National Critical Information Infrastructure Protection Centre

सत्यमेव जयते

NCIIPC

सम्पूर्ण सुरक्षा

A unit of NTRO

Cyber Security & Incident Management

(12 October 2023)

Outline

- Need for Cyber Security
- Incident Management
- Incident Response Plan
- Modern Incident Response Life Cycle
- Key Areas of Concerns
- Best Practices

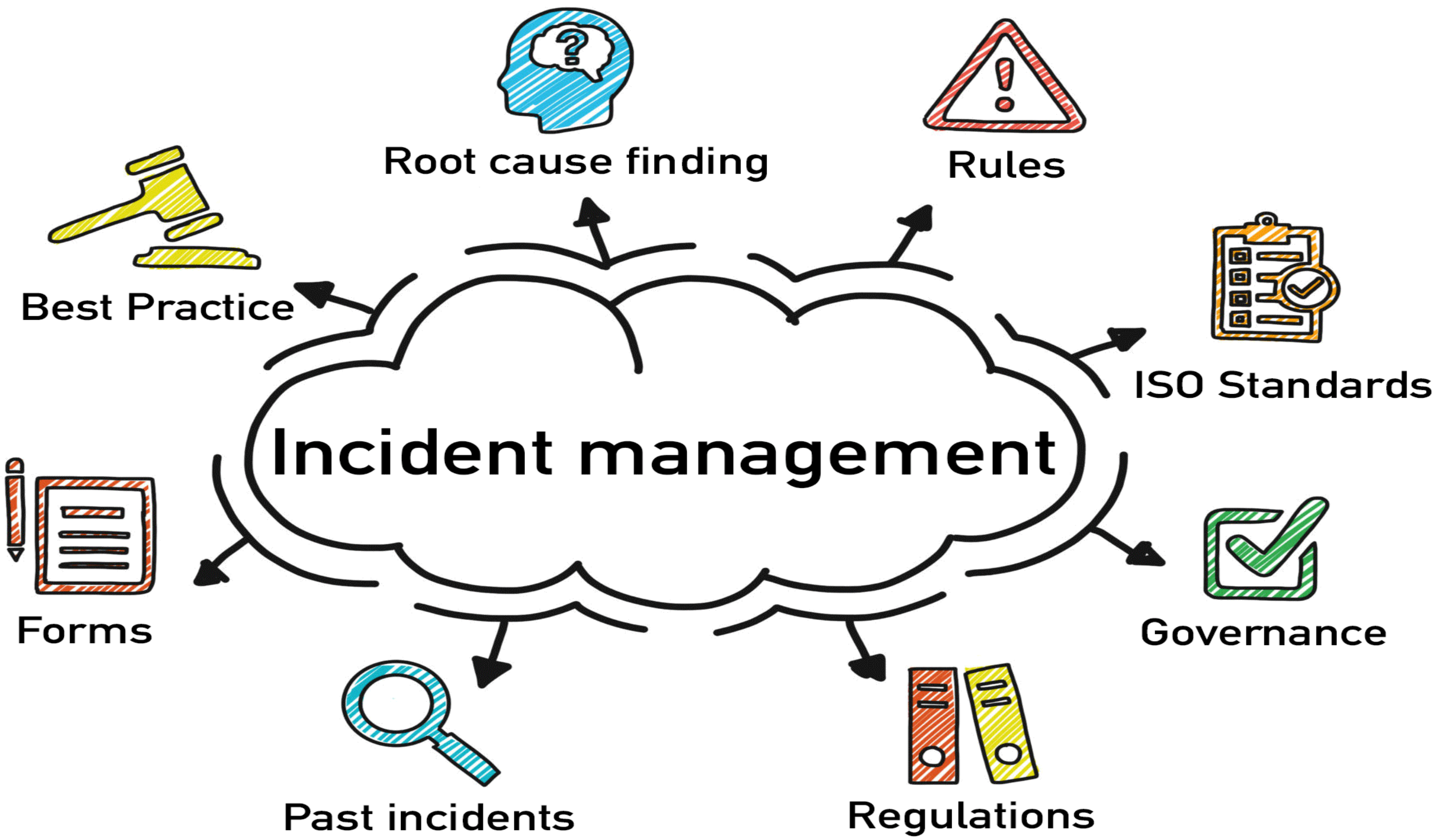
Need for Cyber Security

- **Protection against cyber threats :**
  - OT systems vulnerable to cyber threats.
- **Maintaining system integrity:**
  - Ensuring the integrity of these systems is essential to prevent unauthorized modifications.
- **Safeguarding public safety:**
  - Robust cybersecurity measures help protect public safety by preventing unauthorized access and malicious activities.
- **Mitigating operational risks:**
  - Cybersecurity in OT helps identify and mitigate operational risks associated with automation and control systems.

Incident Management

- Matured plan for security incident management
- Creating an Incident Response Team (IRT)
- Establish clear communication channel
- Centralised incident tracking system
- Develop incident response playbooks
- Regular vulnerability Assessment
- Compliance with regulatory requirement

Incident Management



Importance of Incident Management

- Prepare an organization for any potential Cyber incidents ahead.

- Ensure that standardized methods and procedures are used for efficiently and prompt Incident response, technical analysis, documentation, ongoing management and reporting.

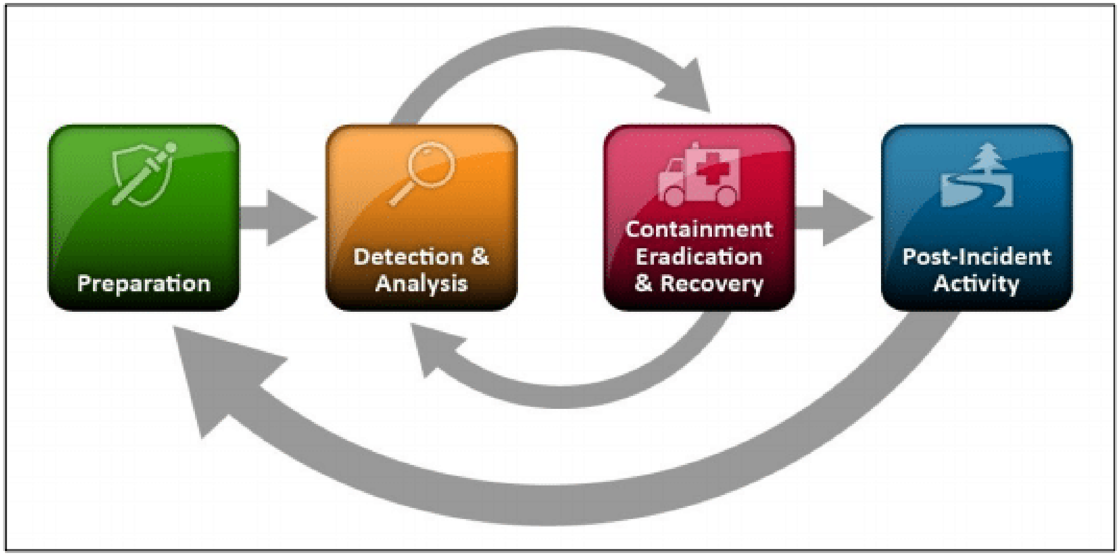
- Increase visibility and communication of incidents to CISO / organization.

- Reducing downtime.

Incident Response Plan

Preparation

- Policy
- Response Plan / Strategy
- Communication
- Documentation
- Team
- Access control
- Tools



Incident Response Plan

Detection of Compromised Systems

- Check the logs of all perimeter network devices such as firewalls, proxy servers etc.
- Domain Controller / Active Directory server.
- IP addressing schemes / DHCP server logs.
- Check SIEM, NAC, EDR or such security systems.

Incident Response Plan

Containment and Evidence collection

- Capture volatile memory of the live system without disconnecting from the network.
- Create forensic image of all the physical storage drives.
- Alternate / backup systems must be built and used as replacement.
- Extracted and preserved network artefacts such as firewall logs, proxy logs, VPN logs, Emails etc.

Incident Response Plan

Analysis of evidences

- Analyses of the collected artefacts shall be carried out (Scope of the compromise / gather additional actionable information / Root Cause of the incident).
- Original evidence shall be kept aside and copies of evidences should be created and used for analysis.
- Analysis should also focus identification of additional indicators and other artefacts.

Incident Response Plan

Eradication / Remediation and Clean up

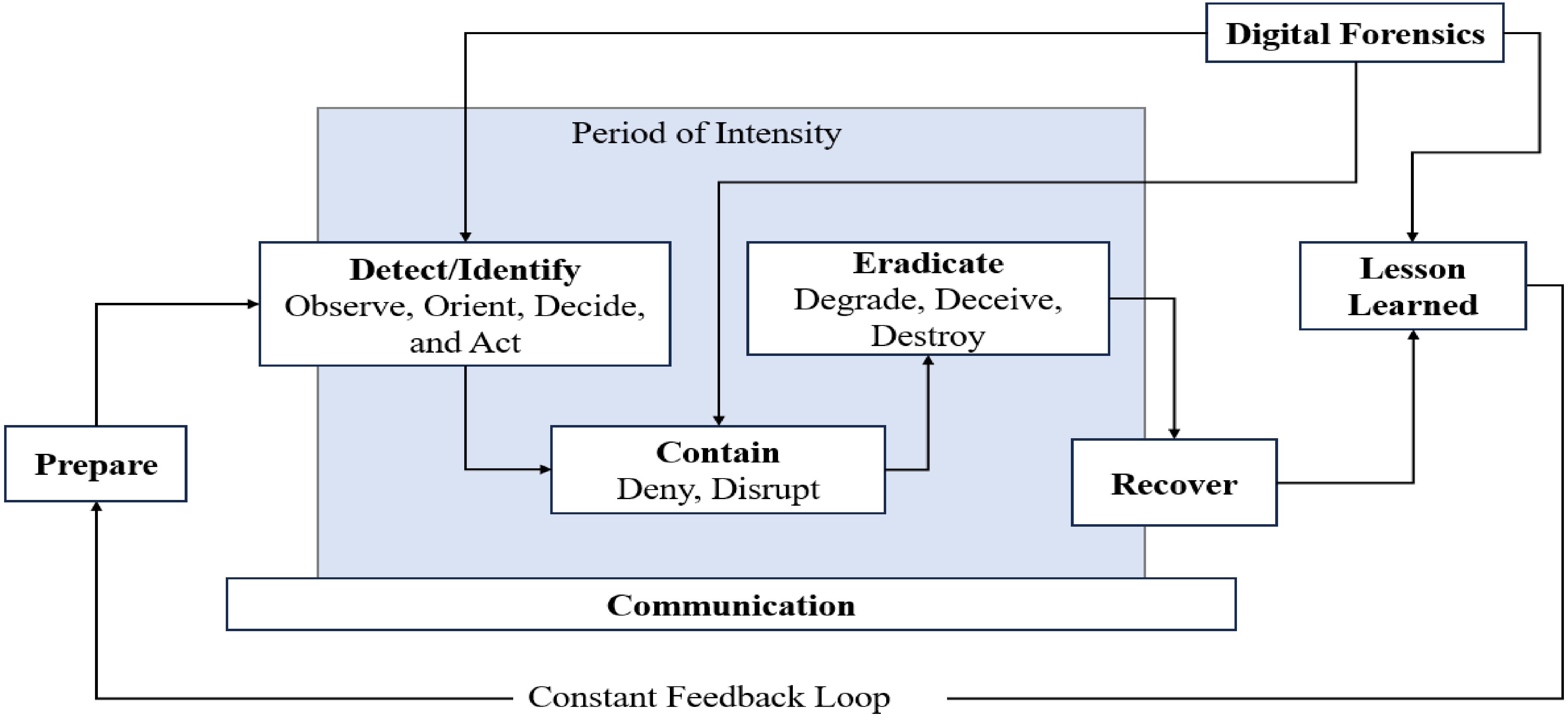
- Root cause
- Applying basic security best practices
- Scan for malware
- Affected systems should be rebuilt and restored from clean backup

Incident Response Plan

Post-Incident Activity

- **Lesson learned**
  - what happened and when
  - how well the IR team performed
  - whether documented procedures were followed
  - whether those procedures were adequate
  - what information was missing when it was needed
  - what actions slowed recovery
  - what could be done differently
  - what can be done to prevent future incidents
  - How well did support teams
  - what precursors or indicators can be looked for in the future

Modern Incident Response Life Cycle



Key Areas of Concerns

- Non existence of Basic Security Measures
- Network perimeter security devices not in place
- Improper network segregation
- Misconfiguration / no hardening measures for system / server / devices
- Unwanted ports / services open
- Absence of centralised logging mechanism
- Issue with availability of logs / Insufficient logging issues
- Users not sufficiently trained / experienced in cyber security related matters.
- Issue with Implementation of ISP on ground
- Usage of multiple USBs / portable devices
- Missing clear Roles and Responsivity of Users
- Cyber security related clauses in Service Level Agreements (SLA)
- End of Life / Support Systems
- Concern of Risk Assessment
- Remote access & management
- Lack of inventory management
- Multifactor Authentication (MFA) not in place
- Lack of monitoring of logs
- Cyber security Audit concern

Best Practices

- Build an incident response plan / team
- Asset identification, tracking and management system
- Update all the Indicators of Compromise (IoCs)
- Isolate the suspected / compromised cyber Assets from the network immediately
- Segregation of Security Zones and having defense in depth
- Clear knowledge and classification of criticalities and prioritised measures for it
- Regular Vulnerability Assessments, Auditing and compliance within timelines
- Performance monitoring with established metrics
- Security Updates and Patch Management
- Follow whitelist approach
- Use system with least privilege
- Strict Configuration / Change Management Process
- Ensure secure communication / data transfer
- Conduct cyber awareness program (include lesson learned from past incidents)

Thank You !

Incident Reporting: ir@nciipc.gov.in

Toll Free : 1800 11 4430