KONICA MINOLTA

Giving Shape to Ideas

BUILDING AN EFFECTIVE INCIDENT RESPONSE PLAN

FOR

HYPOTHETICAL HEALTHCARE, INC.

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

AGENDA

- Overview / Purpose / Scope
- NIST Incident Response Guidelines
- Playbooks
- Incident Response Tabletop Test
- Incident Response – Lessons Learned
- Take Home

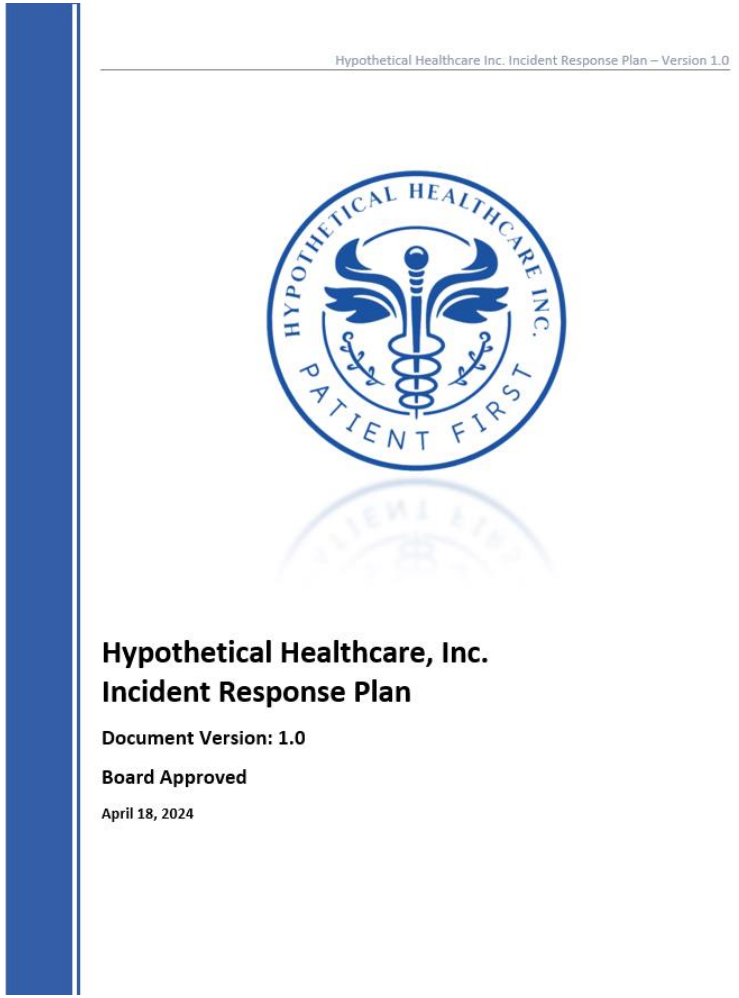
All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Overview

The Incident Response Plan (IRP) **establishes a protocol to respond to information security incidents** that pose a threat to the privacy of confidential and /or sensitive information for the organization and its customers.



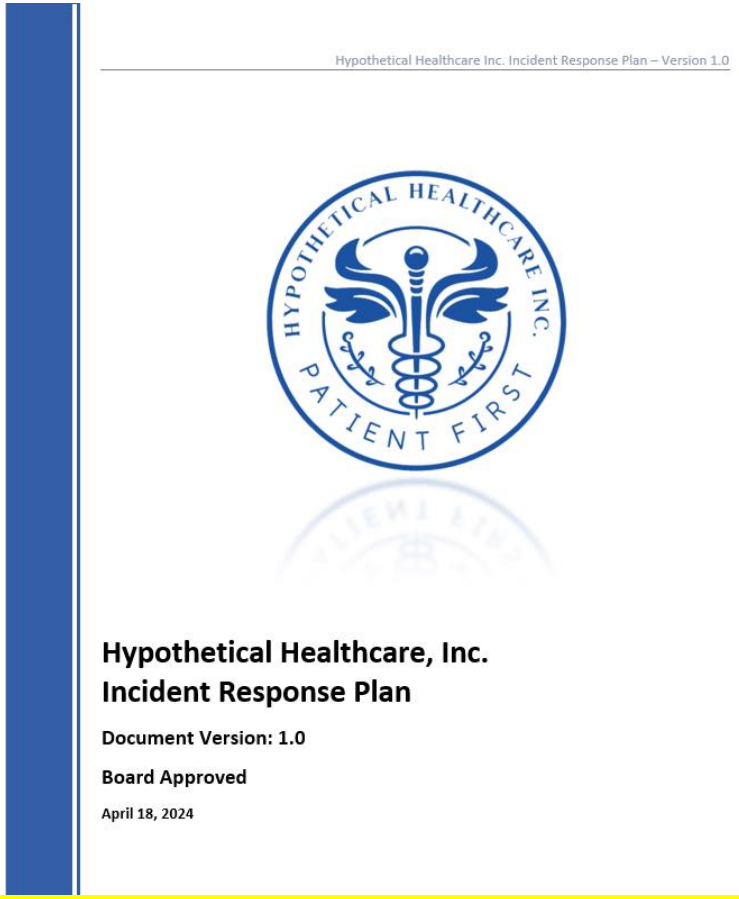
All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA | Giving Shape to Ideas

Purpose

The IRP **should clearly define the incident handling process and procedures** used by the organization to respond to threats to ensure the protection of organizational and customer information.

It **should be used to respond to any type of detected security incident** that compromises physical or digital information.



Types: cybersecurity attacks | social engineering attacks | internal theft of information | virus/malware intrusion | data breaches | attack on critical medical devices |overt unauthorized access to organizational physical sites or datacenters.

All Covered
IT SERVICES FROM KONICA MINOLTA

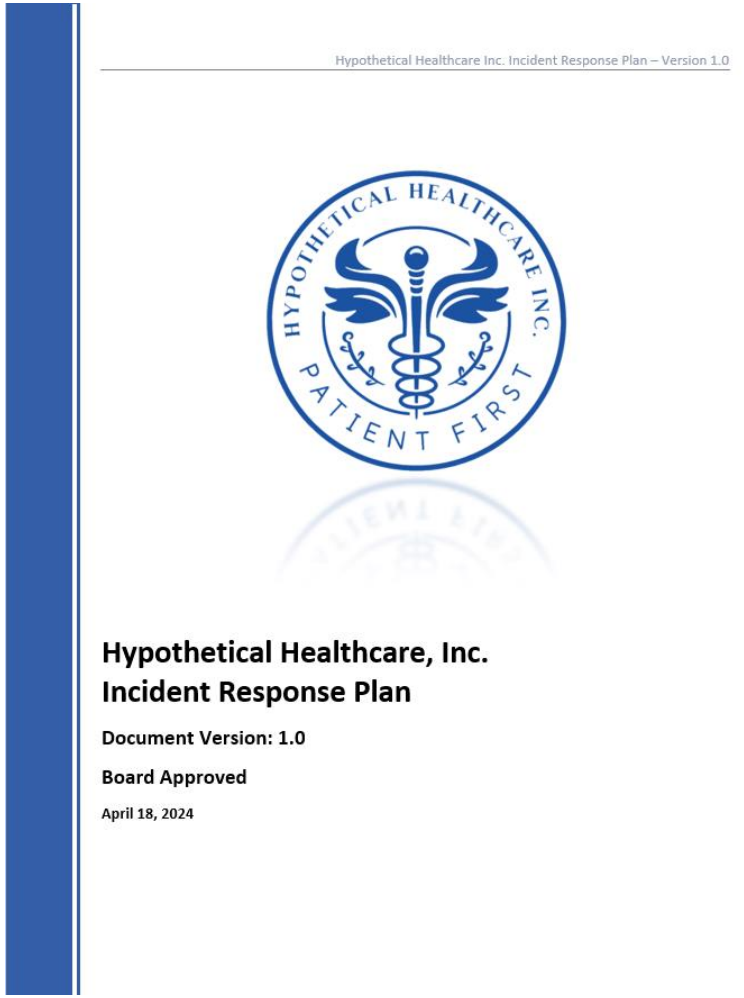
KONICA MINOLTA

Giving Shape to Ideas

Scope

The IRP applies to all information assets that are protected within the organization system boundary including:

- Protected Health Information (PHI) and electronic protected health information (e-PHI) assets
- Company-owned assets and/or
- Assets contracted for use through third-party service providers



All Covered
IT SERVICES FROM KONICA MINOLTA

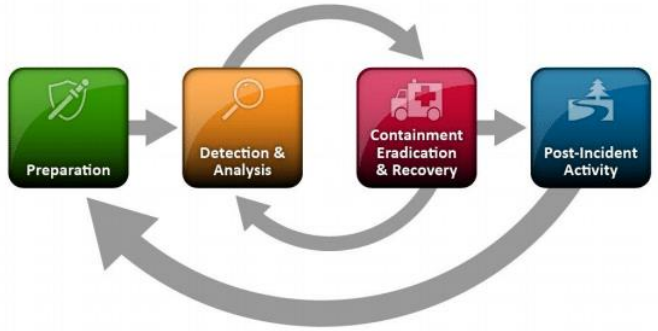
KONICA MINOLTA | Giving Shape to Ideas

NIST Incident Response Guidelines

NIST Cybersecurity Framework v2.0

National Institute of Standards and Technology

NIST SP 800-61, Computer Security Incident Handling Guide



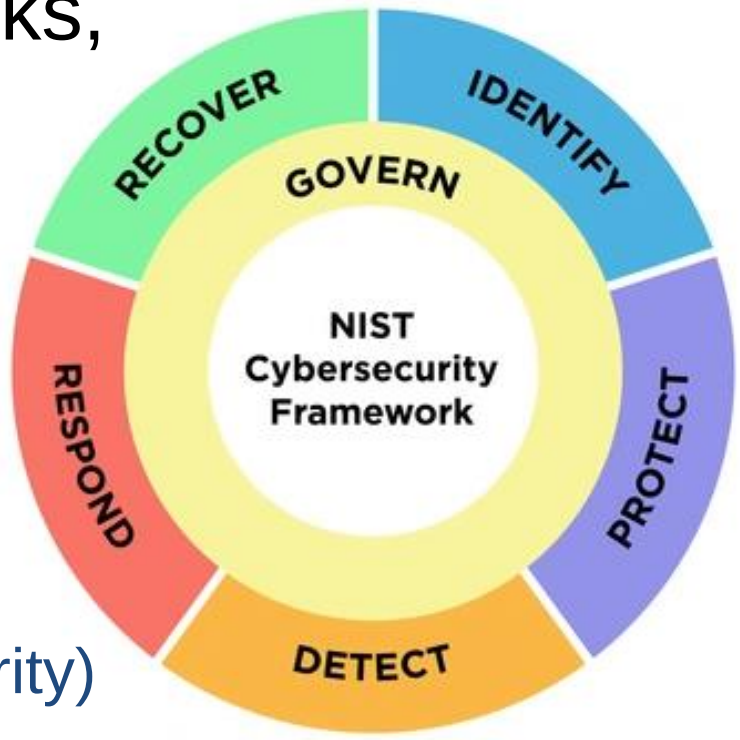
All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA | Giving Shape to Ideas

NIST Incident Response Guidelines

NIST Cybersecurity Framework v2.0

helps organizations manage cybersecurity risks, understand, assess, prioritize, and communicate its cybersecurity efforts.



Features:

- 6 Functions / 22 Categories / 106 Subcategories
- Current Profile (helps identify current security posture)
- Target Profile (helps identify where you want to be)
- 4 Tiers (i.e., helps identify how risk are managed / maturity)

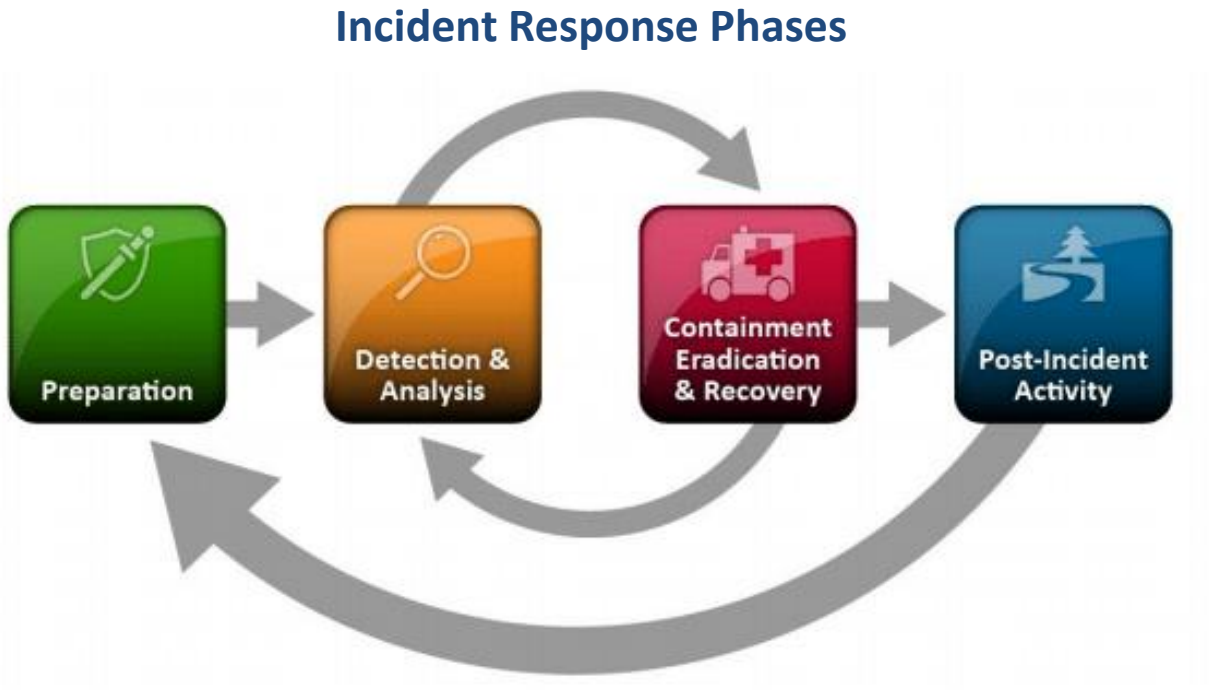
Information Security | Incident Response | Business Continuity / Disaster Recovery | Third-Party Risk Management

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA | Giving Shape to Ideas

NIST Incident Response Guidelines

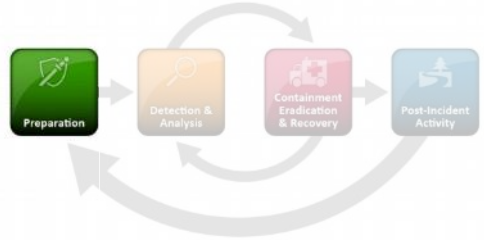
NIST SP 800-61, Computer Security Incident Handling Guide helps organizations provides establish an incident response capability to detect and resolve information security incidents that may have an impact on physical or electronic information.



All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA | Giving Shape to Ideas

Planning and Preparation



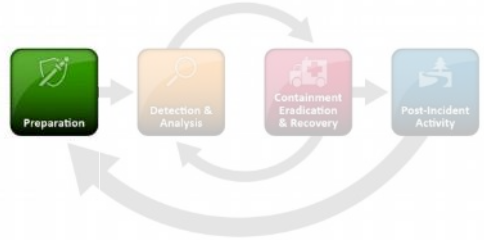
The NIST Incident Response methodology emphasizes preparation to…

- **establish an incident response capability** so that the organization is ready to respond to incidents

- **prevent incidents** by ensuring that systems, networks, and applications are sufficiently secure.

KONICA MINOLTA | Giving Shape to Ideas

Planning and Preparation



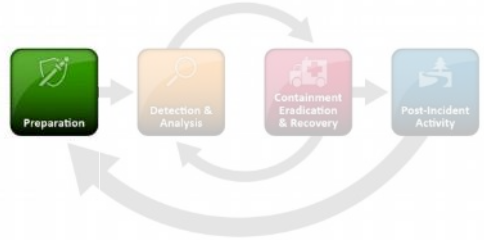
Building an effective Incident Response capability involves:

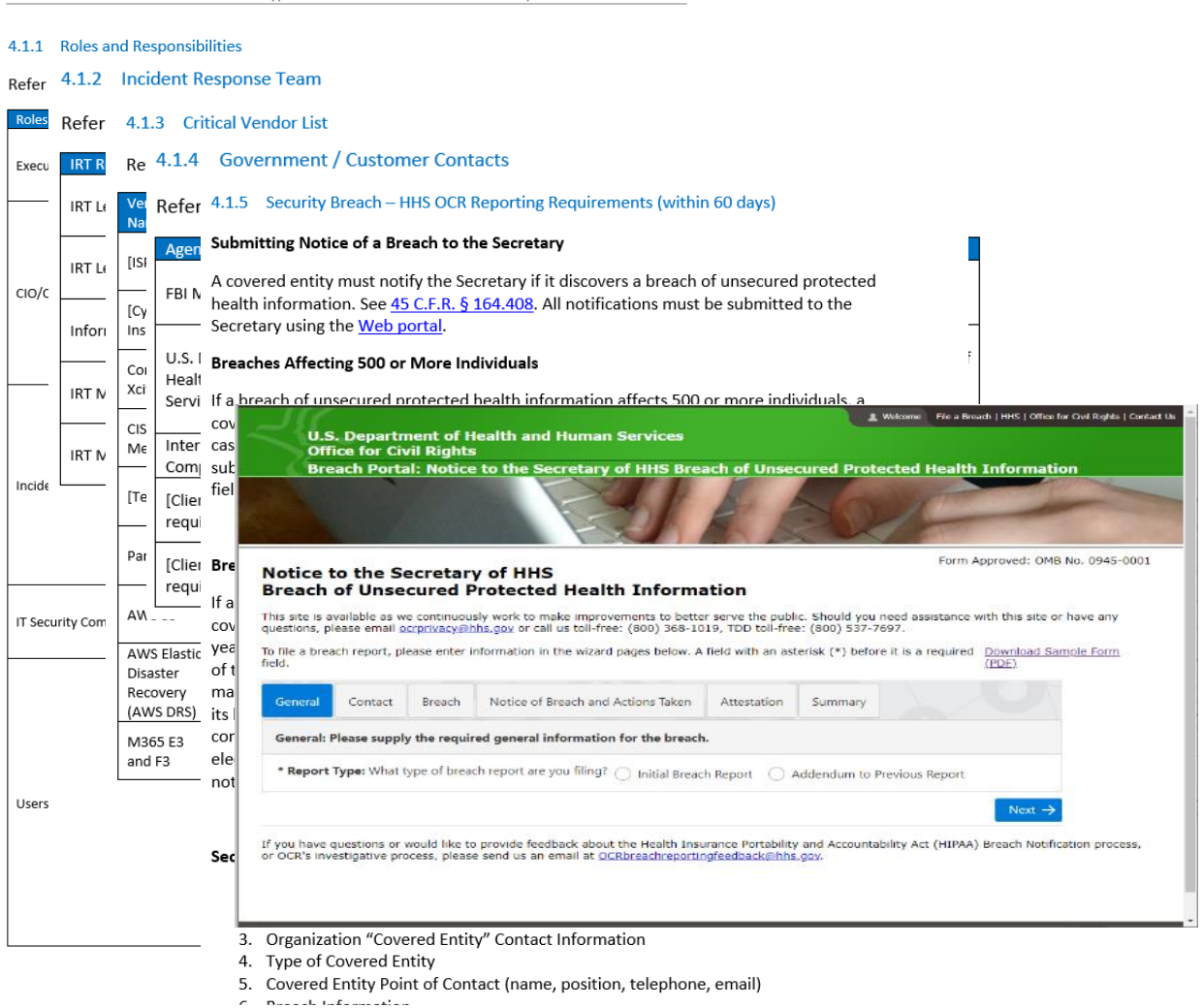
- Policy, Plan, Procedures, and Playbooks
- Security Risk Assessments
- Employee Security Awareness Training
- Incident Response Testing

KONICA MINOLTA

Giving Shape to Ideas

Planning and Preparation





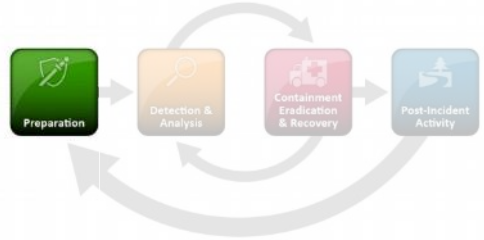
Incident Response Plans consider:

- Roles and Responsibilities
- Incident Response Team
- Critical Vendors
- Government / Customer Contacts
- Incident / Breach Reporting
- Preventive Measures

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA | Giving Shape to Ideas

Planning and Preparation



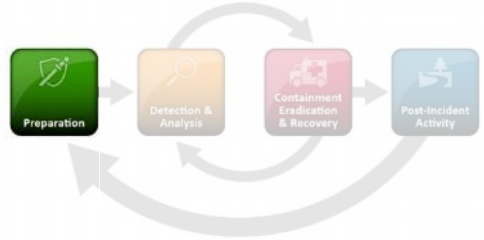
IR Plans should consider **Preventive Measures**:

- **Incident Response Testing:** Periodically test the plan to identify the vulnerabilities and risks, determine lessons learned, and enhance security measures.
- **Third-party Testing:** Penetration Testing and Vulnerability Scanning
- **Host and Network Security:** Hosts are hardened to standard configurations. Perimeter firewalls are configured to “deny-all” with “permit-by-exception” for identified services/connections (e.g., VPN, dedicated connections).
- **Malware Prevention:** Endpoint Detection Response (EDR) and Security Information and Event Management (SIEM) capability.
- **User Awareness Training**: All users receive awareness training on security policies and procedures including common threat tactics (e.g., phishing) and insider threat. Training is conducted during onboarding and annually as a refresher.

KONICA MINOLTA

Giving Shape to Ideas

Planning - Playbooks



5 Playbook Scenario

5.1 Cybersecurity Incident

5.1.1 Detection & Analysis

1. **IT Administrator** is notified tha system notification).
   - **IT Administrator** will notify
   - If DDoS occurs, **IT Administ**
2. **Notify SOC. IT Lead** will coordi
   a. SOC Contact Information -
   b. The SOC initiates Incident I

   Ensure the following is ide
   - Assigned SOC point of
   - Established communica (e.g., hourly)
   - Established clear path t
   - Root Cause Analysis up
3. **Contact Cyber Insurance Provi** to provide investigation assista

   Contact information below:
   - [Name of Cyber Insurance]
   - Email:
   - Toll free:

   Please include the following in
   - Policy Number:
   - Your Contact Information:
   - Brief Incident Description:
   - Insured by:
   - Policy Number:
   - Insurance Carrier:
   - Effective Date:
4. **Establish IRT Communication**
5. **Identify type of event.** The **IRT** collaborates with the **SOC** to analyze root cause and identify the

Event Type
Ransomware
Virus/Malware
Zero-day Attacks
Distributed Denial of Service
Physical Incident

5.1.2 Containment & Eradication

1. **The SOC investigates the incident in accordance with the SLA**. The **SOC** remains in contact with **IRT** until incident resolution.
2. **Determine Next Steps.** The **IRT** collaborates with **SOC** to conduct appropriate steps to contain and remediate the incident.
3. **Redirect services during disruption**. The **IRT Lead** redirects management and staff to alternative servers and/or services during the incident disruption.
   - If main servers are down, redirect users to appropriate cloud services during disruption.
   - **IT Administrator** reviews backup/restore procedures for affected system or specific users affected.
4. **Preserve forensic evidence**. IT Administrator may need to preserve forensic evidence depending on the extent of the incident.
   - The Insurance Company or Third-Party Forensics may have guidance
   - The SOC will need to provide information and potential access to SIEM logs as needed.
5. **Determine notification necessary.** IRT must determine the customer notification, government authority notification, insurance company and attorney notification are necessary, based on initial findings through identification, analysis, containment, and remediation/eradication steps.
   - Necessary personnel identify the initial source of the breach.
   - Necessary personnel documents the facts of the incident.
   - Necessary personnel contact the appropriate parties required.
   - If data is compromised, refer to section 4.1.5 Security Breach – HHS OCR Reporting Requirements (within 60 days), and Appendix C.

5.1.3 Recovery

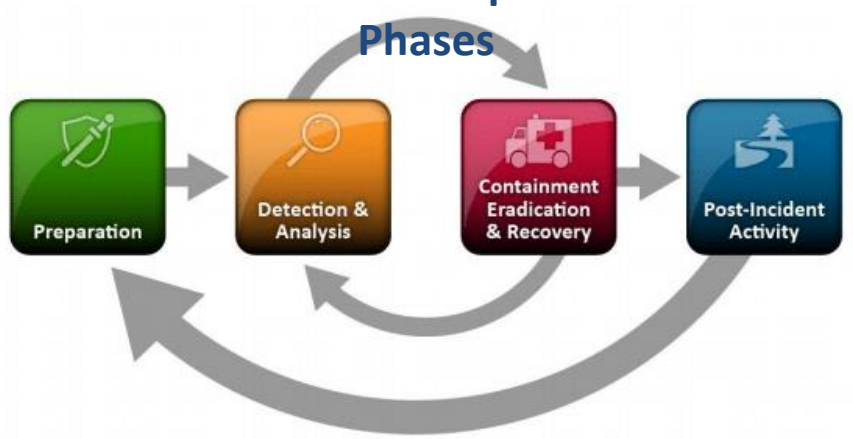
1. **Restore services. IT Lead** coordinates with recovery service provider (i.e., service provider) to restore lost data, servers, and file shares once remediation has taken place.
2. **Verify services are restored.** IRT verifies that containment, remediation/eradication, and recovery efforts are complete, and systems are operating satisfactorily.
3. **Verify Building Security System is operational.** IRT Facilities/Operations will ensure security systems are working for physical security…

5.1.4 Post-Incident Activity

1. **Document the incident.** The **IRT**, in conjunction with the SOC, conducts a reasonable investigation and documents the incident on the Incident Response Form, attaching as much supporting documentation as possible to allow for a full analysis of the source and

Playbooks document the steps used to respond to a specific scenarios using the Incident Response phases…

Incident Response Phases



All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA | Giving Shape to Ideas

Detection & Analysis

Incident detection occurs either by human observation, or through system monitoring (e.g., SIEM, IDS/IPS (Intrusion Detection/Intrusion Prevention), EDR, anti-malware software, event logs).

Analysis involves gathering and comparing related events against the system baseline (expected behavior) to determine deviations or anomalies that may be occurring.

KONICA MINOLTA | Giving Shape to Ideas

Containment, Eradication & Recovery

Containment of the incident is necessary to minimize and isolate the damage. Root cause analysis should be conducted, and may require third party support (e.g., SOC, forensic analysis).

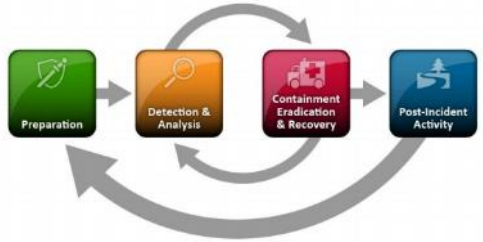
Eradication involves eliminating components of the incident. For example: deleting malware, disabling compromised accounts, identifying/mitigating exploited vulnerabilities. It is important to identify all affected hosts within the organization systems for remediation.

Recovery involves restoring systems to normal operations, confirming system functionality is normal, and conducting necessary remediation activities to prevent similar incidents. For example: restoring system backups, rebuilding systems, patching and updates, account management, finetuning firewalls, and increasing system monitoring (e.g., EDR, SIEM) to prevent future attacks.

KONICA MINOLTA

Giving Shape to Ideas

Post-Incident Activities



Incident Response Report			
Person Involved			
Department		Job Title	
Supervisor			
Date of Incident		Time	
Location		Incident ID	

Incident Details	
☐ Cyber Incident (e.g., Phishing, Ransomware, DDoS, Virus/Malware)	Describe what happened:
☐ In-Person Incident (e.g., Social engineering)	Describe what happened:
☐ Phone Incident (e.g., Social engineering)	Describe what happened:

Areas for improvement
•

Lessons learned
•

Recommended actions	Responsibility	Timeframe
1.		
2.		
3.		

☐ Incident Response Report APPROVED			
Name		Position	

Once the incident is resolved, **the Incident Response Team conducts an incident review to capture lessons learned** (e.g., vulnerabilities, enhancements) used to improve the process.

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Incident Response Tabletop Test

All Covered
IT SERVICES FROM KONICA MINOLTA

Purpose

This tabletop/supervised walkthrough exercise is a facilitated discussion about what the organization would do in response to a **compromised system with full access to ePHI data.**

Goals

- To **assess the healthcare organization's ability to respond** using your current plans, policies, capabilities, and resources;
- To **help identify improvements** that could make the difference in keeping your organization operational during/after an event.

KONICA MINOLTA

Giving Shape to Ideas

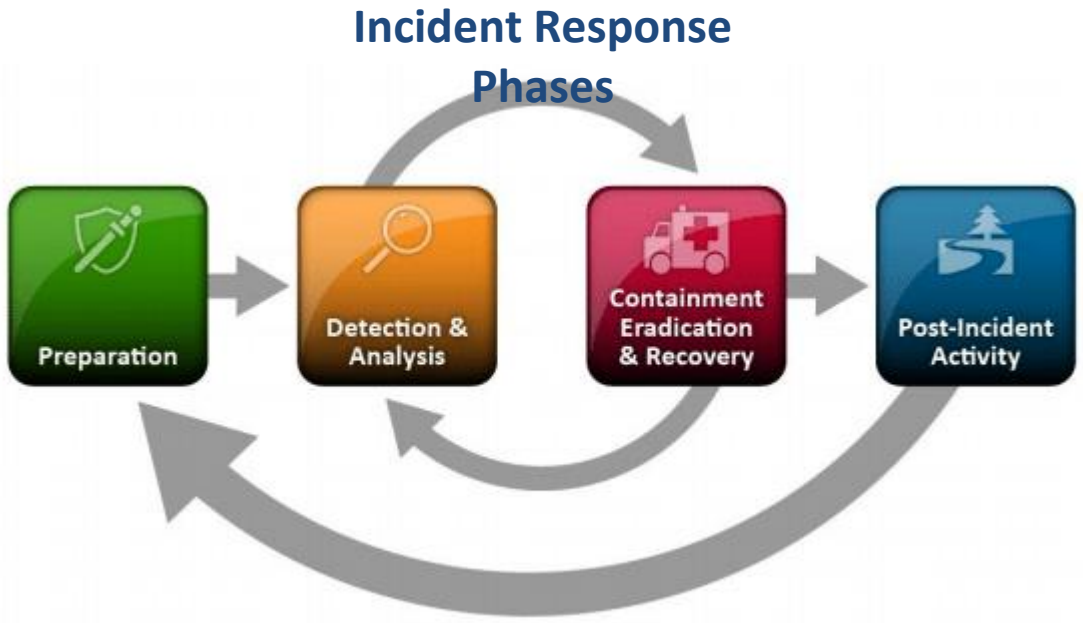
Objectives

- **Promote common understanding** of how the organization responds to a cybersecurity incident
- **Identify opportunities** for improvement
- **Strengthen collaboration** between team leaders

KONICA MINOLTA

Giving Shape to Ideas

Policy Highlights: Incident Response



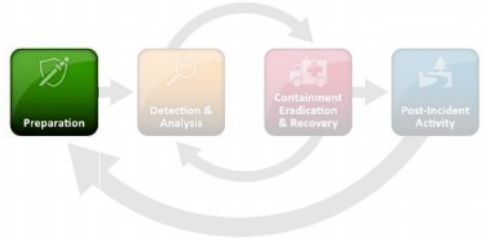
Everyone plays a role in information security…

If you see something, say something!

Report security incidents to: **CISO** or **IT Helpdesk**

KONICA MINOLTA | Giving Shape to Ideas

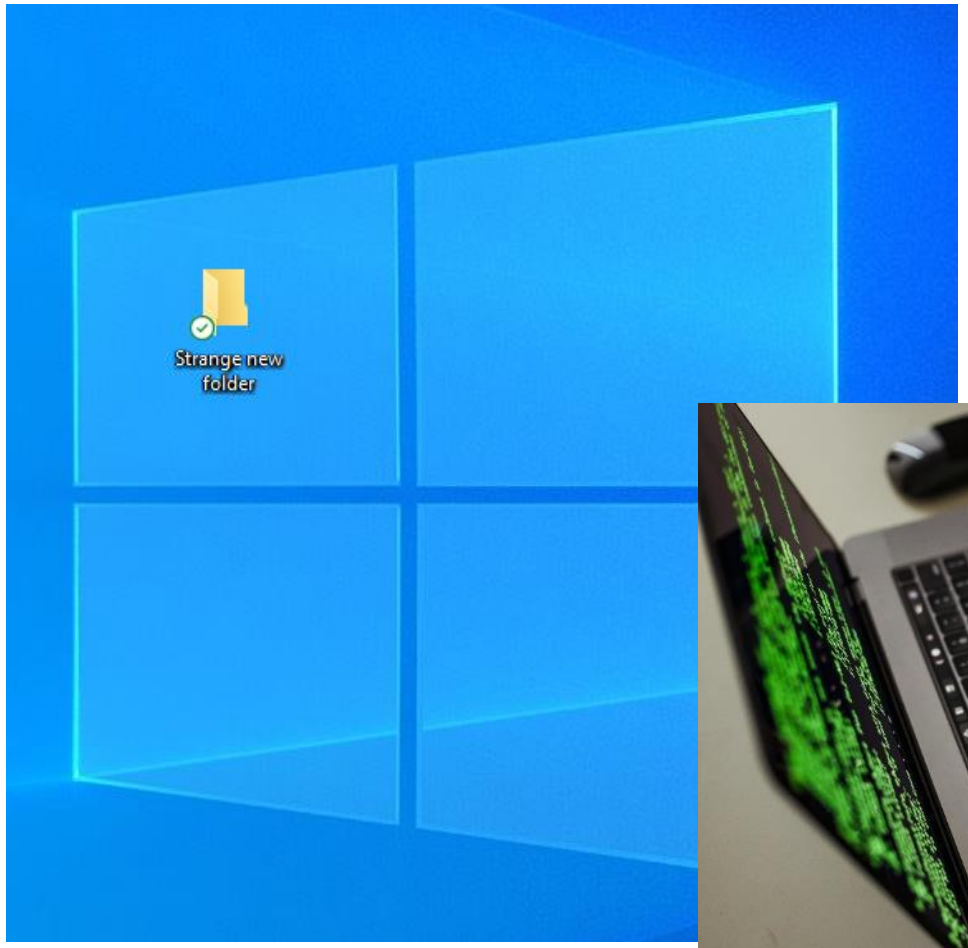
Planning and Preparation



- **Know how to locate** the **Incident Response Plan**
- **Know your role** in response to a cyber incident
- **Update the plan periodically** for changes in infrastructure and organizational changes
- **Perform testing** of the plan **periodically**
- **Employee Training** – train often and use different methods to test employee knowledge
- **Identify critical process owners/key decision makers**

All Covered
IT SERVICES FROM KONICA MINOLTA

Unauthorized Access Scenario - 1



Monday, 8:00am

While logging into the workstation, a provider (a.k.a. JW) realizes a **strange new folder on his desktop** containing **system files.** The **provider notified IT helpdesk** of the situation immediately.

KONICA MINOLTA | Giving Shape to Ideas

Unauthorized Access Scenario - 1

Monday, 8:00am

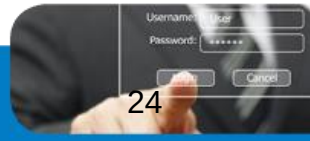
While logging into the computer, a provider (a.k.a. JW) realizes a **strange new folder on his desktop** containing **system files.** The **provider notified IT helpdesk** of the situation immediately.

Detection and Analysis:

- What is the plan for **Detection & Analysis**?
- Who contacts Incident Response Team?
- Type of event? Severity?
- What services are impacted?

Services to Consider:

- Network Infrastructure & Connectivity
- Electronic Health Records Systems
- Patient Care Platforms
- Mission Critical Medical Devices
- Cloud Storage Service
- Microsoft Office / Applications
- Telephone Communications
- E-mail Communications
- Security & Facilities
- Backup Recovery Service

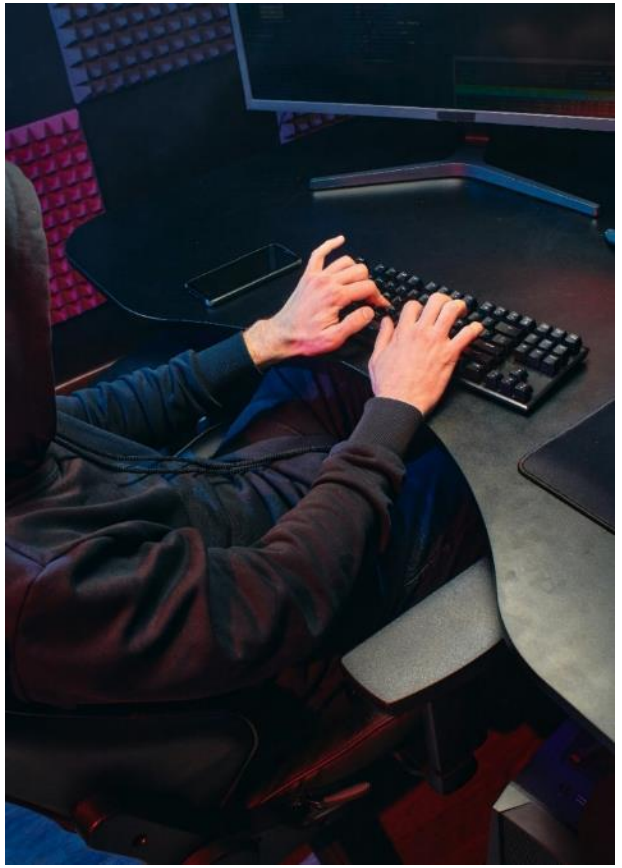


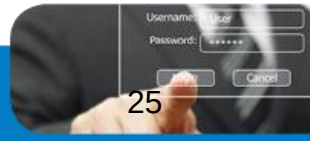
Unauthorized Access Scenario - 1

Monday, 10:00am

The IT team determines **the computer has been exposed** using a malicious DLL (Dynamic Link Libraries) code enabling escalation of privilege **with full permission to the system**, and **access to a healthcare database containing ePHI.**

The IT team also believes **JW's account may also be compromised**.





KONICA MINOLTA | Giving Shape to Ideas

Unauthorized Access Scenario - 1

Monday, 10:00am

The IT team determines **the computer has been exposed** using a malicious DLL enabling escalation of privilege **with full permission to the system**, and **access to healthcare database containing ePHI.** The IT team also believes **JW's account may also be compromised**.

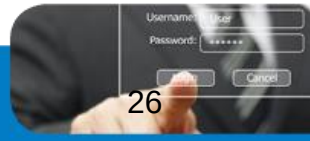
Containment, Remediation and Recovery:

- What is the plan for **Containment and Remediation**?
- Incident Response Team course of action?
- Who is involved in remediating the incident?
- What are the **Recovery** steps?

Services to Consider:

- Network Infrastructure & Connectivity
- Electronic Health Records Systems
- Patient Care Platforms
- Mission Critical Medical Devices
- Cloud Storage Service
- Microsoft Office / Applications
- Telephone Communications
- E-mail Communications
- Security & Facilities
- Backup Recovery Service

All Covered
IT SERVICES FROM KONICA MINOLTA



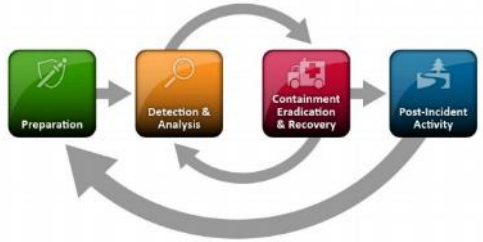
Conclusion of Incident

Reporting incident…

- To whom?
- By when?
- By whom?
- What is required to submit a report?

Security Breach – HHS OCR Reporting Requirements (within 60 days)
Determine if breach affects more or less than 500 individuals and notify Secretary in accordance with 45 C.F.R. § 164.408.

How Did We Do?



- What were the strengths of our plan?
- What were the weaknesses?
- What are our follow-ups?
  - ❑ Infrastructure changes
  - ❑ Procedural / Documentation changes

KONICA MINOLTA

Giving Shape to Ideas

Incident Response – Lessons Learned

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Considerations – Why did this happen?

Considerations – ask WHY?

- Why did we not know about this “Known” Vulnerability?
- Why was our software outdated?
- Why was the system config altered?
- Why was the service able to escalate privileges?
- Why were the user’s credentials compromised?
- Why were there no alerts of privilege escalation?
- Did this occur by a visitor?

Follow up actions:

Vulnerability Management Program: Manages threats, vulnerabilities and risks

Patching: Timely patching prevents breach

MEDR: Detects/Contains/Remediates

MDM: Secures device configurations

GPO: Enforces controls across enterprise (Privileges, USB access, MFA, Password Complexity)

SIEM: Detects/Alerts privilege escalation

Physical Security: monitors physical access

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: VMP

Vulnerability Management Program (VPM) establishes a continuous process of identifying, categorizing and remediating vulnerabilities using vulnerability scanning with automated risk assessment of threats and vulnerabilities.

Addresses – Discovery of "Known" Vulnerabilities; Outdated Software; and System Misconfigurations

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: Patching

Patch Management is the process of applying updates (e.g., security patches, bug fixes and features) to software, drivers, and firmware to protect against vulnerabilities and provide the best system operating performance.

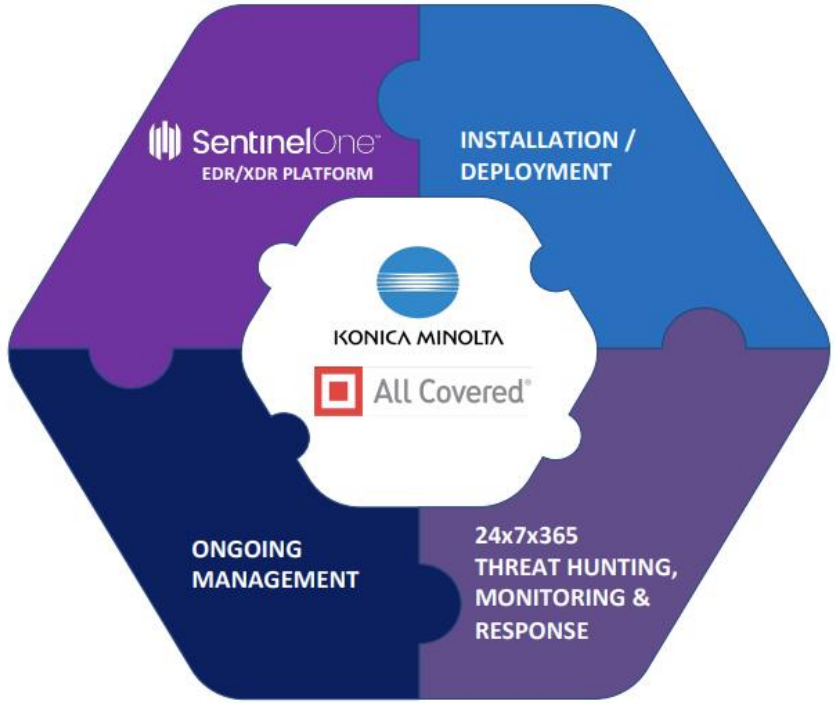
Addresses – Remediates vulnerabilities and performance issues with software updates

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: MEDR



EDR (Endpoint Detection & Response)
Behavior-based protection
Effective against known and unknown threats
Total visibility into activity on endpoints
Provides ability to proactively "threat hunt"
Go back in time to see what happened
Most effective against modern threats

Managed Endpoint Detection and Response (MEDR) provides behavior-based endpoint protection using modern techniques and data-centered approach to pre-emptively detect malicious activity and responds before endpoint is exposed.

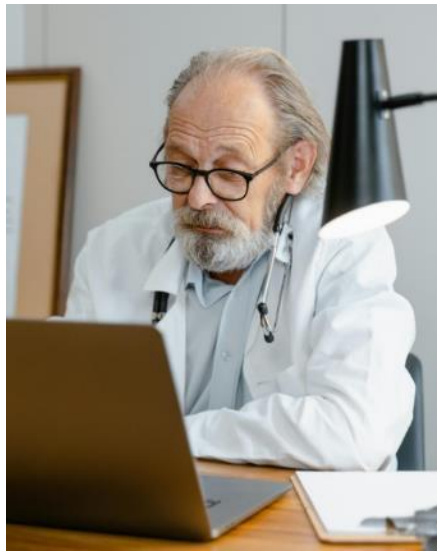
Addresses – Threat discovery with managed EDR solution and Human event monitoring – Security Operations Center (SOC)!

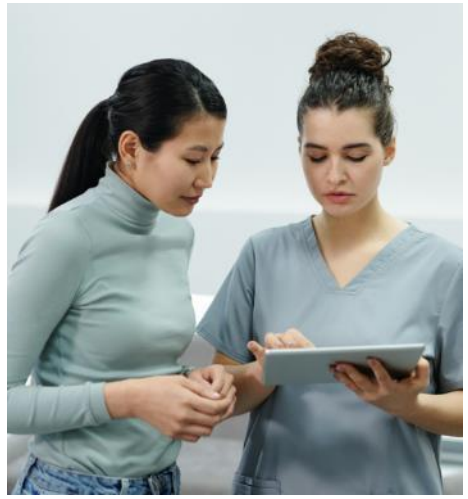
All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: MDM





Mobile Device Management (MDM) enables IT to automate, control, and secure administrative policies on any device connected to an organization's network keeping information secure.

Addresses – Protects mobile devices of various platforms (iOS, Android, Win, Mac, Linux) on-premise and remote…

All Covered

IT SERVICES FROM KONICA MINOLTA

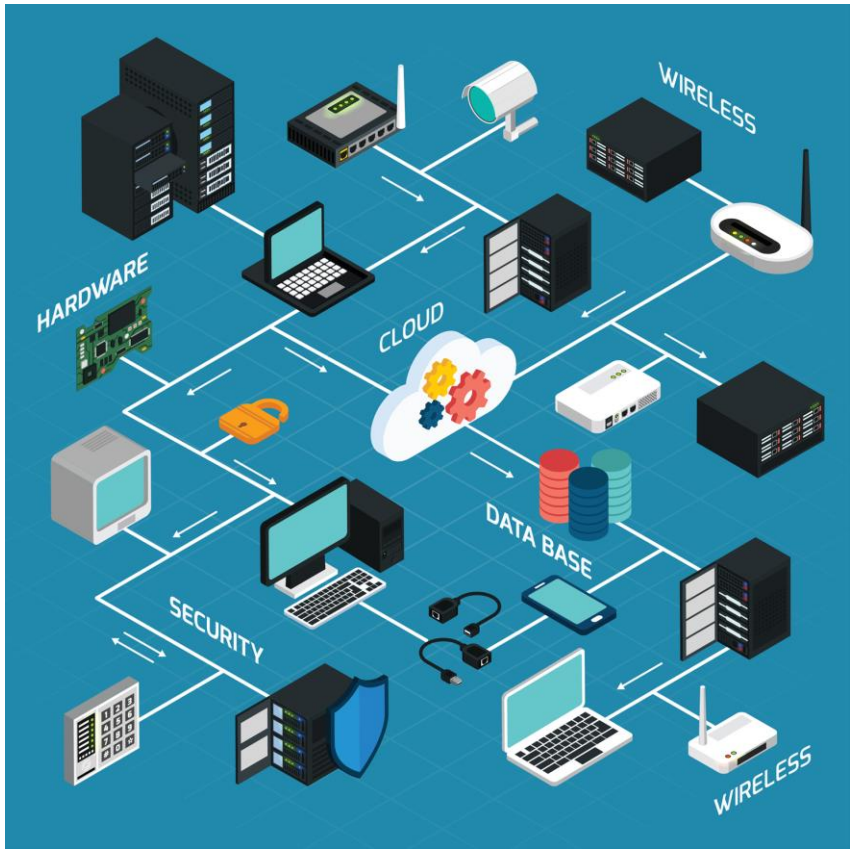
KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: Group Policy

Group Policy Management
Administer group policy objects (GPOs) and settings in systems and active directory across the enterprise.

Addresses – Service privilege escalation; Restricting USB port access; Enforcing MFA and strong passwords

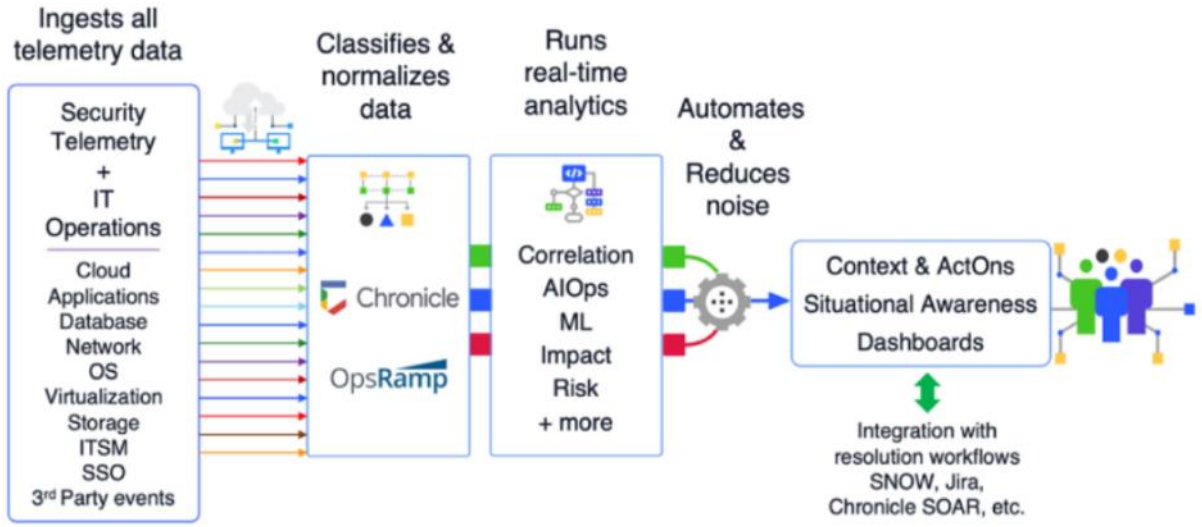


All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: SIEM



Security Information and Event Management (SIEM) collects telemetry data from network devices like servers, routers, switches, firewalls, applications, etc., correlates and alerts on nefarious, anomalous or malicious activities.

Addresses – Monitors, logs, and alerts of suspicious or malicious activity with Security Operations Center (SOC) support

All Covered
IT SERVICES FROM KONICA MINOLTA

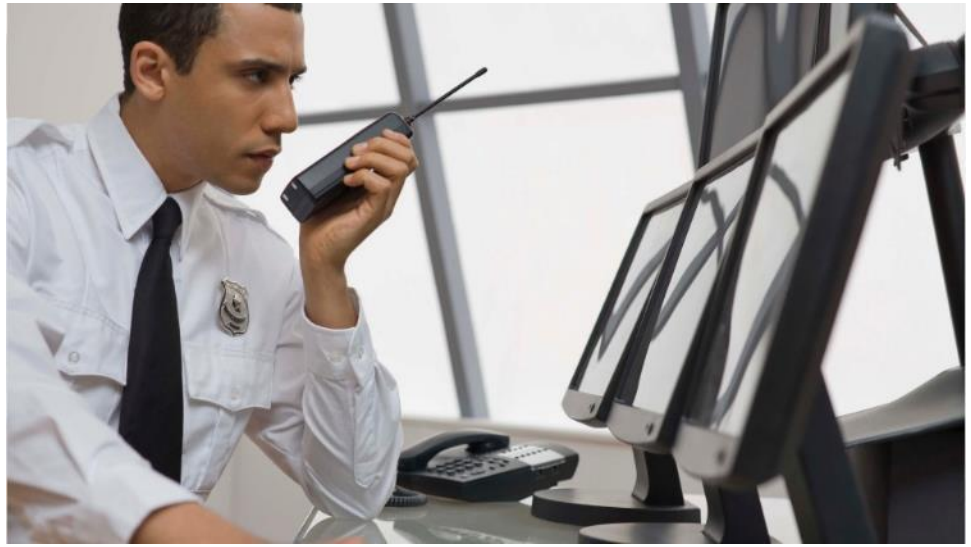
KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: Physical Security

Physical Security

Understanding and monitoring the risk and gaps within the organization physical security controls, facilities, and location.



Addresses – Monitoring and restricting physical access (e.g., facility, devices)

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: Defense in Depth

MESSAGING PROTECTION	ENDPOINT PROTECTION	PATCHING	THREAT RESPONSE & REMEDIATION	VULNERABILITY MANAGEMENT	UTM UNIFIED THREAT MANAGEMENT	SECURITY INFORMATION & EVENT MANAGEMENT (LOGS)	COMPLIANCE & CONSULTING	OFFENSIVE SECURITY
Email Antivirus	Managed Antivirus	Managed Microsoft patching	*MEDR Managed Endpoint Detection & Response Artificial Intelligence Machine Learning 24/7 SOC	*MVS Managed Vulnerability Scan Service	*MUTM Managed Firewall/UTM Service	***SIEM/MDR** Machine Learning Threat Intelligence Feeds 24/7 SOC	*Security Assessments Baseline/Gap/Risk *Cybersecurity Assessment Tool	*Network Penetration Testing
Spam Filtering	Managed Malware Protection	*Third Party patching		*VMP Vulnerability Management Program			*Written Information Security Program *System Security Plan *Security Awareness Training	*Application Penetration Testing
Email Continuity	DNS Filtering						*vCISO/vISO *Vendor Risk Mgt *IT Audit Support *Incident Response *Business Continuity	*Red Team *Adversarial Simulation
Phishing Protection	*Web Content Filtering							
*Email Encryption	*Mobile Device Management							
*Email Archiving	*Endpoint Encryption							

MANAGED SECURITY AWARENESS TRAINING AND TESTING

Compliance – HIPAA / HITECH Privacy & Security

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Preventive Measures: Defense in Depth

Compliance – HIPAA / HITECH Privacy & Security

- On-Site Annual Risk Assessment
- Vulnerability Scanning
- Policy & Procedures Review *(specific to HIPAA/HITECH)*
- Staff Training
- HIPAA/HITECH Compliance On-going
- Compliance Portal Access

All Covered
IT SERVICES FROM KONICA MINOLTA

KONICA MINOLTA

Giving Shape to Ideas

Compliance – HIPAA / HITECH Privacy & Security

- Take Home Resources

SCAN ME

All Covered
IT SERVICES FROM KONICA MINOLTA