CHAPTER 2

Incident Readiness

Chapter Overview

01

Preparing Your Process

IR plans, lifecycle models, escalation, communication, and legal prep

02

Preparing Your People

CSIRT structure, roles, training, tabletop exercises, and retainers

03

Preparing Your Technology

Visibility, responder tools, BC/DR, and deception techniques

Preparing Your Process

Plan before the incident — not during it

The Incident Response Plan

A documented IR plan is the foundation of effective incident response

Plan must define: scope, roles, authority, and escalation triggers

Integrate with legal, HR, PR, and executive leadership

Plans should be tested and updated at least annually

Retain outside IR counsel before an incident occurs — not after

Regulatory requirements (HIPAA, PCI-DSS, GDPR) may mandate specific notification timelines

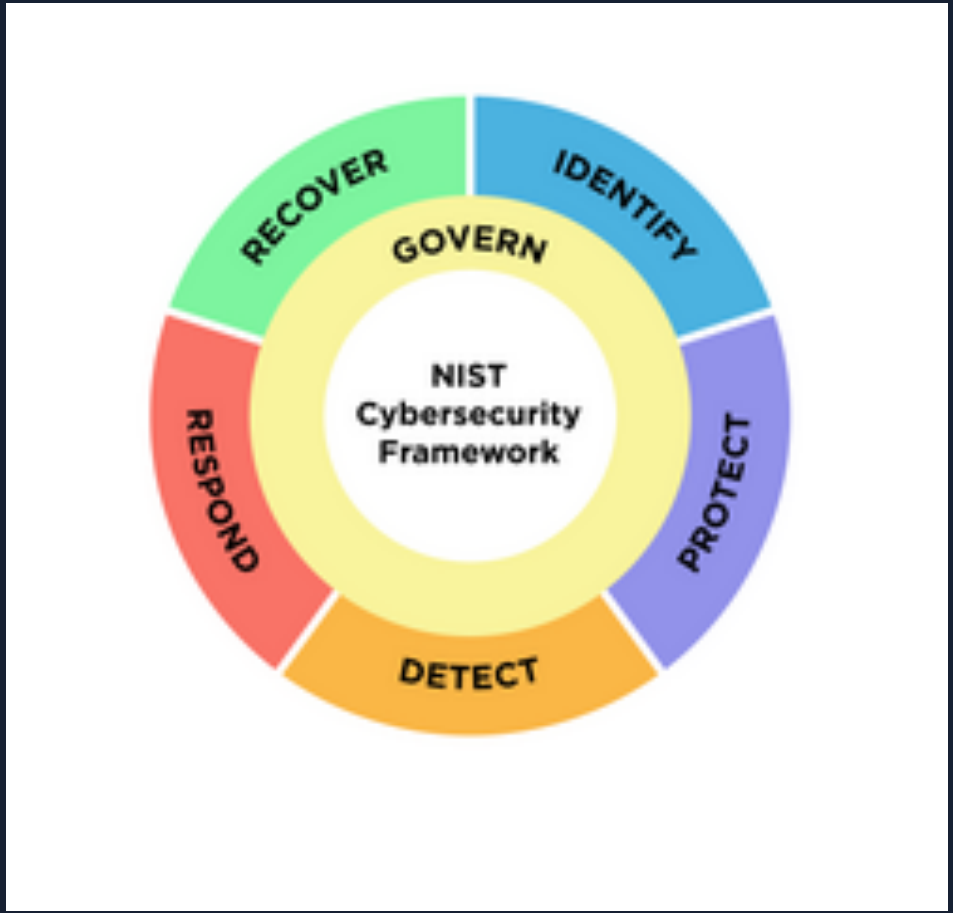
IR Lifecycle Models

NIST SP 800-61 (4 phases)

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity

PICERL (SANS / 6 phases)

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned



Incident response is a cycle — preparation feeds back from every incident

Escalation & Communication

Escalation Procedures

Define clear thresholds for escalating severity

Chain of command must be documented and rehearsed

24/7 contact list for key roles (IR lead, legal, exec)

Time-boxed escalation: if no response in X mins, go up

Communication Plans

Internal: IT, management, affected business units

External: customers, regulators, law enforcement

Out-of-band channel if primary systems are compromised

Legal review required before external disclosure

Preparing Your People

Your team is your most important security tool

CSIRT: Structure & Roles

Core IR Team Roles

IR Manager: coordinates response and decisions

Lead Investigator: technical analysis lead

Threat Intelligence Analyst: context and attribution

Forensic Analyst: evidence collection and analysis

Legal / Compliance Liaison

Extended Team

IT Operations: network/system changes

Communications / PR: public messaging

Executive Sponsor: authority and resources

External IR Retainer: surge capacity

Law Enforcement Liaison (when needed)

Training & Exercises

Tabletop exercises: walk through a scenario in discussion — low cost, high value

Red team / purple team exercises: simulate real attacks against real defenses

Technical drills: practice memory acquisition, log analysis, malware triage

Cross-training: ensure no single point of failure on critical skills

After-action reviews: every exercise and real incident produces lessons learned

Track skill gaps and address through targeted training or hiring

Preparing Your Technology

You cannot respond to what you cannot see

Ensuring Adequate Visibility

Logging is the foundation of incident response — collect before you need it

Windows Event Logs: enable process creation (4688), PowerShell (4103/4104), logon events

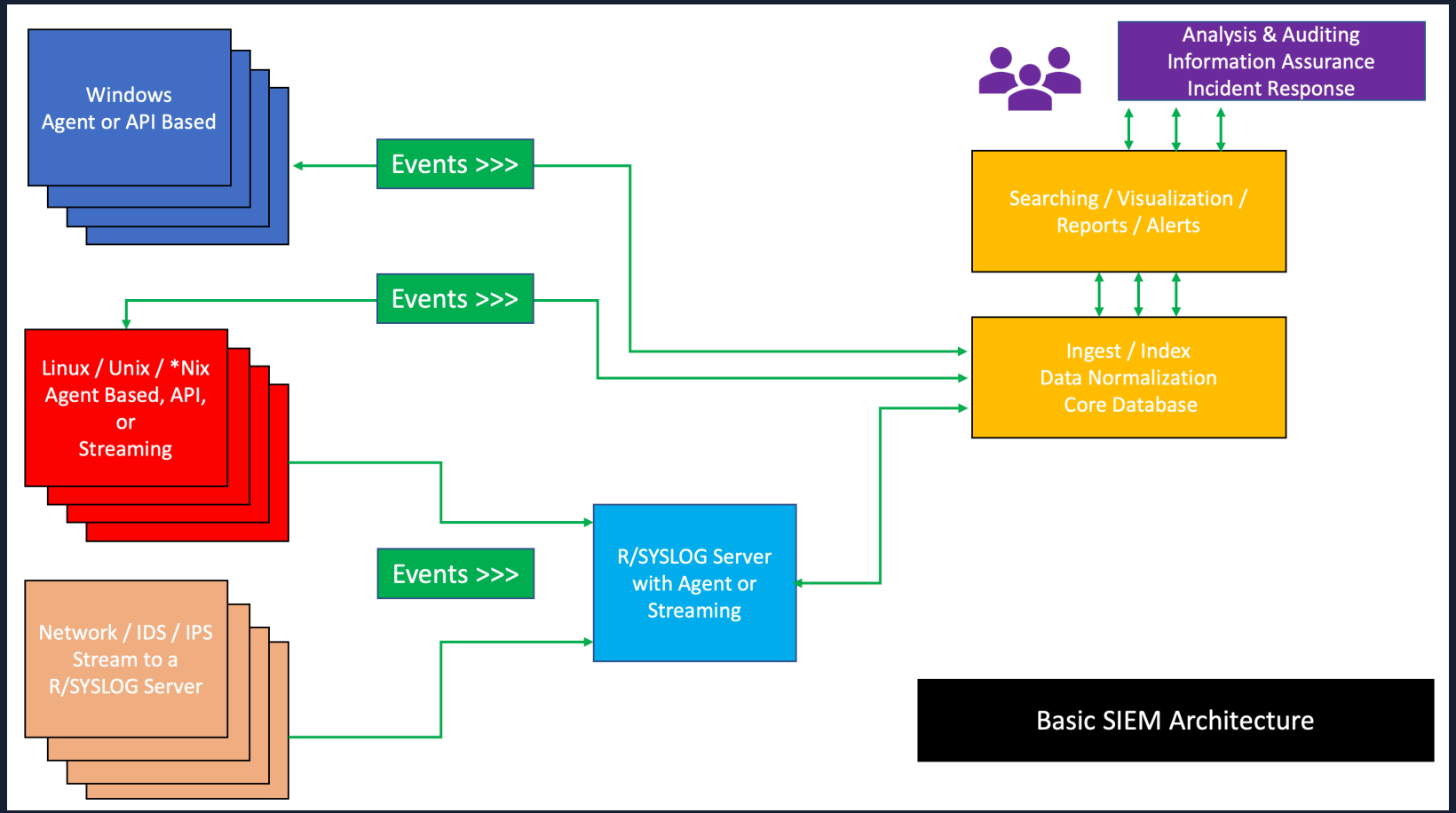
Sysmon: adds rich process, network, and file creation telemetry

Network monitoring: NetFlow, full packet capture (where feasible), DNS logs

EDR (Endpoint Detection & Response): behavioral detection + remote triage capability

SIEM: centralize and correlate logs for detection and investigation

Ensure log retention meets regulatory and investigative requirements



Security Operations Center — centralized monitoring and alerting

Arming Your Responders

Jump Kit / Go Bag

Bootable forensic media (SIFT, CAINE, Paladin)

Write blockers (hardware) for dead-box imaging

Large-capacity encrypted USB/external drives

Network tap and cables

Forensic-grade documentation supplies

Remote Triage Capabilities

EDR console for remote isolation and investigation

PowerShell Remoting / WMI for live triage at scale

Centralized log search (SIEM) from any location

Out-of-band access (IPMI/iDRAC) for critical servers

Business Continuity & Disaster Recovery

BC/DR Planning

Identify critical systems and their recovery priority

Define **RTO (Recovery Time Objective)** per system

- Max tolerable downtime

Define **RPO (Recovery Point Objective)** per system

- How much data you can afford to lose

Ensure backups are isolated from production network

Test restores regularly — untested backups are not backups

Incident Integration

IR plan and BCP must reference each other

Ransomware scenario: clean restore from offline backup

Alternate communication paths if email is compromised

Pre-approved vendor contacts for emergency hardware

Deception Techniques

Deception shifts the advantage to defenders — attackers must be right every time

Honeypots: decoy systems that attract and expose attacker activity

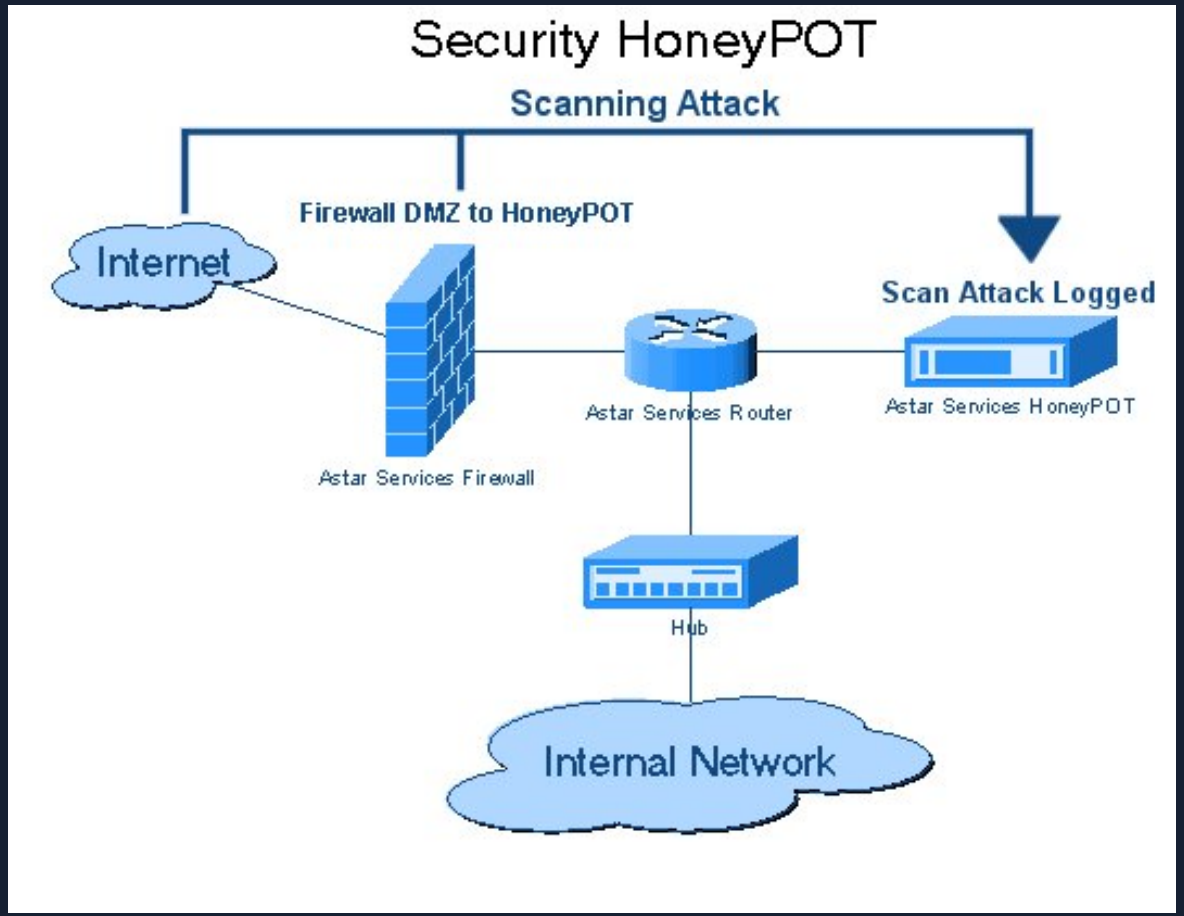
Honeynets: full decoy network segments with realistic assets

Honeytokens: fake credentials, documents, or registry keys that trigger on access

Canary tokens: embedded traps in files, URLs, or directories

Any interaction with a deception asset is a high-confidence alert

Low false-positive rate makes deception alerts highly actionable



Honeypot concept: decoy assets that detect attackers before real damage occurs

Conclusion

If you are not prepared for battle, the war is over before it begins

Effective IR requires documented processes, trained people, and the right tools

Visibility is everything — you cannot respond to what you cannot see

Deception techniques can give defenders an early-warning advantage

Practice through tabletop exercises before a real incident occurs

Preparation feeds directly into faster, more effective incident response

Knowledge Check