academic institutions, entrepreneurs, and inventors. We aspire to cultivate a vibrant, sustainable, and locally engaged MedTech community that will stimulate economic growth in the area.*

AMPLIFY
Medtech

# How will we do this?

AMPLIFY Medtech

# Whom do we serve?

***MedTech Startups***

***MedTech Corporations***

***MedTech Service Providers***

***Entrepreneurial Service Organizations (ESOs)***

***Economic Development Agencies***

***Academic Institutions***

***Entrepreneurs***

***Inventors***

AMPLIFY Medtech

# How Do We Create Impact?

- ***Unify the Ecosystem***
- ***Enhance Collaboration***
- ***Facilitate Access to Resources***
- ***Community Engagement***
- ***Support Economic Growth***
- ***Promote Sustainability***

AMPLIFY Medtech

# Our Core Values

- ***Collaboration***
- ***Accelerating Innovation***
- ***Economic Development***
- ***Sustainability***
- ***Inclusivity***
- ***Integrity***

AMPLIFY
Medtech

# Upcoming Events

- **February 20, 2025:** Crafting a Compelling Pitch to Raise Investment and Scale Your Company
- **March 20, 2025:** Bringing MedTech Products to Market: Navigating US Healthcare Reimbursement
- **April 17, 2025:** Dilutive Funding for MedTech Innovators: SBIRs and Beyond

AMPLIFY
Medtech

# Contact

fehmidak@kapamedinc.com

WORRY FREE IT SERVICES

Advantage.Tech

# Cybersecurity Considerations for MedTech

VERSION 1.1 | JANUARY 2025

WORRY FREE IT SERVICES

Advantage.Tech

# #Whoami

## Chris May

Security Director
Advantage Technology
Cmay@advantage.tech
866-497-8060


ATCC


Q:
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
CYBER SECURITY

Advantage.Tech

# Recent Headlines*

- Ransomware Attack on Major Hospital Chain Exposes Patient Data
- Insulin Pump Vulnerabilities Prompt Urgent Manufacturer Alerts
- Healthcare IoT Devices Under Increased Cyber Attack, Says Industry
- Global Regulatory Bodies Push for ‘Software Bill of Materials’ in MedTech
- Cloud Misconfigurations Leave Patient Data at Risk
- Cyber Threats to Hospital Robots and Automated Surgical Systems Raise Alarms
- Medical Device Patch Delays Prompt Criticism from Security Researchers
- Companies’ Employees To Blame For Cyber-Attacks: Report

# The Finger of Blame

# Agenda

- The Rapid Growth of MedTech & Why Cybersecurity Matters
- Unique Cyber Threats in MedTech
- Regulatory Compliance (HIPAA, FDA, etc.)
- Best Practices for Security
- Incident Response Strategies
- Future Trends (AI & Cloud)
- Q&A

Advantage.Tech

**“As medical devices become more interconnected and interoperable, they can improve patient care and create efficiencies in the health care system. However, these same features also increase cybersecurity risks, potentially impacting device performance and patient safety.**

– Scott Gottlieb, M.D. | Former FDA Commissioner

# The Rapid Growth of MedTech

- · **Explosive IoT Adoption:** A surge in connected medical devices and wearables is expanding the healthcare ecosystem.
- · **Remote Care & Telemedicine:** Patients increasingly rely on virtual consultations and remote monitoring, driving new device innovations.
- · **AI & Big Data Analytics:** Advanced algorithms are powering faster, more accurate diagnoses and personalized treatments.
- · **Booming Investment & Startups:** Venture capital and tech firms are pouring resources into digital health solutions at an unprecedented rate.
- · **Integration with EHRs:** Seamless data flow between devices and electronic health records is revolutionizing patient care and workflow efficiency.

# Risks of Inadequate Security

- Patient Safety: Device tampering can lead to incorrect dosing or therapy interruptions.
- Data Breaches: PHI (Protected Health Information) is lucrative on the black market.
- Reputational Damage: Breaches erode trust in MedTech products and brands.
- Financial Impact: Legal fees, regulatory fines, and breach remediation costs can be massive.

# Device Security Risks

- Legacy Systems: Many medical devices run outdated operating systems.
- Firmware Exploits: Attackers target vulnerabilities in device firmware.
- Remote Access: IoT-enabled devices often have wireless or network connectivity that can be hacked.
- Physical Tampering: Devices in hospitals or patient homes can be accessed directly.

# Patient Data Vulnerabilities

High-Value PHI: Medical records can be sold for large sums, making patient data a prime target for cybercriminals.

Data Tampering: Altered records can lead to misdiagnoses or incorrect treatments, posing serious patient safety risks.

Ransomware Attacks: Criminals encrypt critical patient data, demanding payment for restoration and causing significant care disruptions.

Insider & Third-Party Threats: Employees, contractors, or vendors with access to sensitive data can unintentionally or maliciously compromise security.

# Key Regulation and Guidelines

HIPAA (Health Insurance Portability and Accountability Act) - Focuses on protecting the confidentiality, integrity, and availability of Protected Health Information (PHI). It imposes administrative, physical, and technical safeguards, with penalties for non-compliance.

FDA Guidelines - Emphasize a risk-based lifecycle approach for securing medical devices. Guidance spans from pre-market considerations—like secure device design and vulnerability assessments—to post-market requirements such as patch management, ongoing monitoring, and coordinated disclosure of security issues.

ISO 14971 - Details a structured risk management process for medical devices—identifying potential hazards, estimating and evaluating risks, implementing control measures, and monitoring effectiveness throughout the device's lifespan.

NIST Cybersecurity Framework (CSF) - Traditionally based on five core functions—Identify, Protect, Detect, Respond, and Recover—the draft version 2.0 proposes a sixth function, "Govern," which underscores organizational oversight of cybersecurity risks. This Framework offers best practices and a common language to guide continuous assessment and improvement of an organization's security posture.

# HIPAA & FDA Essentials

HIPAA Security Rule: Administrative, physical, and technical safeguards.

FDA Pre-Market: Cybersecurity must be considered during device design.

FDA Post-Market: Ongoing monitoring, patch management, and vulnerability reporting.

Shared Responsibility: Manufacturers, healthcare providers, and IT teams must collaborate.

# FDA Draft Guidance (2022) & Expanded Authority (2023)

The FDA's "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (draft, April 2022) emphasizes secure product development, vulnerability disclosure, and robust post-market processes.

Additionally, the Consolidated Appropriations Act of 2023 grants the FDA new authority to require specific cybersecurity measures in device submissions, reinforcing the mandate for ongoing monitoring, patch management, and incident response

Advantage.Tech

# “When it comes to medical devices, cybersecurity is patient safety. Even one small vulnerability can be the difference between harm and life-saving care.”

— Dr. Schwartz | Deputy Director of the FDA’s Center for Devices and Radiological Health

Note: This is a paraphrase reflecting statements Dr. Schwartz (Deputy Director of the FDA’s Center for Devices and Radiological Health) has made in various speeches and interviews about the gravity of cyber risks in MedTech.

# Best Practices

# Secure Development & Network Segmentation

01

**Secure Development Lifecycle:** Integrate security testing and threat modeling from the start.

02

**Patch Management:** Regular updates to address vulnerabilities promptly.

03

**Network Segmentation:** Isolate critical systems and devices from less secure areas.

04

**Least Privilege:** Grant users only the access they absolutely need.

# Encryption, Authentication & Training

**Data Encryption:** Encrypt PHI in transit (TLS/SSL) and at rest.

**Strong Authentication:** Use multifactor authentication (MFA) for both staff and device maintenance.

**Regular Security Training:** Educate employees about phishing, social engineering, and proper data handling.

**Vendor & Third-Party Management:** Assess security posture of partners and suppliers.

# Incident Response

# Preparing for Cyber Incidents

01

**Incident Response Plan (IRP):** Define roles, responsibilities, and communication pathways.

02

**Tabletop Exercises:** Simulate breaches to test readiness.

03

**Monitoring & Detection:** Use intrusion detection systems (IDS) and real-time monitoring.

04

**Legal & Regulatory Contacts:** Know your reporting obligations to agencies and affected parties.

# Recovery & Post-Incident Actions

**Containment**
Immediately isolate compromised systems to prevent further spread of malicious activity.

**Eradication**
Completely remove all malware or unauthorized access points, and apply necessary patches.

**Restoration**
Recover data from verified backups, then thoroughly test systems to confirm integrity before resuming operations.

**Post-Incident Review**
Investigate the root cause, update security policies, and integrate lessons learned into future preparedness.

**Transparent Communication**
Notify patients, regulators, and key stakeholders if PHI is compromised, ensuring compliance with legal requirements.

# Future Trends – AI & Cloud

# AI in MedTech

**AI-Driven Diagnostics**
Integrating advanced algorithms into medical imaging, remote monitoring, and predictive analytics can significantly improve patient outcomes. However, these AI models rely on large volumes of high-quality data—ensuring **accurate and secure data inputs** is crucial to avoid misdiagnosis or bias.

**Data Poisoning Attacks**
Malicious actors can insert tampered or false information into the data pipeline, causing AI models to produce unreliable or harmful results. **Preventing unauthorized alterations** of training and validation datasets is key to maintaining the integrity of AI-enabled solutions.

**Model Confidentiality**
Proprietary algorithms are often the competitive edge in MedTech AI. **Protecting intellectual property** from theft or reverse-engineering safeguards an organization's innovations and prevents adversaries from exploiting model weaknesses.

**Continuous Validation**
AI models must be monitored and retrained periodically to ensure they still perform accurately and securely. **Regular audits** help catch data drift, potential vulnerabilities, and emerging attack vectors—keeping AI applications both effective and safe.

# Cloud Security

**Shared Responsibility Model:** Cloud providers secure the infrastructure; you secure data and applications.

**Encryption & Key Management:** Control your own encryption keys where possible.

**Regulatory Compliance in the Cloud:** Ensure cloud services meet HIPAA/FDA requirements.

**Scalability & Disaster Recovery:** Cloud can facilitate faster recovery if configured securely.

# Key Takeaways

**Proactive Cybersecurity:** Incorporate security from the ground up.

**Regulatory Alignment:** Understand and comply with HIPAA, FDA, and global standards.

**Ongoing Vigilance:** Regular updates, training, and incident response drills.

**Future-Ready:** Plan for AI and cloud security challenges now.

# Best Practices To Safeguard Your Data

# Information Security Process and Program

# Policies, Procedures and Information Security Program Consulting


EXTERNAL CISO
ADVISORY SERVICES

STAFF
AUGMENTATION

# Risk Analysis and Assessment/Testing


## Security Risk Assessments

- NIST 800-53

## Vulnerability Scans

- NESSUS

## Penetration Testing

# Sector Specific Enforcement

## Legal risk

- Office for Civil Rights (OCR) Investigations
- State AG enforcement
- Congressional investigations
- Class Action lawsuits

# Risk assessment

National Institute of Standards and Technology

- The National Institute of Standards and Technology (NIST) released a voluntary methodology to assess and reduce cyber risks in *critical infrastructure* sectors. It was updated in 2017.
- Your security program should be proportional to the data you handle and the size and nature of the business.

# Vulnerability assessment

## NIST recommends that you:

- Perform a company-wide vulnerability assessment
- Implement a comprehensive information security program
- Review your program periodically
- Implement data security policies, like data classification, password strength, access control, encryption, data disposal, and patch management
- Implement an incident response plan

# Difference between Penetration Testing and Vulnerability Assessment?

*Vulnerability Assessment:*

- Typically is general in scope and includes a large assessment.
- Predictable. ( I know when those darn Security guys scan us)
- Unreliable at times and high rate of false positives. (I’ve got a banner)
- Vulnerability assessment invites debate among System Admins.
- Produces a report with mitigation guidelines and action items.

*Penetration Testing:*

- Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
- Unpredictable by the recipient. (Don’t know the “how?” and “when?”)
- Highly accurate and reliable. (I’ve got root!)
- Penetration Testing = Proof of Concept against vulnerabilities.
- Produces a binary result:  Either the team owned you, or they didn't.

# Scope of Penetration Testing

### Targeted Recon.

- Targeted exploitation of vulnerable software.

### Social Engineering

- Hi HelpDesk...I'm Mr. Jones...Can you tell me what my password is?

### Physical facilities audit

- Hmm, I forgot my badge... but there's 200 yards of fence missing on the east side of the center

### Wireless War Driving

- Detection of rogue or weakly encrypted AP's.

### Dumpster Diving

- How much fun can I have in the dumpster...whoops...I've found someone's Tax forms with SSN.

# Why Bother?

Active pen-testing teaches you things that security planning will not

- What are the vulnerability scanners missing?

Are your users and system administrators actually following their own policies?

- host that claims one thing in security plan but it totally different in reality
  - Audit Physical Security
- Just what is in that building no one ever goes in?
- The strongest network based protections are useless if there is a accessible unlocked terminal, unlocked tape vault, etc.

Raises security awareness

- I better not leave my terminal unlocked because I know that those security guys are lurking around somewhere.

Helps identify weakness that may be leveraged by insider threat or accidental exposure.

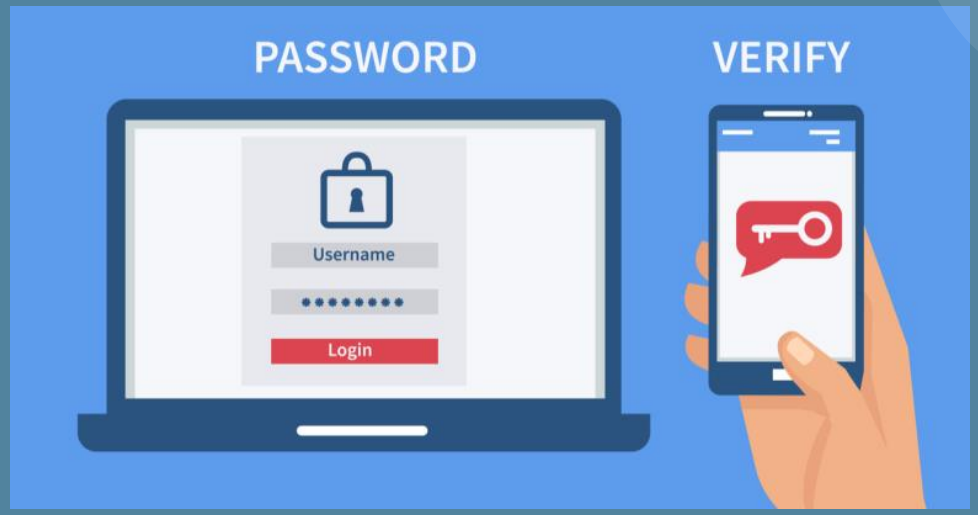
Provides Senior Management a realistic view of their security posture

Great tool to advocate for more funding to mitigate flaws discovered

If I can break into it, so could someone else!

# Authentication and Authorization

- Two factor or multi-factor authentication
  - Password and PIN
  - Biometrics
- Password managers
- Group Policies
  - Enforce “Least Privileges” rule




SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

# How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

| Number of characters | Lowercase letters only | At least one uppercase letter | At least one uppercase letter +number | At least one uppercase letter +number+symbol |
|---|---|---|---|---|
| 1 | Instantly | Instantly | - | - |
| 2 | Instantly | Instantly | Instantly | - |
| 3 | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 1 min | 6 min |
| 8 | Instantly | 22 min | 1 hrs | 8 hrs |
| 9 | 2 min | 19 hrs | 3 days | 3 wks |
| 10 | 1 hrs | 1 mths | 7 mths | 5 yrs |
| 11 | 1 day | 5 yrs | 41 yrs | 400 yrs |
| 12 | 3 wks | 300 yrs | 2,000 yrs | 34,000 yrs |

Source: Security.org

statista

# Passwords. Keep them strong, private, and don’t reuse them

Protect your accounts and passwords

- Make passwords strong (still needed)
- Keep them private (don’t share among users)
- Use unique passwords for different websites (NO PASSWORD REUSE)
- Limit use of employees using corporate e-mail accounts as their identifier on third-party website

# Change and Configuration Management

- Automation of configurations
  - Security Automation
- Patch management / automatic updates
- Change management software

# Threat Management

- Endpoint protection
  - Anti-virus
  - Spam filtering
  - Encryption
- Firewall
- Content Filtering
- Backup / Disaster recovery


It’s OK,
You have a good backup, right?

# Proper Backup Procedure

- Choose your application
- Scheduling
- Implementation
- Inventory (content and media)
- Verify
- Automate
- Secure

# Evolution of Security

Where most commercial companies want to be

**SOC as a Service plays here**

Where most commercial companies are today.

GAP

## Basic

Passwords / AD

Patch Management

Backups

## Perimeter

Firewalls

SPAM / Web Filters

WAF/Proxy

## Defense-in-Depth

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS/IPS/CASB

## Detection And Response

Log Aggregation & Correlation

Human / Threat Intelligence

Incident Detection & Response

## Containment and Remediation

Intrusion Containment

Remediation

Policy Update

**Prevention is not enough…**

# What is the evolution?

NIST

**53%** cost per incident is spent in detection and response

**240** days to detect a security incident

**46** days to respond to security incident

## 1 Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

## 2 Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

## 3 Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

## 4 Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

## 5 Recover

- Recovery Planning
- Improvements
- Communications

Requires People & Time

# Security Positions in the US are a Challenge:

Talent is very expensive with familiarity building a SOC (Security Operations Center)

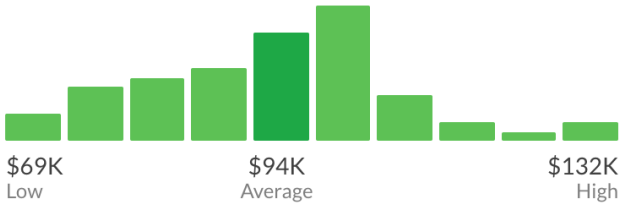
## Senior Information Security Analyst Salaries

1,485 Salaries  Updated Jul 13, 2018

Industries | Company Sizes | Years of Experience

Average Base Pay

**$94,344** /yr




Additional Cash Compensation

| | |
|---|---|
| Average | $6,291 |
| Range | $1,223 - $16,981 |

**How much does a Senior Information Security Analyst make?**
The national average salary for a Senior Information Security Analyst is $94,344 in United States. Filter by... More

## Information Security Architect Salaries

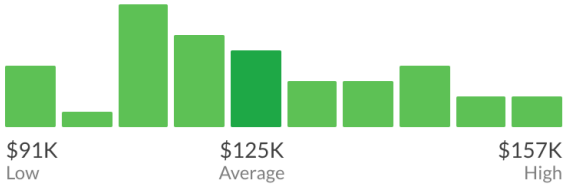
307 Salaries  Updated Jun 5, 2018

Industries | Company Sizes | Years of Experience

To filter salaries for Information Security Architect, Sign In or Register.

Average Base Pay

**$124,637** /yr

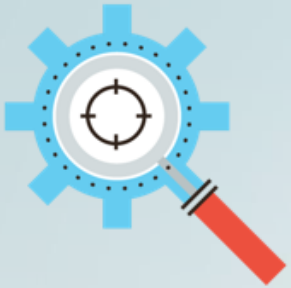



Additional Cash Compensation

| | |
|---|---|
| Average | $xx,xxx |
| Range | $xx,xxx |

**How much does a Information Security Architect make?**
The national average salary for a Information Security Architect is $124,637 in United States. Filter by... More

# Solution: SOC-as-a-Service



## Comprehensive

Unified Security with centralized view

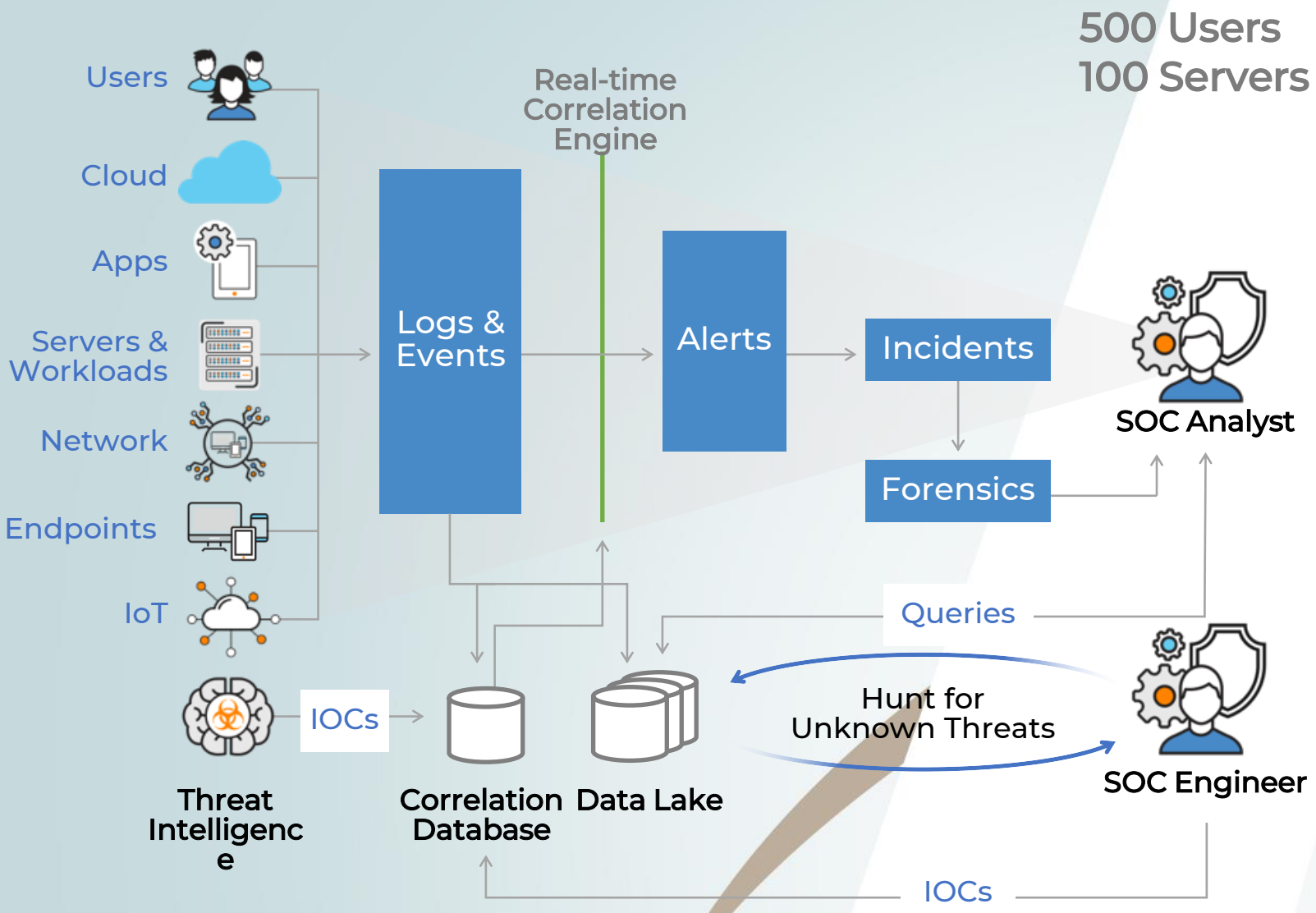
## 24x7 Monitoring

Focused on Managed Detection and Response

## Predictable Pricing

Fixed monthly price faster, better, cheaper

# Backend Process




500 Users
100 Servers

~600M+ Observations/Week
~700-1000 Investigations/Week
**~1-5 Incidents/Week**

## Real-time Correlation

- Analyze billions of events
- Real-time correlation against IOCs
- Reduced false positives

## Forensics

- Search and research quickly
- Construct blast zone analysis and remediate

## Hunt

- Hunt for unknown threats with deep analytics and machine learning
- Identify new IOCs to improve monitoring

I finally realized it.
People are **prisoners**
of their phones,
that's why they are
called **cell** phones.

Spirit Science

# Q & A

advantage
TECHNOLOGY