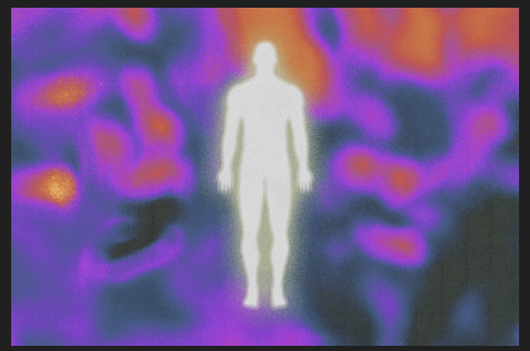
CYBERSECURITY PRESENTATION



Computer Vision for Healthcare

74921 59300 4 18863 70782 0

AGENDA

TOPICS COVERED

- Risk Assessment
- Threat Modeling
- Network & Data
- Third-party Risk
- Business Continuity
- Incident Response

PEOPLE

Back to Agenda Page

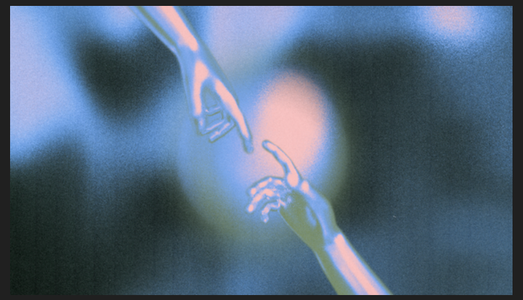
VISION

- 200 Bay Area Employees
- Numerous vendors and contractors
  - Maintenance
  - Infrastructure
- 24h cybersecurity monitoring team in India

Client

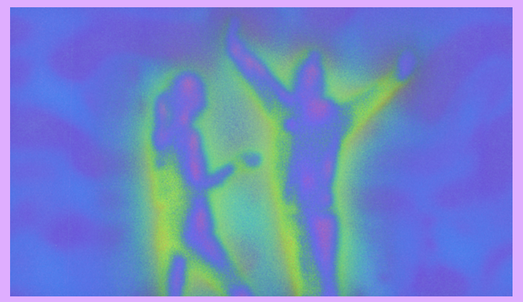
- 60,000 employees globally
- Technicians, nurses, doctors, admin staff, etc.
- Dedicated lab facilities, but also clinics within partner organizations such as pharmacy and grocery chains.

TECHNO LOGY



VISION INFRASTRUCTURE

- Highly efficient infrastructure that remains secure but accessible
- Model library and AI training interface



CLIENT INFRASTRUCTURE

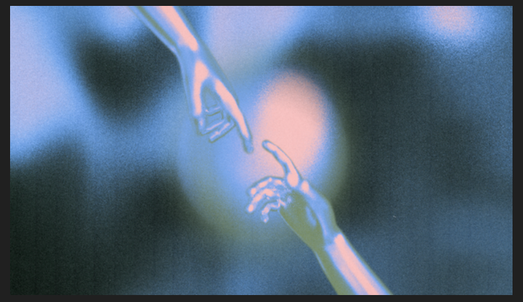
- The client has their own dedicated cloud environment
- The client provides a patient facing web app

CONSIDERATIONS

- Usage, storage, and transmission of data
- Compliance with health care regulations
- Vendor oversight

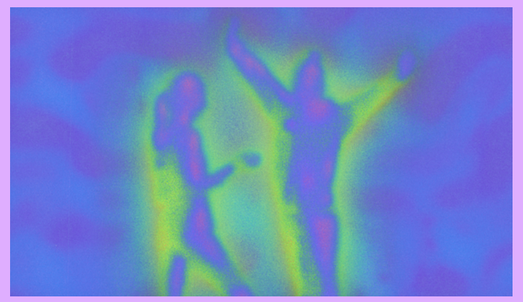
Back to Agenda Page

PROCESS



TRAINING DATA LIBRARY & MODEL LIBRARY

- Utilize a pretrained model for detection



DATA PROCESSING AND LABELING INTERFACE

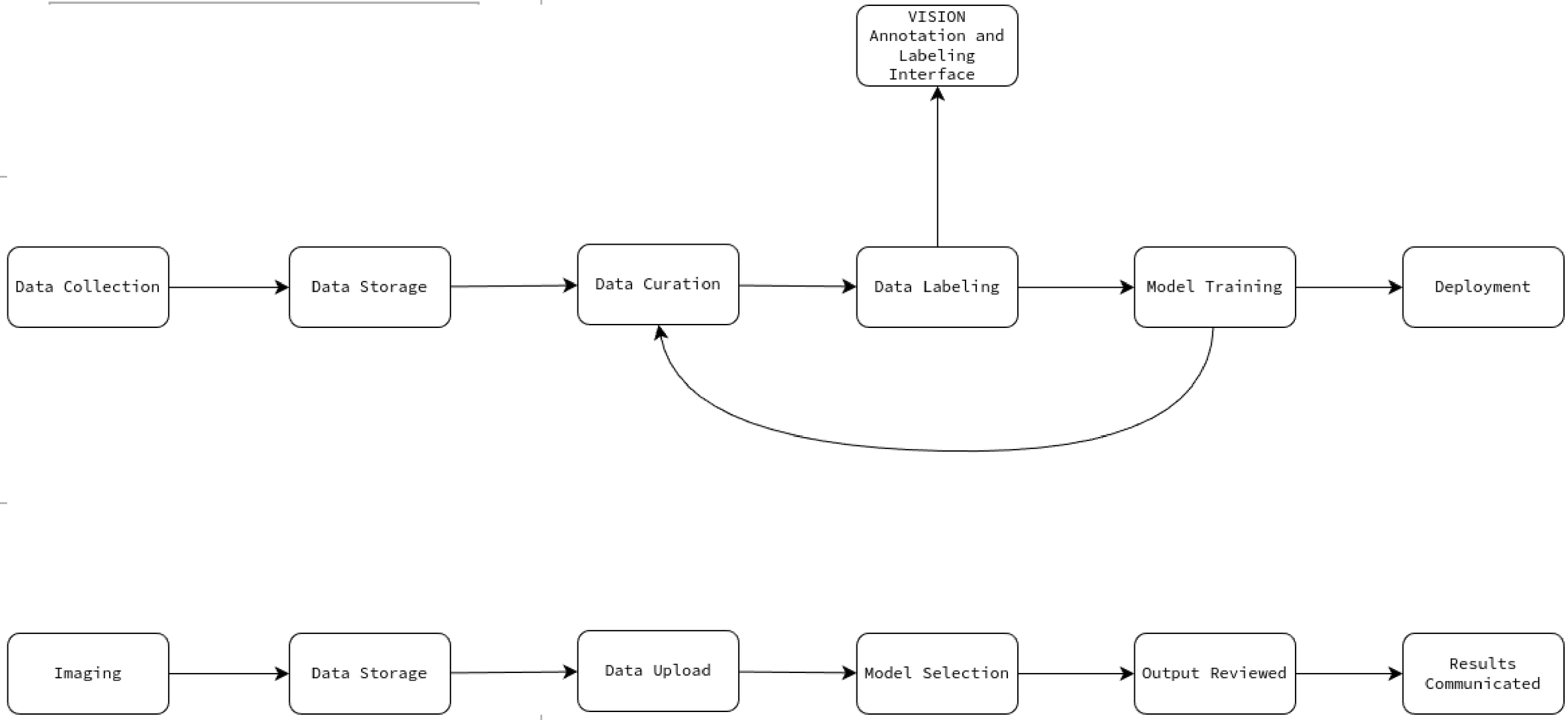
- Utilize VISION’s interface to train a custom model

CONSIDERATIONS

- Anonymize patient data
- Regulations around medical data

Back to Agenda Page

DATA FLOWS


VISION
Annotation and
Labeling
Interface
Data Collection
Data Storage
Data Curation
Data Labeling
Model Training
Deployment
Imaging
Data Storage
Data Upload
Model Selection
Output Reviewed
Results
Communicated

Risk Register					
Risk Description	Likelihood	Impact	Severity	Mitigation	Risk ID
Leak of employee or patient PII	Likely	Major	Very High	- Conduct security audits to identify and remediate vulnerabilities - Implement access controls and encryption to protect sensitive data	1
Theft of medical records or images	Moderate	Major	High	- Use anonymization techniques when storing or transferring medical data to minimize impact if a breach occurs - Enable logging and monitoring to detect unauthorized access attempts	2
Ransomware	Likely	Severe	Extreme	- Maintain offline backups. - Consider cyber insurance.	3
Leak of IP	Moderate	Significant	Medium	- Implement access controls and authorization policies (Zero Trust)	4
Inaccurate AI output sent to wrong party	Moderate	Significant	Medium	- Validate AI results - Ensure communication is tested - Encrypt and anonymize	5
Failure to comply with regulations	Unlikely	Major	Medium	- Encrypt PII and medical data at rest and in transit - Conduct regular audits	6
Insider Threat	Moderate	Major	High	- Implement least privilege - Monitor access logs and user behavior for anomalies	7

RISK REGISTER

Back to Agenda Page

0012 7482901 2744103 0592346 8774510 7255

Back to Agenda Page

PATIENT DATA

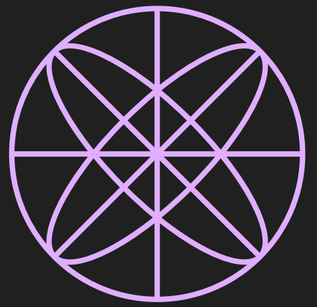
Highly regulated medical data and sensitive personal information

IP

VISION’s intellectual property should be protected to maintain competitive advantage

CORE SYSTEM

Confidentiality and availability are of outmost importance

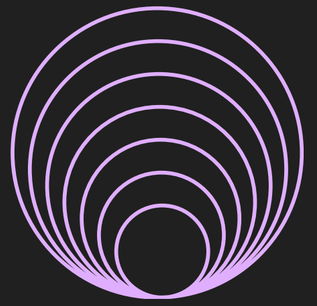


0012 7482901 2744103 0592346 8774510 7255

Back to Agenda Page

VULNERABILITY MANAGEMENT

Perform regular vulnerability scans on all systems and infrastructure. Remediate any critical or high severity vulnerabilities.

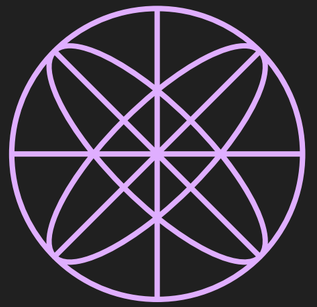


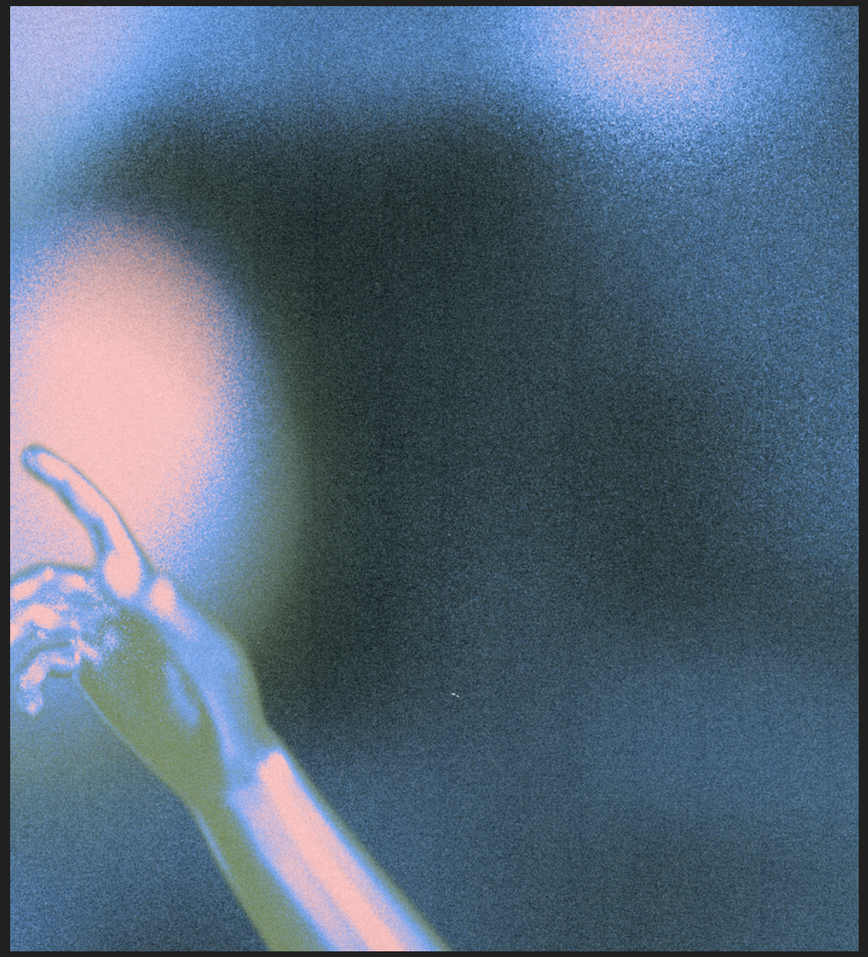
PENETRATION TESTING

Conduct annual penetration tests on all external facing systems and infrastructure.

LOGGING & MONITORING

Send logs from all systems to a central SIEM for analysis and correlation. Subscribe to threat intelligence feeds to stay up to date

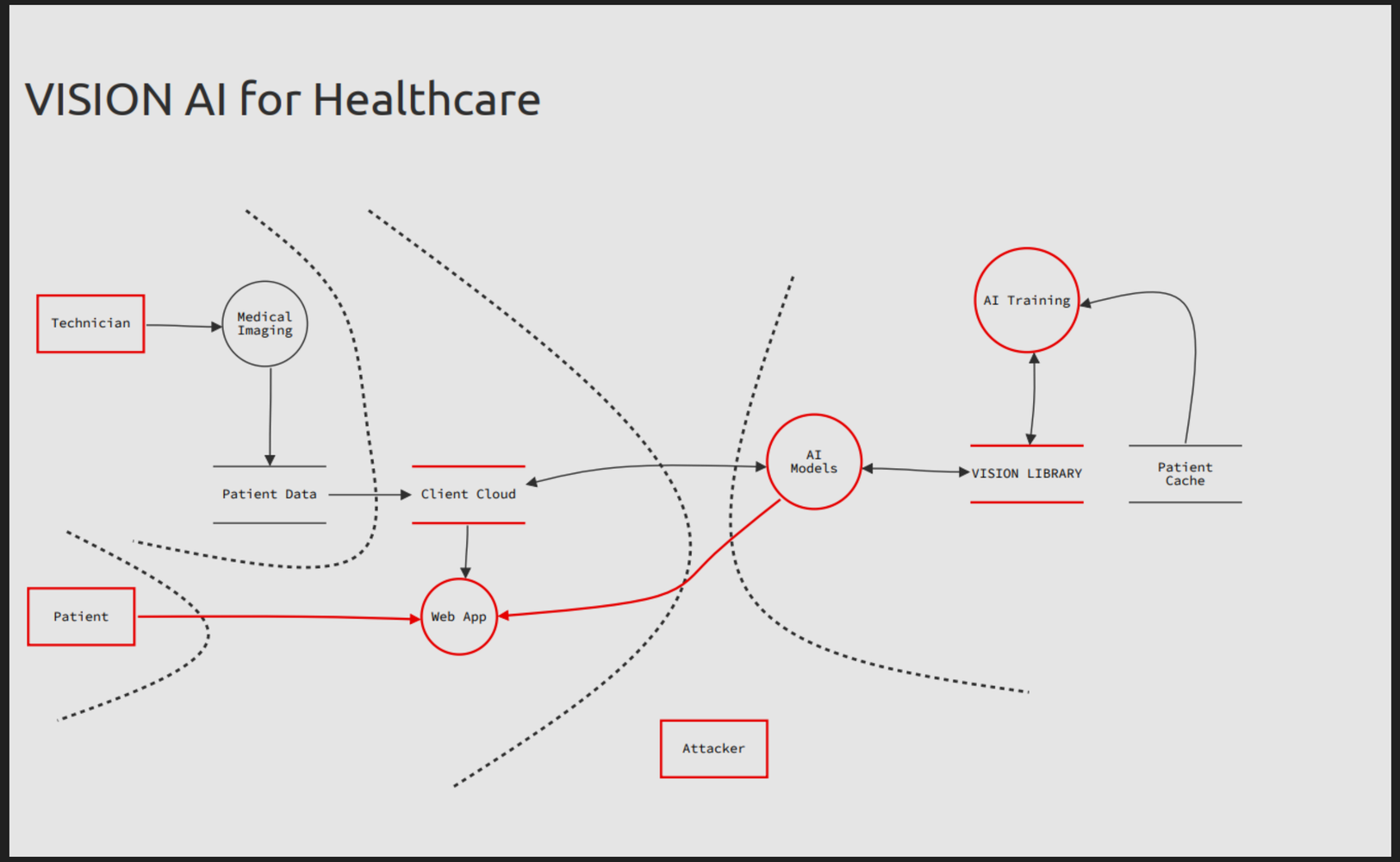




Back to Agenda Page

RECOMMENDATIONS

- Strengthening data privacy protections and compliance with healthcare regulations
- Isolating client data environments from VISION systems
- Hardening cloud infrastructure and continuously monitoring for threats
- Securing AI model training pipelines and outputs
- Encrypting data transfers and authenticating recipients
- Enforcing MFA and least privilege access controls
- Physical security for facilities and proper disposal of old equipment
- Business continuity through redundancy, backups, and disaster recovery testing



STRIDE Threat Model:

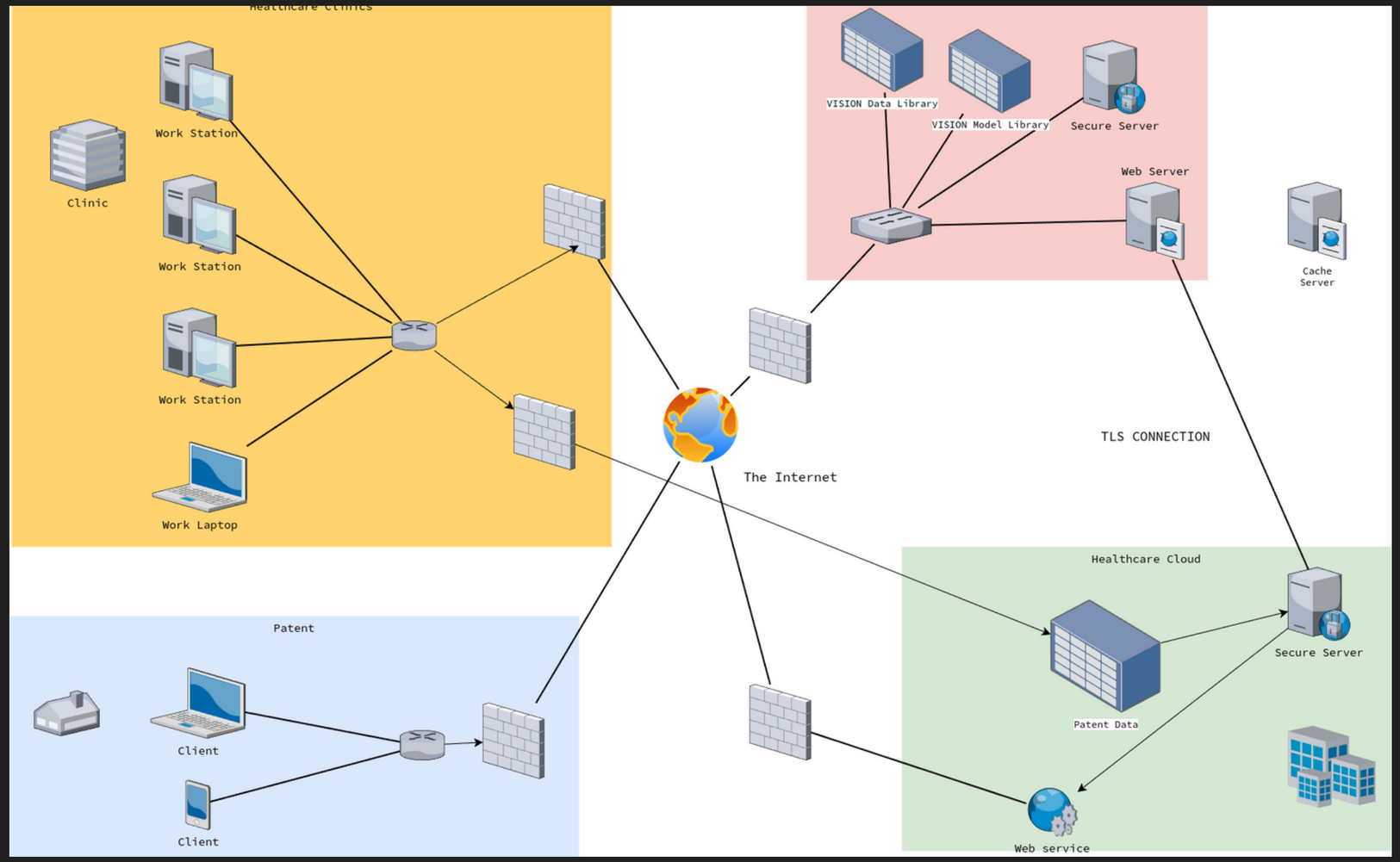
Spoofing
Tampering
Repudiation
Information Disclosure
Elevation of Privilage

An iterative process used with the risk register to identify threats within a proposed architecture

RECOMMENDATIONS

- Implement multi-factor authentication for all user and system accounts to prevent spoofing.
- Enforce principle of least privilege through role-based access controls.
- Rotate credentials regularly to limit impact of compromises.
- Encrypt all network traffic with TLS to prevent data exposure.
- Authenticate all connections internally to prevent spoofing.
- Implement firewall rules and network segmentation to limit mobility.
- Encrypt data in transit and at rest to prevent exposure.
- Use immutable data stores for sensitive data like models and training data.
- Implement robust logging and monitoring to detect tampering.
- Harden systems by removing unnecessary services, closing open ports, and keeping software patched.
- Implement intrusion detection and prevention systems to detect attacks.
- Perform regular vulnerability assessments and penetration testing.

Back to Agenda Page



Network Diagram:
A map of the network infrastructure and interactions

Security Concerns:

- Secure Data Transfer
- Data Storage and Access control
- Data retention and Disposal
- Compliance
- Secure Communication
- Data Segregation and Isolation

RECOMMENDATIONS

- Implement strong access controls
- Keep systems and software up-to-date
- Secure the network perimeter
- Encrypt sensitive data
- Monitor, log, and analyze activity
- Provide security training
- Maintain tested backups and incident response plans
- Work with qualified security partners

Back to Agenda Page

THIRD-PARTY RISK

Third-Party Risk Register					
Risk Description	Likelihood	Impact	Severity	Mitigation	Risk ID
Algorithm Bias	Unlikely	Severe	High	Continuously test models and algorithms for bias. Create an ethics review board.	1
Cloud Cost Escalation	Moderate	Major	High	Monitor usage regularly and optimize costs. Utilize platform agnostic configuration to make migration possible if necessary.	2
Cloud Outage	Unlikely	Major	Medium	Use multiple cloud providers. Replicate data across availability zones.	3
Data Breach	Moderate	Major	High	Harden security posture. Implement multi-factor authentication. Perform penetration testing.	4
Supply Chain Exploit	Likely	Significant	High	Proper due diligence should be conducted to validate these vendors.	5
Non-compliance	Moderate	Significant	Medium	Appoint Data Protection Officer. Implement mandatory data privacy training.	6
Privacy Violations	Unlikely	Major	Medium	Classify data by sensitivity. Limit access to PII data. Implement encryption and data masking.	7

Risk Mitigation Strategies

- Establish a vendor risk management program for due diligence and monitoring
- Include service level agreements (SLAs) and security requirements in contracts
- Conduct regular vendor audits and site visits
- Maintain business continuity plans for vendor failure scenarios
- Require cyber insurance coverage for vendors handling sensitive data
- Diversify vendors to avoid concentration risk
- Implement controls like encryption for data shared with vendors

INCIDENT RESPONSE

Back to Agenda Page

Scope

- Systems, networks, data, and personnel.
- Incidents resulting from malware, unauthorized access, insider threats, and accidental data exposure.

Goals

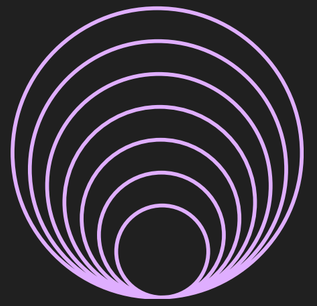
- Detect incidents early and contain them quickly
- Minimize loss or theft of data or disruption of services
- Recover damaged systems and data to restore normal operations
- Learn from incidents and improve defenses and response capabilities

0012 7482901 2744103 0592346 8774510 7255

Back to Agenda Page

DETECTION & ANALYSIS

- Determine scope and root cause of incident.
- Monitor antivirus, firewall, and intrusion detection logs for signs of malware or unauthorized access.

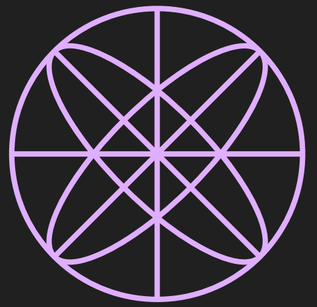


COMMUNICATION PLAN

- Contact CIO and CISO immediately via call/text
- CISO will alert incident response team members
- IT Manager will communicate status to affected departments

CONTAINMENT

- Isolate infected systems
- Block suspicious IP addresses
- Disable compromised user accounts
- Prevent encryption of additional files if ransomware



0012 7482901 2744103 0592346 8774510 7255

Back to Agenda Page

ERADICATION & RECOVERY

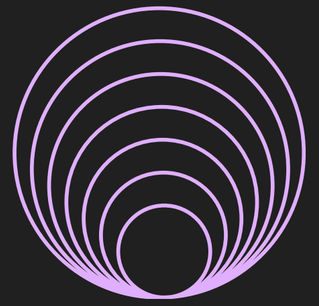
- Wipe and reimage infected systems
- Restore data from backups
- Change passwords and credentials
- Scan restored systems and data

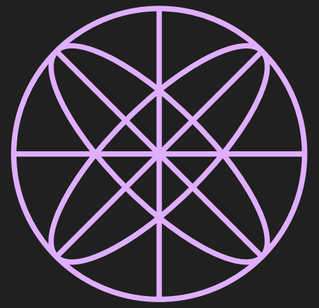
POST-INCIDENT

- Document details of incident
- Review circumstances that led to incident
- Implement additional monitoring or controls to prevent re-occurrence
- Provide updated training to personnel

TOOLING

Firewalls, IDS, IPS, SIEM, EDR, Antivirus, proxy server, VPN, Ticketing, Threat intelligence, Forensic tools, Immutable backuos, cold backups





BUSINESS CONTINUITY

Back to Agenda Page

Top Business Disruptions

- Data breach
- Service outage
- Intellectual property theft
- Non-compliance fines
- Vendor negligence

0012 7482901 2744103 0592346 8774510 7255

Back to Agenda Page

BACKUP STRATEGY

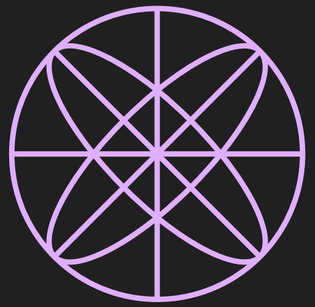
- Database backups will be performed daily.
- Application code stored in version control
- User files and applications backed up weekly

RECOVERY STRATEGY

- Restore data from recent clean backups
- Thorough testing and validation of backups

MONITORING

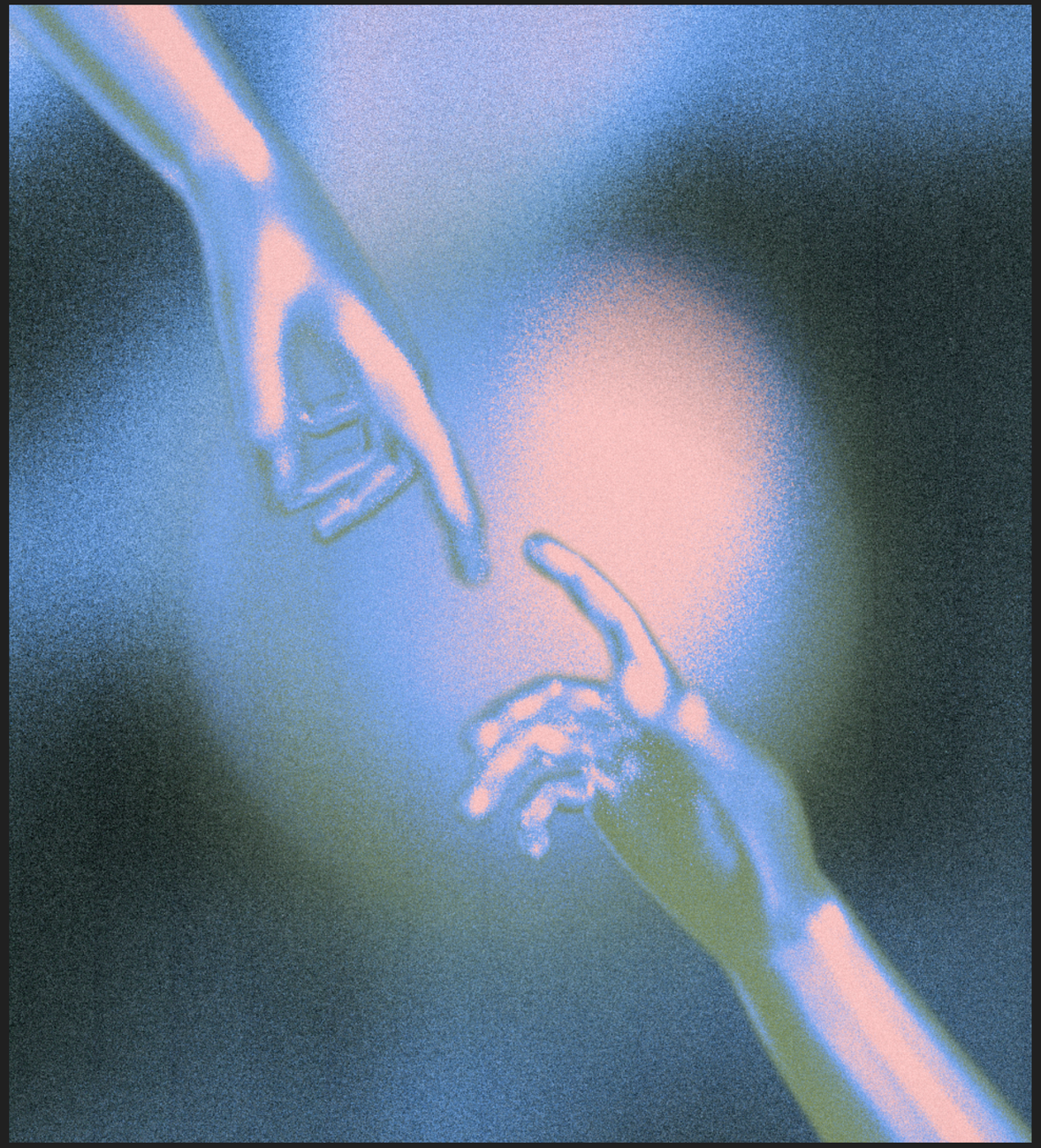
- Backup jobs will be monitored for success/failure.
- Backup failures will trigger alerts.
- Server health monitoring will be implemented to detect system failures.



RECOMMENDATIONS

Back to Agenda Page

- Conduct a risk assessment and business impact analysis to identify critical business functions and processes. Assess potential disruptions and impacts.
- Develop resilience strategies such as redundancy, backup systems, and alternative arrangements to maintain continuity of critical operations.
- Create detailed response and recovery plans outlining actions to take during disruptions. Maintain and test these plans.
- Implement backup systems and procedures for data, code, and other assets. Test backup recovery regularly.
- Incorporate lessons learned from real disruptions into future continuity planning.
- Coordinate with partners and vendors on aligned continuity strategies.
- Provide training and ensure staff understand their roles in continuity plans.



THANK YOU!

HACK THE PLANET!