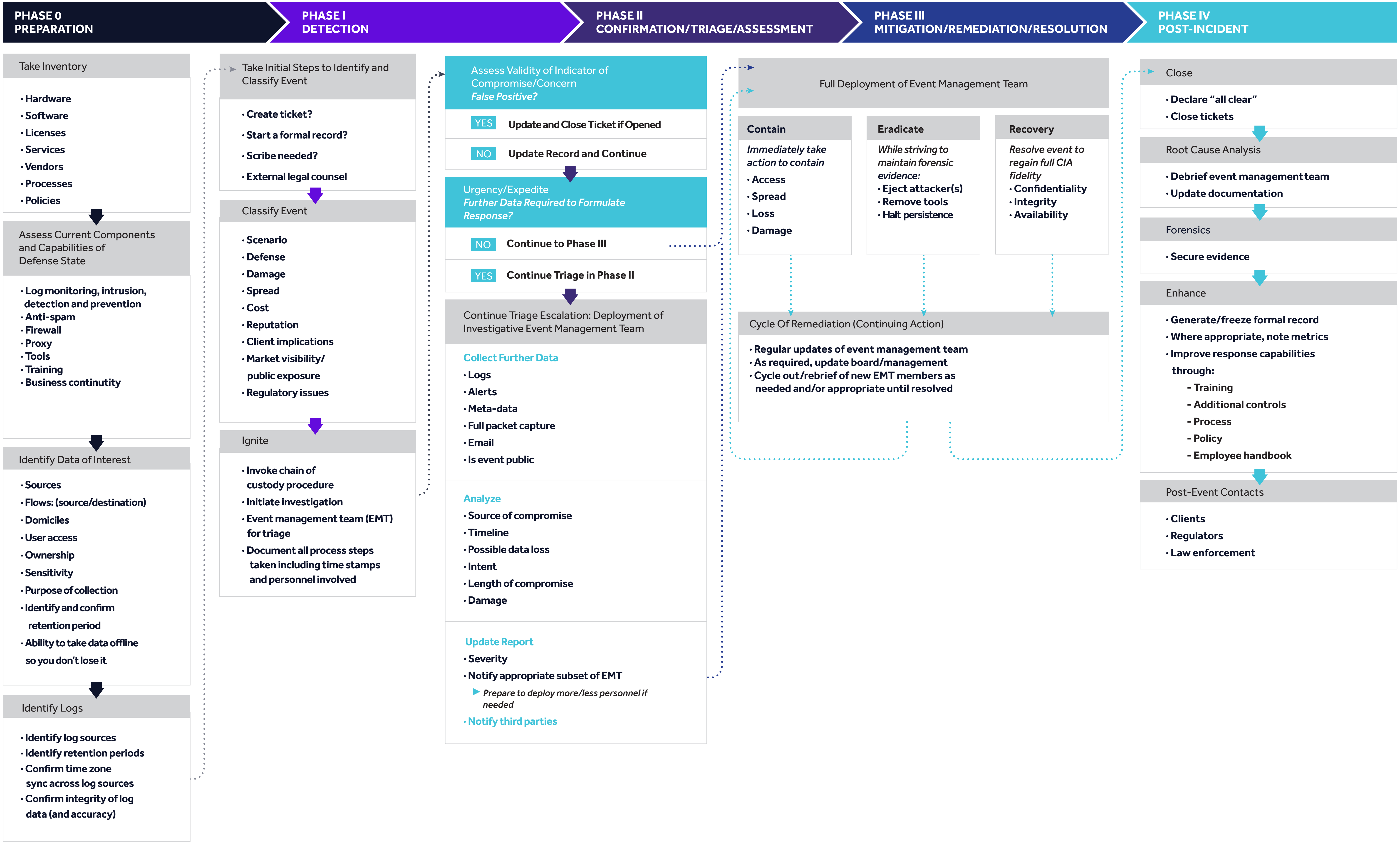
eSENTIRE

Pragmatic Security Event Management Playbook

Malware Compromise - Ransomware - Infrastructure Outage - Local Access without Autorization
Successful Remote Access without Authorization - Lost/Stolen Devices - Inappropriate Behavior
Cloud Service Access w/o Authorization - Data Loss/Extrusion - Direct Financial Loss
Denial of Service (Exteranal) - Physical Breach - Social Engineering

Core IR Process

eSENTIRE



PHASE 0 PREPARATION

Take Inventory

- Hardware
- Software
- Licenses
- Services
- Vendors
- Processes
- Policies

Assess Current Components and Capabilities of Defense State

- Log monitoring, intrusion, detection and prevention
- Anti-spam
- Firewall
- Proxy
- Tools
- Training
- Business continuity

Identify Data of Interest

- Sources
- Flows: (source/destination)
- Domiciles
- User access
- Ownership
- Sensitivity
- Purpose of collection
- Identify and confirm retention period
- Ability to take data offline so you don't lose it

Identify Logs

- Identify log sources
- Identify retention periods
- Confirm time zone sync across log sources
- Confirm integrity of log data (and accuracy)

PHASE I DETECTION

Take Initial Steps to Identify and Classify Event

- Create ticket?
- Start a formal record?
- Scribe needed?
- External legal counsel

Classify Event

- Scenario
- Defense
- Damage
- Spread
- Cost
- Reputation
- Client implications
- Market visibility/ public exposure
- Regulatory issues

Ignite

- Invoke chain of custody procedure
- Initiate investigation
- Event management team (EMT) for triage
- Document all process steps taken including time stamps and personnel involved

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Assess Validity of Indicator of Compromise/Concern

False Positive?

YES Update and Close Ticket if Opened

NO Update Record and Continue

Urgency/Expedite

Further Data Required to Formulate Response?

NO Continue to Phase III

YES Continue Triage in Phase II

Continue Triage Escalation: Deployment of Investigative Event Management Team

Collect Further Data

- Logs
- Alerts
- Meta-data
- Full packet capture
- Email
- Is event public

Analyze

- Source of compromise
- Timeline
- Possible data loss
- Intent
- Length of compromise
- Damage

Update Report

- Severity
- Notify appropriate subset of EMT
  - ▶ *Prepare to deploy more/less personnel if needed*
- Notify third parties

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Full Deployment of Event Management Team

Contain

Immediately take action to contain

- Access
- Spread
- Loss
- Damage

Eradicate

While striving to maintain forensic evidence:

- Eject attacker(s)
- Remove tools
- Halt persistence

Recovery

Resolve event to regain full CIA fidelity

- Confidentiality
- Integrity
- Availability

Cycle Of Remediation (Continuing Action)

- Regular updates of event management team
- As required, update board/management
- Cycle out/rebrief of new EMT members as needed and/or appropriate until resolved

PHASE IV POST-INCIDENT

Close

- Declare "all clear"
- Close tickets

Root Cause Analysis

- Debrief event management team
- Update documentation

Forensics

- Secure evidence

Enhance

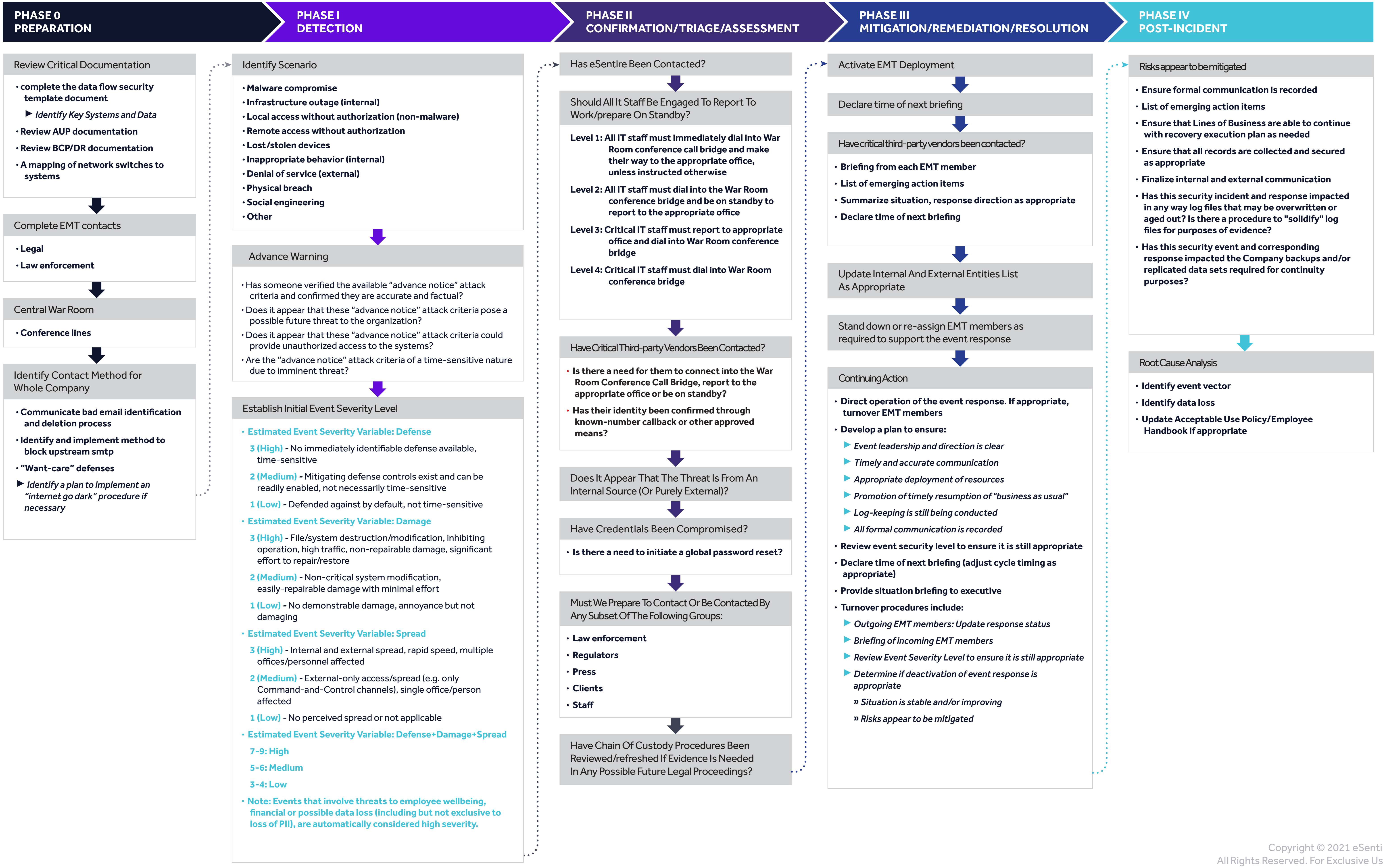
- Generate/freeze formal record
- Where appropriate, note metrics
- Improve response capabilities through:
  - Training
  - Additional controls
  - Process
  - Policy
  - Employee handbook

Post-Event Contacts

- Clients
- Regulators
- Law enforcement

Scenario Qualification Workflow

eSENTIRE



PHASE 0 PREPARATION

Review Critical Documentation

- complete the data flow security template document
  - ▶ *Identify Key Systems and Data*
- Review AUP documentation
- Review BCP/DR documentation
- A mapping of network switches to systems

Complete EMT contacts

- Legal
- Law enforcement

Central War Room

- Conference lines

Identify Contact Method for Whole Company

- Communicate bad email identification and deletion process
- Identify and implement method to block upstream smtp
- "Want-care" defenses
  - ▶ *Identify a plan to implement an "internet go dark" procedure if necessary*

PHASE I DETECTION

Identify Scenario

- Malware compromise
- Infrastructure outage (internal)
- Local access without authorization (non-malware)
- Remote access without authorization
- Lost/stolen devices
- Inappropriate behavior (internal)
- Denial of service (external)
- Physical breach
- Social engineering
- Other

Advance Warning

- Has someone verified the available "advance notice" attack criteria and confirmed they are accurate and factual?
- Does it appear that these "advance notice" attack criteria pose a possible future threat to the organization?
- Does it appear that these "advance notice" attack criteria could provide unauthorized access to the systems?
- Are the "advance notice" attack criteria of a time-sensitive nature due to imminent threat?

Establish Initial Event Severity Level

- Estimated Event Severity Variable: Defense
  - 3 (High) - No immediately identifiable defense available, time-sensitive
  - 2 (Medium) - Mitigating defense controls exist and can be readily enabled, not necessarily time-sensitive
  - 1 (Low) - Defended against by default, not time-sensitive
- Estimated Event Severity Variable: Damage
  - 3 (High) - File/system destruction/modification, inhibiting operation, high traffic, non-repairable damage, significant effort to repair/restore
  - 2 (Medium) - Non-critical system modification, easily-repairable damage with minimal effort
  - 1 (Low) - No demonstrable damage, annoyance but not damaging
- Estimated Event Severity Variable: Spread
  - 3 (High) - Internal and external spread, rapid speed, multiple offices/personnel affected
  - 2 (Medium) - External-only access/spread (e.g. only Command-and-Control channels), single office/person affected
  - 1 (Low) - No perceived spread or not applicable
- Estimated Event Severity Variable: Defense+Damage+Spread
  - 7-9: High
  - 5-6: Medium
  - 3-4: Low
- Note: Events that involve threats to employee wellbeing, financial or possible data loss (including but not exclusive to loss of PII), are automatically considered high severity.

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Has eSentire Been Contacted?

Should All It Staff Be Engaged To Report To Work/prepare On Standby?

Level 1: All IT staff must immediately dial into War Room conference call bridge and make their way to the appropriate office, unless instructed otherwise

Level 2: All IT staff must dial into the War Room conference bridge and be on standby to report to the appropriate office

Level 3: Critical IT staff must report to appropriate office and dial into War Room conference bridge

Level 4: Critical IT staff must dial into War Room conference bridge

Have Critical Third-party Vendors Been Contacted?

- Is there a need for them to connect into the War Room Conference Call Bridge, report to the appropriate office or be on standby?
- Has their identity been confirmed through known-number callback or other approved means?

Does It Appear That The Threat Is From An Internal Source (Or Purely External)?

Have Credentials Been Compromised?

- Is there a need to initiate a global password reset?

Must We Prepare To Contact Or Be Contacted By Any Subset Of The Following Groups:

- Law enforcement
- Regulators
- Press
- Clients
- Staff

Have Chain Of Custody Procedures Been Reviewed/refreshed If Evidence Is Needed In Any Possible Future Legal Proceedings?

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Activate EMT Deployment

Declare time of next briefing

Have critical third-party vendors been contacted?

- Briefing from each EMT member
- List of emerging action items
- Summarize situation, response direction as appropriate
- Declare time of next briefing

Update Internal And External Entities List As Appropriate

Stand down or re-assign EMT members as required to support the event response

Continuing Action

- Direct operation of the event response. If appropriate, turnover EMT members
- Develop a plan to ensure:
  - ▶ *Event leadership and direction is clear*
  - ▶ *Timely and accurate communication*
  - ▶ *Appropriate deployment of resources*
  - ▶ *Promotion of timely resumption of "business as usual"*
  - ▶ *Log-keeping is still being conducted*
  - ▶ *All formal communication is recorded*
- Review event security level to ensure it is still appropriate
- Declare time of next briefing (adjust cycle timing as appropriate)
- Provide situation briefing to executive
- Turnover procedures include:
  - ▶ *Outgoing EMT members: Update response status*
  - ▶ *Briefing of incoming EMT members*
  - ▶ *Review Event Severity Level to ensure it is still appropriate*
  - ▶ *Determine if deactivation of event response is appropriate*
    - » *Situation is stable and/or improving*
    - » *Risks appear to be mitigated*

PHASE IV POST-INCIDENT

Risks appear to be mitigated

- Ensure formal communication is recorded
- List of emerging action items
- Ensure that Lines of Business are able to continue with recovery execution plan as needed
- Ensure that all records are collected and secured as appropriate
- Finalize internal and external communication
- Has this security incident and response impacted in any way log files that may be overwritten or aged out? Is there a procedure to "solidify" log files for purposes of evidence?
- Has this security event and corresponding response impacted the Company backups and/or replicated data sets required for continuity purposes?

Root Cause Analysis

- Identify event vector
- Identify data loss
- Update Acceptable Use Policy/Employee Handbook if appropriate

Malware Compromise - Workstation

eSENTIRE

PHASE 0 PREPARATION

Operating Systems

- **Ensure workstations are running standardized, officially supported operating systems**

Patch Rigor

- **Ensure patching rigor is maintained - OS and applications regularly scanned for "unwanted" software**

AV Defense

- **Enterprise AV is up-to-date, legal and signatures are regularly updated**

Tool Suite

- **Ensure appropriate tools for investigations are available (as needed, rapidly)**

Hardening

- **Ensure hardening measures have been performed**
  - *As local admin*
  - *Application whitelisting*
  - *Browser hardening*
- **Review vulnerability scans**
  - *Lock down (USB/CD/DVD) external media access*

PHASE I DETECTION

Identify "Patient Zero"

- **ESOC**
- **Endpoint alert**
- **User alert**
- **Security Information and Event Management (SIEM)**

Gauge Severity

- **Spread**
  - *Isolate as appropriate as a precaution*

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Isolate and Confirm

- **Network Disconnect**
  - *Physical (Disconnect Cable)*
  - *Wireless*
    - *» Disable*
    - *» Lock out via controller*
  - *Logical*
    - *» Switch port lockout*
    - *» VLAN isolation*
    - *» Firewall SHUN*

Identify Action

- **ESOC**
  - *Honeypot analysis*
  - *Static analysis*
  - *Threat intel - IoC*
  - *"Deep dig" of network traffic*
- **Behaviors**
  - *Keylogger*
  - *Drive encryption*
  - *Mine local data*
  - *Command & control (C2) channels*
- **Intent**
  - *Generic*
  - *Targeted*
  - *Persistent*

Identify Vector

- **www**
- **Email**
- **Personal USB**

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Forensics

- **Memory/Live Image**
  - *Do not shut down/power off*
  - *Note: May Contaminate System*
- **Hard Drive**
  - *Power Down*
  - *Isolate System*
  - *Review Forensic Handling Practices*
  - *Create Forensic Image*

Data Loss

- **GC, clients, legal**
- **PR**
- **Law enforcement**
- **Compliance**

Contain

- **Alert rest of company**
- **Block further download**
- **Shun C2 channels**
- **Blacklist DNS queries**
- **Block in email server**
- **Update anti-spam**

Eradicate/Recovery

- **Destroy/wipe hd/re-image**
- **Perform av/am scan**
- **Patch vulnerability**

Reset all credentials

- **Corporate**
- **Personal**

Focused Alert

- **24 hours to watch for further indications before "stand down"**

PHASE IV POST-INCIDENT

Root Cause Analysis

- **Summarize vector**
- **Review tool suite**
  - *Employee readiness*
  - *Communication*
  - *Defenses*

Forensics

- **Perform or continue**
- **Ensure chain-of-custody is maintained throughout**

Finalize Report

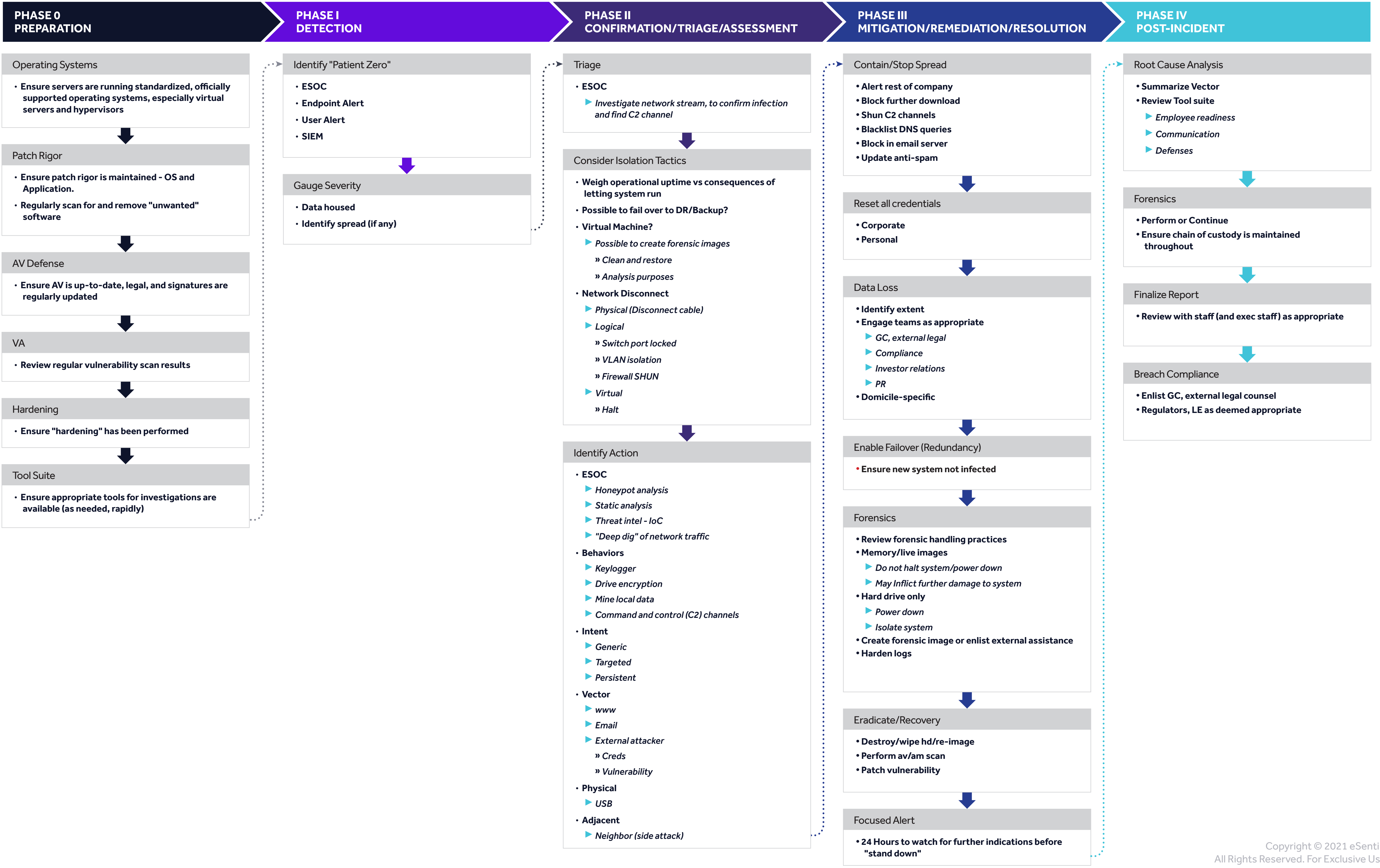
- **Review with staff (and executive staff) as appropriate**

Breach Compliance

- **Enlist GC, external legal counsel**
- **Regulators, LE as deemed appropriate**

Malware Compromise - Server

eSENTIRE



PHASE 0 PREPARATION

Operating Systems
- Ensure servers are running standardized, officially supported operating systems, especially virtual servers and hypervisors

Patch Rigor
- Ensure patch rigor is maintained - OS and Application.
- Regularly scan for and remove "unwanted" software

AV Defense
- Ensure AV is up-to-date, legal, and signatures are regularly updated

VA
- Review regular vulnerability scan results

Hardening
- Ensure "hardening" has been performed

Tool Suite
- Ensure appropriate tools for investigations are available (as needed, rapidly)

PHASE I DETECTION

Identify "Patient Zero"
- ESOC
- Endpoint Alert
- User Alert
- SIEM

Gauge Severity
- Data housed
- Identify spread (if any)

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Triage
- ESOC
  - *Investigate network stream, to confirm infection and find C2 channel*

Consider Isolation Tactics
- Weigh operational uptime vs consequences of letting system run
- Possible to fail over to DR/Backup?
- Virtual Machine?
  - *Possible to create forensic images*
    - *Clean and restore*
    - *Analysis purposes*
- Network Disconnect
  - *Physical (Disconnect cable)*
  - *Logical*
    - *Switch port locked*
    - *VLAN isolation*
    - *Firewall SHUN*
  - *Virtual*
    - *Halt*

Identify Action
- ESOC
  - *Honeypot analysis*
  - *Static analysis*
  - *Threat intel - IoC*
  - *"Deep dig" of network traffic*
- Behaviors
  - *Keylogger*
  - *Drive encryption*
  - *Mine local data*
  - *Command and control (C2) channels*
- Intent
  - *Generic*
  - *Targeted*
  - *Persistent*
- Vector
  - *www*
  - *Email*
  - *External attacker*
    - *Creds*
    - *Vulnerability*
- Physical
  - *USB*
- Adjacent
  - *Neighbor (side attack)*

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Contain/Stop Spread
- Alert rest of company
- Block further download
- Shun C2 channels
- Blacklist DNS queries
- Block in email server
- Update anti-spam

Reset all credentials
- Corporate
- Personal

Data Loss
- Identify extent
- Engage teams as appropriate
  - *GC, external legal*
  - *Compliance*
  - *Investor relations*
  - *PR*
- Domicile-specific

Enable Failover (Redundancy)
- Ensure new system not infected

Forensics
- Review forensic handling practices
- Memory/live images
  - *Do not halt system/power down*
  - *May Inflict further damage to system*
- Hard drive only
  - *Power down*
  - *Isolate system*
- Create forensic image or enlist external assistance
- Harden logs

Eradicate/Recovery
- Destroy/wipe hd/re-image
- Perform av/am scan
- Patch vulnerability

Focused Alert
- 24 Hours to watch for further indications before "stand down"

PHASE IV POST-INCIDENT

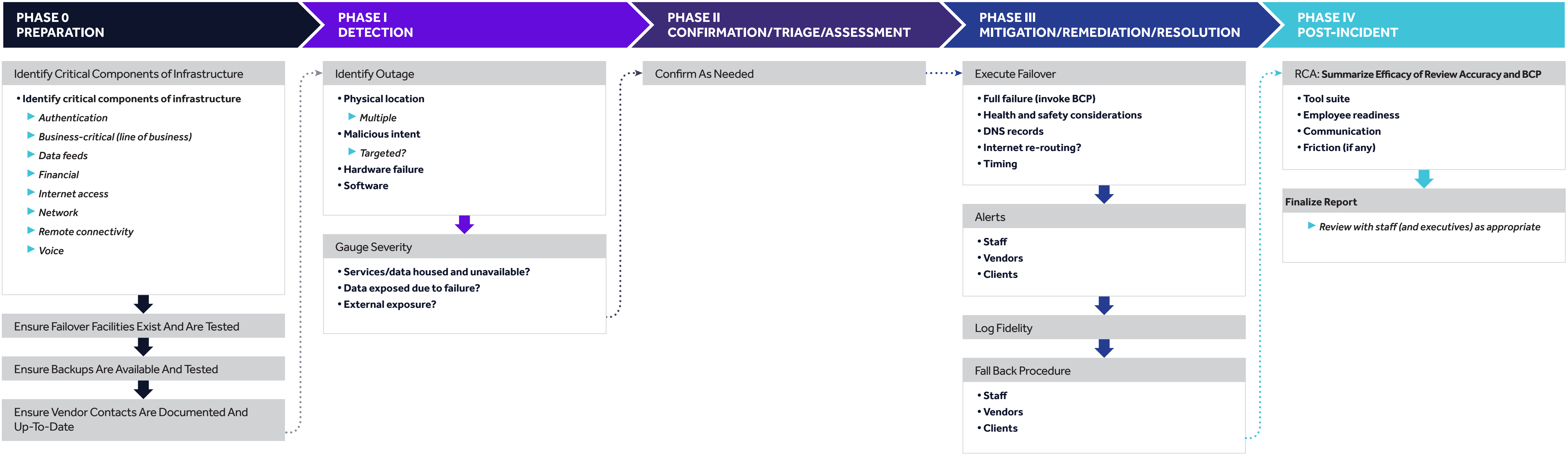
Root Cause Analysis
- Summarize Vector
- Review Tool suite
  - *Employee readiness*
  - *Communication*
  - *Defenses*

Forensics
- Perform or Continue
- Ensure chain of custody is maintained throughout

Finalize Report
- Review with staff (and exec staff) as appropriate

Breach Compliance
- Enlist GC, external legal counsel
- Regulators, LE as deemed appropriate

Infrastructure Outage (Internal)



PHASE 0
PREPARATION

Identify Critical Components of Infrastructure

- **Identify critical components of infrastructure**
  - *Authentication*
  - *Business-critical (line of business)*
  - *Data feeds*
  - *Financial*
  - *Internet access*
  - *Network*
  - *Remote connectivity*
  - *Voice*

Ensure Failover Facilities Exist And Are Tested

Ensure Backups Are Available And Tested

Ensure Vendor Contacts Are Documented And Up-To-Date

PHASE I
DETECTION

Identify Outage

- **Physical location**
  - *Multiple*
- **Malicious intent**
  - *Targeted?*
- **Hardware failure**
- **Software**

Gauge Severity

- **Services/data housed and unavailable?**
- **Data exposed due to failure?**
- **External exposure?**

PHASE II
CONFIRMATION/TRIAGE/ASSESSMENT

Confirm As Needed

PHASE III
MITIGATION/REMEDIATION/RESOLUTION

Execute Failover

- **Full failure (invoke BCP)**
- **Health and safety considerations**
- **DNS records**
- **Internet re-routing?**
- **Timing**

Alerts

- **Staff**
- **Vendors**
- **Clients**

Log Fidelity

Fall Back Procedure

- **Staff**
- **Vendors**
- **Clients**

PHASE IV
POST-INCIDENT

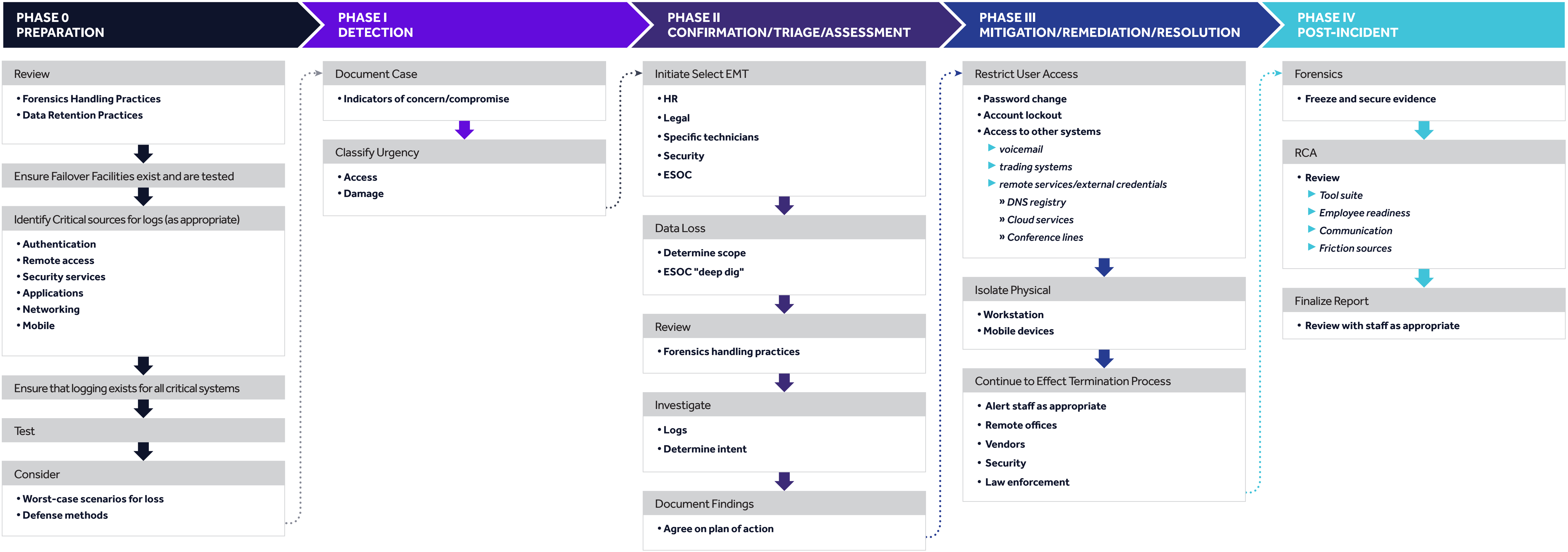
RCA: **Summarize Efficacy of Review Accuracy and BCP**

- **Tool suite**
- **Employee readiness**
- **Communication**
- **Friction (if any)**

Finalize Report

- *Review with staff (and executives) as appropriate*

Local Access W/O Auth (Non-Malware)



PHASE 0 PREPARATION

Review
- Forensics Handling Practices
- Data Retention Practices

Ensure Failover Facilities exist and are tested

Identify Critical sources for logs (as appropriate)
- Authentication
- Remote access
- Security services
- Applications
- Networking
- Mobile

Ensure that logging exists for all critical systems

Test

Consider
- Worst-case scenarios for loss
- Defense methods

PHASE I DETECTION

Document Case
- Indicators of concern/compromise

Classify Urgency
- Access
- Damage

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT
- HR
- Legal
- Specific technicians
- Security
- ESOC

Data Loss
- Determine scope
- ESOC "deep dig"

Review
- Forensics handling practices

Investigate
- Logs
- Determine intent

Document Findings
- Agree on plan of action

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Restrict User Access
- Password change
- Account lockout
- Access to other systems
  - *voicemail*
  - *trading systems*
  - *remote services/external credentials*
    - *DNS registry*
    - *Cloud services*
    - *Conference lines*

Isolate Physical
- Workstation
- Mobile devices

Continue to Effect Termination Process
- Alert staff as appropriate
- Remote offices
- Vendors
- Security
- Law enforcement

PHASE IV POST-INCIDENT

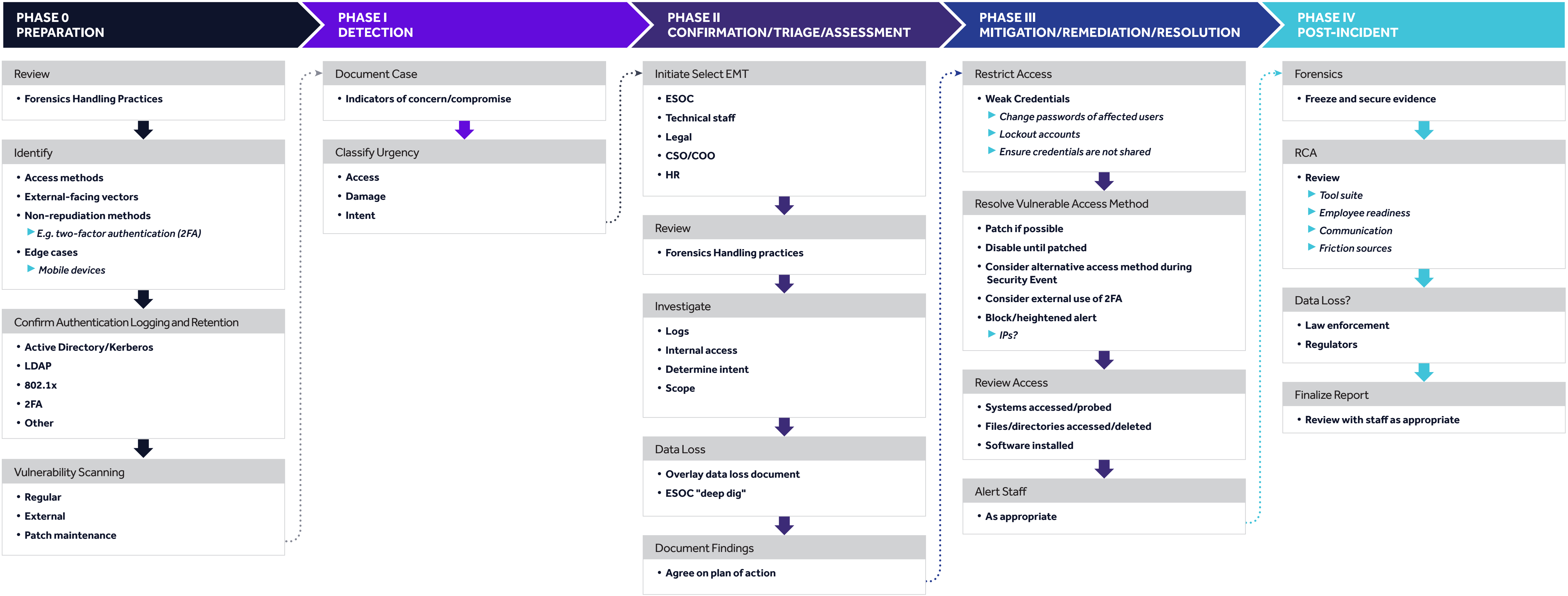
Forensics
- Freeze and secure evidence

RCA
- Review
  - *Tool suite*
  - *Employee readiness*
  - *Communication*
  - *Friction sources*

Finalize Report
- Review with staff as appropriate

Successful Remote Access Without Authorization

eSENTIRE



PHASE 0 PREPARATION

Review
- Forensics Handling Practices

Identify
- Access methods
- External-facing vectors
- Non-repudiation methods
  - *E.g. two-factor authentication (2FA)*
- Edge cases
  - *Mobile devices*

Confirm Authentication Logging and Retention
- Active Directory/Kerberos
- LDAP
- 802.1x
- 2FA
- Other

Vulnerability Scanning
- Regular
- External
- Patch maintenance

PHASE I DETECTION

Document Case
- Indicators of concern/compromise

Classify Urgency
- Access
- Damage
- Intent

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT
- ESOC
- Technical staff
- Legal
- CSO/COO
- HR

Review
- Forensics Handling practices

Investigate
- Logs
- Internal access
- Determine intent
- Scope

Data Loss
- Overlay data loss document
- ESOC "deep dig"

Document Findings
- Agree on plan of action

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Restrict Access
- Weak Credentials
  - *Change passwords of affected users*
  - *Lockout accounts*
  - *Ensure credentials are not shared*

Resolve Vulnerable Access Method
- Patch if possible
- Disable until patched
- Consider alternative access method during Security Event
- Consider external use of 2FA
- Block/heightened alert
  - *IPs?*

Review Access
- Systems accessed/probed
- Files/directories accessed/deleted
- Software installed

Alert Staff
- As appropriate

PHASE IV POST-INCIDENT

Forensics
- Freeze and secure evidence

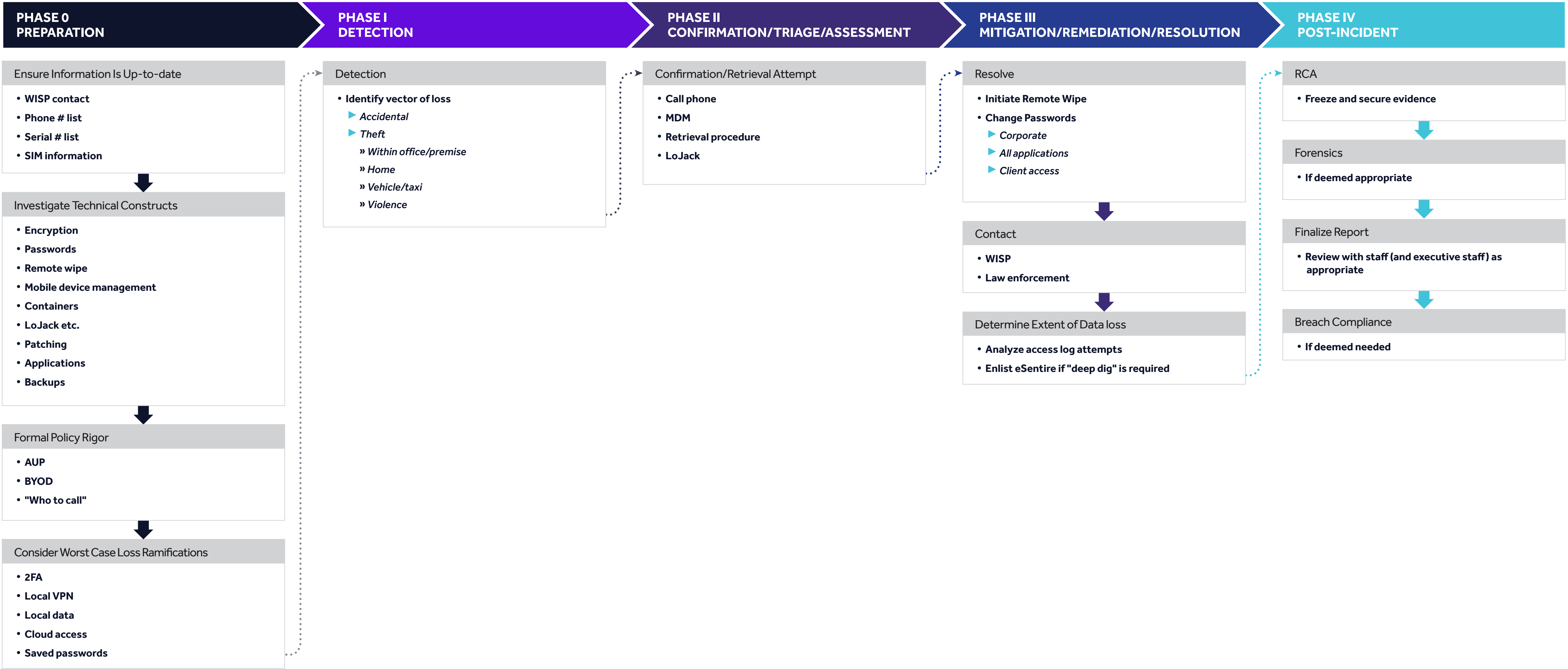
RCA
- Review
  - *Tool suite*
  - *Employee readiness*
  - *Communication*
  - *Friction sources*

Data Loss?
- Law enforcement
- Regulators

Finalize Report
- Review with staff as appropriate

Lost/Stolen Devices

eSENTIRE



PHASE 0
PREPARATION

Ensure Information Is Up-to-date

- **WISP contact**
- **Phone # list**
- **Serial # list**
- **SIM information**

Investigate Technical Constructs

- **Encryption**
- **Passwords**
- **Remote wipe**
- **Mobile device management**
- **Containers**
- **LoJack etc.**
- **Patching**
- **Applications**
- **Backups**

Formal Policy Rigor

- **AUP**
- **BYOD**
- **"Who to call"**

Consider Worst Case Loss Ramifications

- **2FA**
- **Local VPN**
- **Local data**
- **Cloud access**
- **Saved passwords**

PHASE I
DETECTION

Detection

- **Identify vector of loss**
  - *Accidental*
  - *Theft*
    - *Within office/premise*
    - *Home*
    - *Vehicle/taxi*
    - *Violence*

PHASE II
CONFIRMATION/TRIAGE/ASSESSMENT

Confirmation/Retrieval Attempt

- **Call phone**
- **MDM**
- **Retrieval procedure**
- **LoJack**

PHASE III
MITIGATION/REMEDIATION/RESOLUTION

Resolve

- **Initiate Remote Wipe**
- **Change Passwords**
  - *Corporate*
  - *All applications*
  - *Client access*

Contact

- **WISP**
- **Law enforcement**

Determine Extent of Data loss

- **Analyze access log attempts**
- **Enlist eSentire if "deep dig" is required**

PHASE IV
POST-INCIDENT

RCA

- **Freeze and secure evidence**

Forensics

- **If deemed appropriate**

Finalize Report

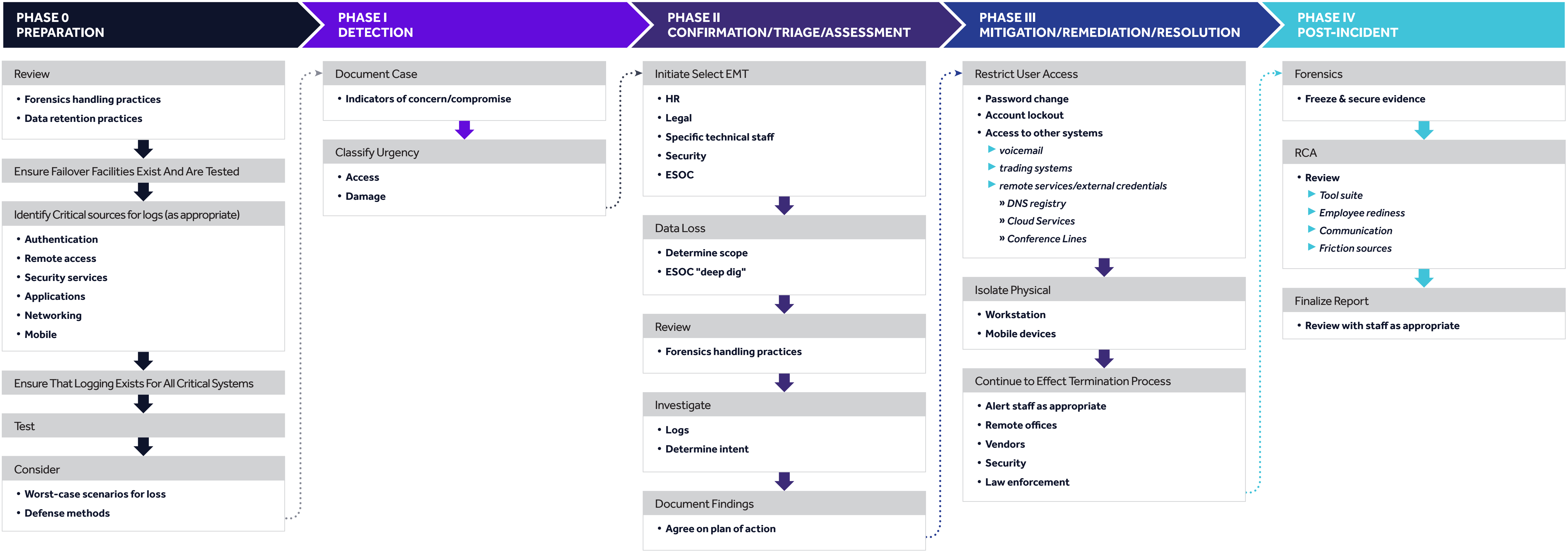
- **Review with staff (and executive staff) as appropriate**

Breach Compliance

- **If deemed needed**

Inappropriate Behavior

eSENTIRE



PHASE 0 PREPARATION

Review
- Forensics handling practices
- Data retention practices

Ensure Failover Facilities Exist And Are Tested

Identify Critical sources for logs (as appropriate)
- Authentication
- Remote access
- Security services
- Applications
- Networking
- Mobile

Ensure That Logging Exists For All Critical Systems

Test

Consider
- Worst-case scenarios for loss
- Defense methods

PHASE I DETECTION

Document Case
- Indicators of concern/compromise

Classify Urgency
- Access
- Damage

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT
- HR
- Legal
- Specific technical staff
- Security
- ESOC

Data Loss
- Determine scope
- ESOC "deep dig"

Review
- Forensics handling practices

Investigate
- Logs
- Determine intent

Document Findings
- Agree on plan of action

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Restrict User Access
- Password change
- Account lockout
- Access to other systems
  - *voicemail*
  - *trading systems*
  - *remote services/external credentials*
    - » *DNS registry*
    - » *Cloud Services*
    - » *Conference Lines*

Isolate Physical
- Workstation
- Mobile devices

Continue to Effect Termination Process
- Alert staff as appropriate
- Remote offices
- Vendors
- Security
- Law enforcement

PHASE IV POST-INCIDENT

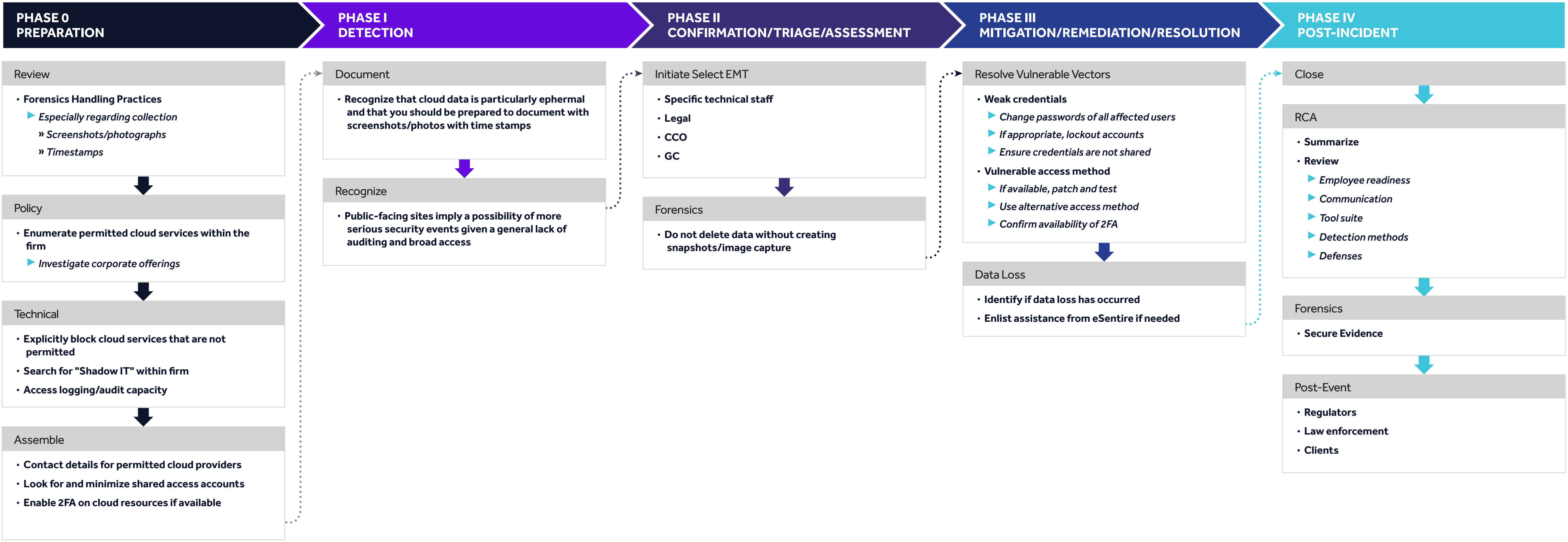
Forensics
- Freeze & secure evidence

RCA
- Review
  - *Tool suite*
  - *Employee rediness*
  - *Communication*
  - *Friction sources*

Finalize Report
- Review with staff as appropriate

Cloud Service Access W/O Autha

eSENTIRE



PHASE 0 PREPARATION

Review

- Forensics Handling Practices
  - *Especially regarding collection*
    - *» Screenshots/photographs*
    - *» Timestamps*

Policy

- Enumerate permitted cloud services within the firm
  - *Investigate corporate offerings*

Technical

- Explicitly block cloud services that are not permitted
- Search for "Shadow IT" within firm
- Access logging/audit capacity

Assemble

- Contact details for permitted cloud providers
- Look for and minimize shared access accounts
- Enable 2FA on cloud resources if available

PHASE I DETECTION

Document

- Recognize that cloud data is particularly ephermal and that you should be prepared to document with screenshots/photos with time stamps

Recognize

- Public-facing sites imply a possibility of more serious security events given a general lack of auditing and broad access

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT

- Specific technical staff
- Legal
- CCO
- GC

Forensics

- Do not delete data without creating snapshots/image capture

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Resolve Vulnerable Vectors

- Weak credentials
  - *Change passwords of all affected users*
  - *If appropriate, lockout accounts*
  - *Ensure credentials are not shared*
- Vulnerable access method
  - *If available, patch and test*
  - *Use alternative access method*
  - *Confirm availability of 2FA*

Data Loss

- Identify if data loss has occurred
- Enlist assistance from eSentire if needed

PHASE IV POST-INCIDENT

Close

RCA

- Summarize
- Review
  - *Employee readiness*
  - *Communication*
  - *Tool suite*
  - *Detection methods*
  - *Defenses*

Forensics

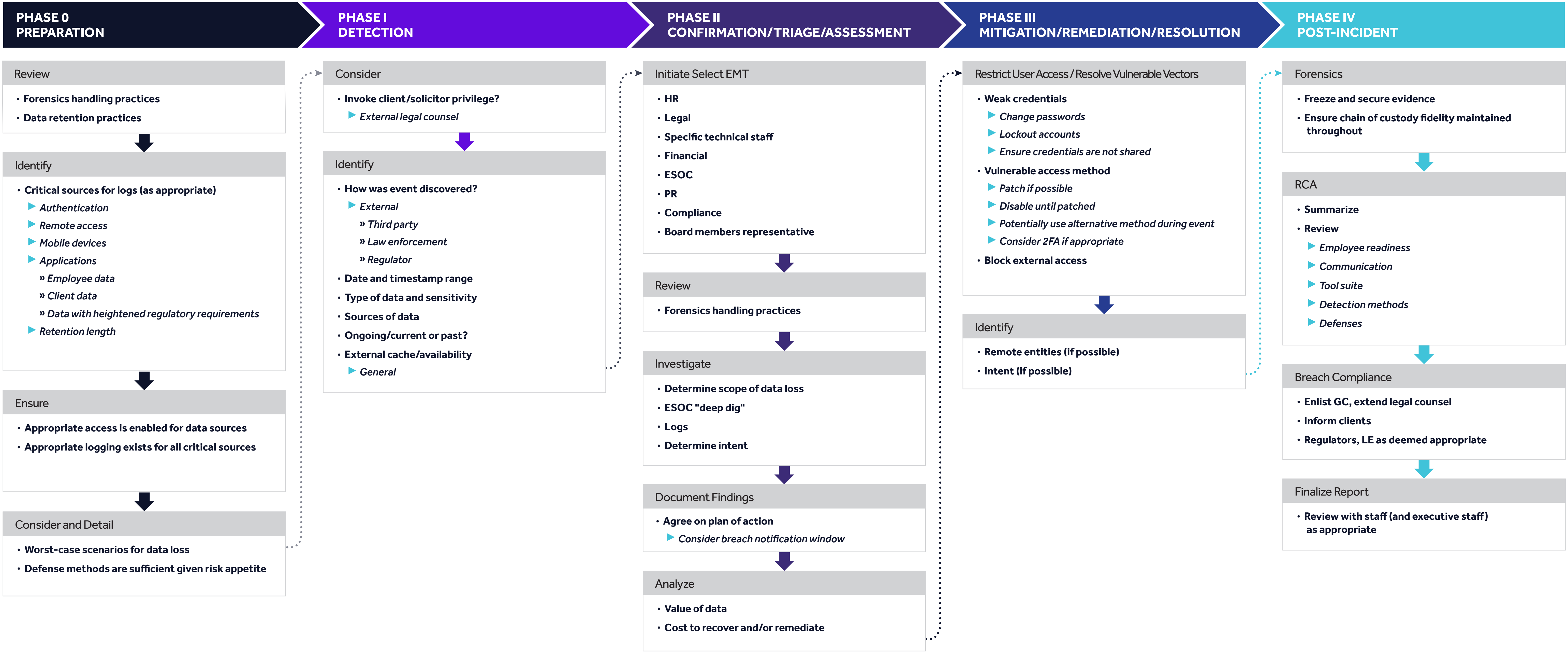
- Secure Evidence

Post-Event

- Regulators
- Law enforcement
- Clients

Data Loss/Extrusion

eSENTIRE



PHASE 0 PREPARATION

Review

- Forensics handling practices
- Data retention practices

Identify

- Critical sources for logs (as appropriate)
  - *Authentication*
  - *Remote access*
  - *Mobile devices*
  - *Applications*
    - *Employee data*
    - *Client data*
    - *Data with heightened regulatory requirements*
  - *Retention length*

Ensure

- Appropriate access is enabled for data sources
- Appropriate logging exists for all critical sources

Consider and Detail

- Worst-case scenarios for data loss
- Defense methods are sufficient given risk appetite

PHASE I DETECTION

Consider

- Invoke client/solicitor privilege?
  - *External legal counsel*

Identify

- How was event discovered?
  - *External*
    - *Third party*
    - *Law enforcement*
    - *Regulator*
- Date and timestamp range
- Type of data and sensitivity
- Sources of data
- Ongoing/current or past?
- External cache/availability
  - *General*

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT

- HR
- Legal
- Specific technical staff
- Financial
- ESOC
- PR
- Compliance
- Board members representative

Review

- Forensics handling practices

Investigate

- Determine scope of data loss
- ESOC "deep dig"
- Logs
- Determine intent

Document Findings

- Agree on plan of action
  - *Consider breach notification window*

Analyze

- Value of data
- Cost to recover and/or remediate

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Restrict User Access / Resolve Vulnerable Vectors

- Weak credentials
  - *Change passwords*
  - *Lockout accounts*
  - *Ensure credentials are not shared*
- Vulnerable access method
  - *Patch if possible*
  - *Disable until patched*
  - *Potentially use alternative method during event*
  - *Consider 2FA if appropriate*
- Block external access

Identify

- Remote entities (if possible)
- Intent (if possible)

PHASE IV POST-INCIDENT

Forensics

- Freeze and secure evidence
- Ensure chain of custody fidelity maintained throughout

RCA

- Summarize
- Review
  - *Employee readiness*
  - *Communication*
  - *Tool suite*
  - *Detection methods*
  - *Defenses*

Breach Compliance

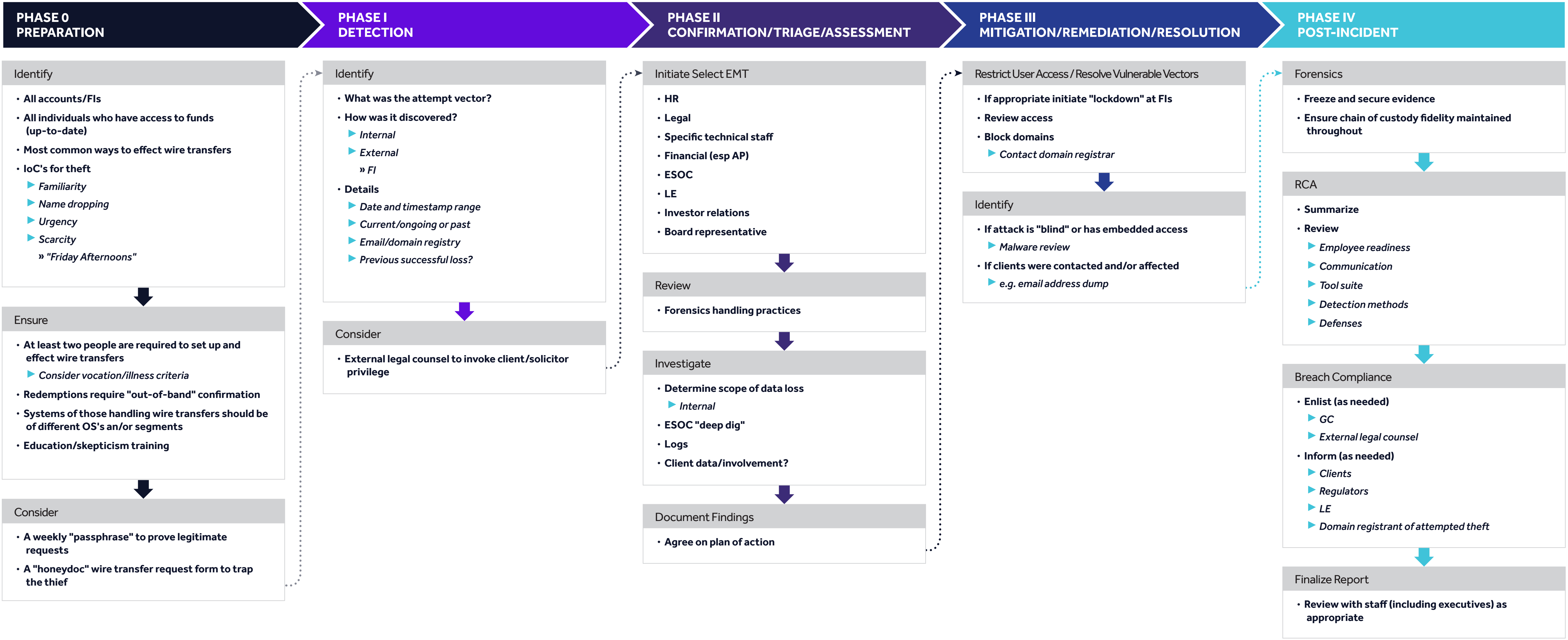
- Enlist GC, extend legal counsel
- Inform clients
- Regulators, LE as deemed appropriate

Finalize Report

- Review with staff (and executive staff) as appropriate

Direct Financial Loss (Non-Physical Theft, Including Attempts)

eSENTIRE



PHASE 0 PREPARATION

Identify

- All accounts/FIs
- All individuals who have access to funds (up-to-date)
- Most common ways to effect wire transfers
- IoC's for theft
  - *Familiarity*
  - *Name dropping*
  - *Urgency*
  - *Scarcity*
    - *"Friday Afternoons"*

Ensure

- At least two people are required to set up and effect wire transfers
  - *Consider vocation/illness criteria*
- Redemptions require "out-of-band" confirmation
- Systems of those handling wire transfers should be of different OS's an/or segments
- Education/skepticism training

Consider

- A weekly "passphrase" to prove legitimate requests
- A "honeydoc" wire transfer request form to trap the thief

PHASE I DETECTION

Identify

- What was the attempt vector?
- How was it discovered?
  - *Internal*
  - *External*
    - *FI*
- Details
  - *Date and timestamp range*
  - *Current/ongoing or past*
  - *Email/domain registry*
  - *Previous successful loss?*

Consider

- External legal counsel to invoke client/solicitor privilege

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT

- HR
- Legal
- Specific technical staff
- Financial (esp AP)
- ESOC
- LE
- Investor relations
- Board representative

Review

- Forensics handling practices

Investigate

- Determine scope of data loss
  - *Internal*
- ESOC "deep dig"
- Logs
- Client data/involvement?

Document Findings

- Agree on plan of action

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Restrict User Access / Resolve Vulnerable Vectors

- If appropriate initiate "lockdown" at FIs
- Review access
- Block domains
  - *Contact domain registrar*

Identify

- If attack is "blind" or has embedded access
  - *Malware review*
- If clients were contacted and/or affected
  - *e.g. email address dump*

PHASE IV POST-INCIDENT

Forensics

- Freeze and secure evidence
- Ensure chain of custody fidelity maintained throughout

RCA

- Summarize
- Review
  - *Employee readiness*
  - *Communication*
  - *Tool suite*
  - *Detection methods*
  - *Defenses*

Breach Compliance

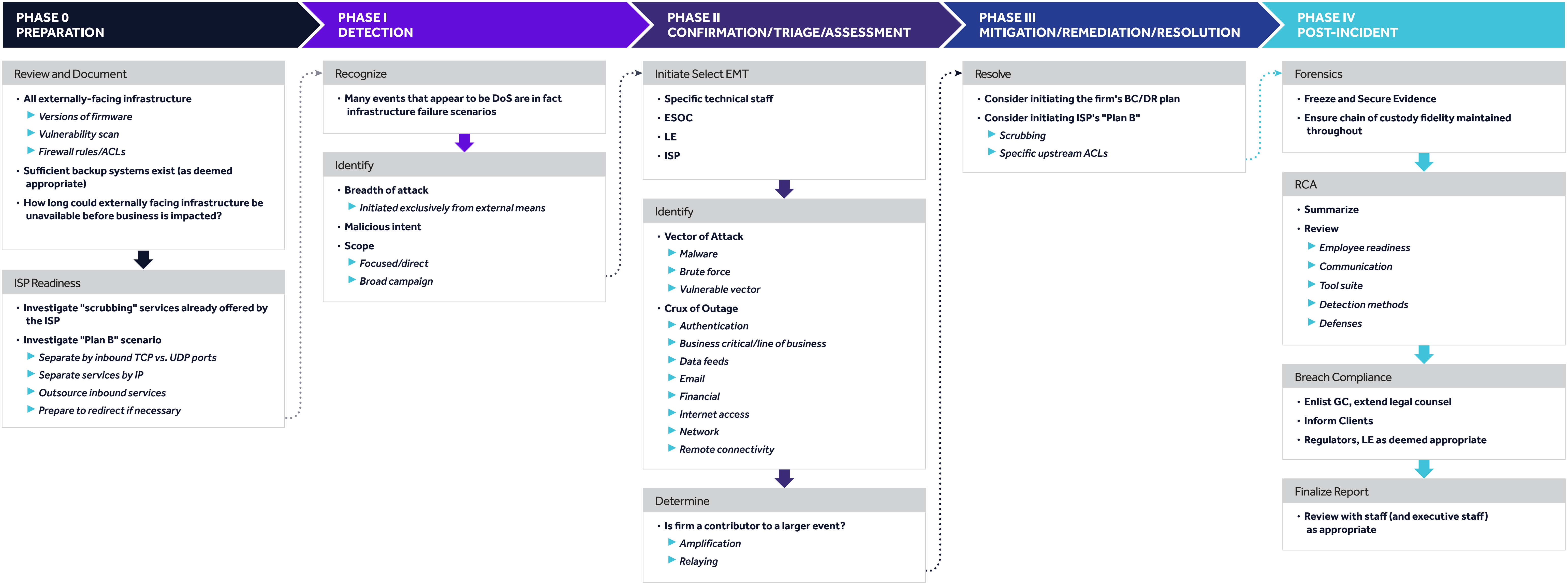
- Enlist (as needed)
  - *GC*
  - *External legal counsel*
- Inform (as needed)
  - *Clients*
  - *Regulators*
  - *LE*
  - *Domain registrant of attempted theft*

Finalize Report

- Review with staff (including executives) as appropriate

Denial of Service (External)

eSENTIRE



PHASE 0 PREPARATION

Review and Document

- **All externally-facing infrastructure**
  - *Versions of firmware*
  - *Vulnerability scan*
  - *Firewall rules/ACLs*
- **Sufficient backup systems exist (as deemed appropriate)**
- **How long could externally facing infrastructure be unavailable before business is impacted?**

ISP Readiness

- **Investigate "scrubbing" services already offered by the ISP**
- **Investigate "Plan B" scenario**
  - *Separate by inbound TCP vs. UDP ports*
  - *Separate services by IP*
  - *Outsource inbound services*
  - *Prepare to redirect if necessary*

PHASE I DETECTION

Recognize

- **Many events that appear to be DoS are in fact infrastructure failure scenarios**

Identify

- **Breadth of attack**
  - *Initiated exclusively from external means*
- **Malicious intent**
- **Scope**
  - *Focused/direct*
  - *Broad campaign*

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Select EMT

- **Specific technical staff**
- **ESOC**
- **LE**
- **ISP**

Identify

- **Vector of Attack**
  - *Malware*
  - *Brute force*
  - *Vulnerable vector*
- **Crux of Outage**
  - *Authentication*
  - *Business critical/line of business*
  - *Data feeds*
  - *Email*
  - *Financial*
  - *Internet access*
  - *Network*
  - *Remote connectivity*

Determine

- **Is firm a contributor to a larger event?**
  - *Amplification*
  - *Relaying*

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Resolve

- **Consider initiating the firm's BC/DR plan**
- **Consider initiating ISP's "Plan B"**
  - *Scrubbing*
  - *Specific upstream ACLs*

PHASE IV POST-INCIDENT

Forensics

- **Freeze and Secure Evidence**
- **Ensure chain of custody fidelity maintained throughout**

RCA

- **Summarize**
- **Review**
  - *Employee readiness*
  - *Communication*
  - *Tool suite*
  - *Detection methods*
  - *Defenses*

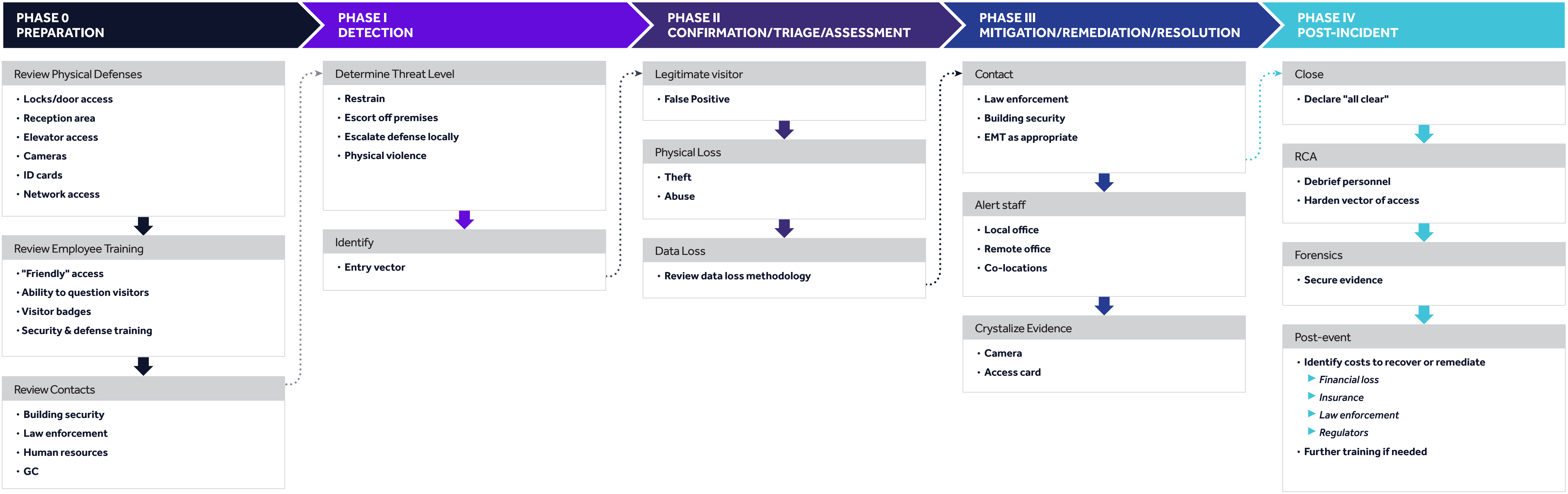
Breach Compliance

- **Enlist GC, extend legal counsel**
- **Inform Clients**
- **Regulators, LE as deemed appropriate**

Finalize Report

- **Review with staff (and executive staff) as appropriate**

Physical Breach



PHASE 0 PREPARATION

Review Physical Defenses

- Locks/door access
- Reception area
- Elevator access
- Cameras
- ID cards
- Network access

Review Employee Training

- "Friendly" access
- Ability to question visitors
- Visitor badges
- Security & defense training

Review Contacts

- Building security
- Law enforcement
- Human resources
- GC

PHASE I DETECTION

Determine Threat Level

- Restrain
- Escort off premises
- Escalate defense locally
- Physical violence

Identify

- Entry vector

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Legitimate visitor

- False Positive

Physical Loss

- Theft
- Abuse

Data Loss

- Review data loss methodology

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Contact

- Law enforcement
- Building security
- EMT as appropriate

Alert staff

- Local office
- Remote office
- Co-locations

Crystalize Evidence

- Camera
- Access card

PHASE IV POST-INCIDENT

Close

- Declare "all clear"

RCA

- Debrief personnel
- Harden vector of access

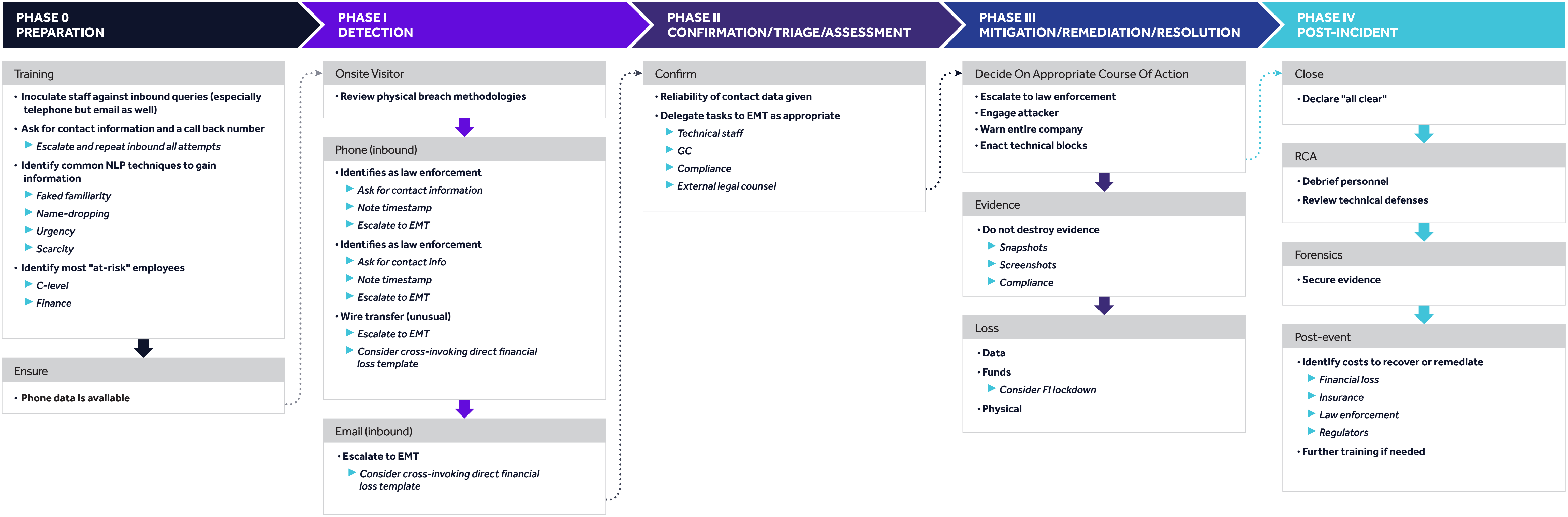
Forensics

- Secure evidence

Post-event

- Identify costs to recover or remediate
  - *Financial loss*
  - *Insurance*
  - *Law enforcement*
  - *Regulators*
- Further training if needed

Social Engineering



PHASE 0 PREPARATION

Training

- Inoculate staff against inbound queries (especially telephone but email as well)
- Ask for contact information and a call back number
  - *Escalate and repeat inbound all attempts*
- Identify common NLP techniques to gain information
  - *Faked familiarity*
  - *Name-dropping*
  - *Urgency*
  - *Scarcity*
- Identify most "at-risk" employees
  - *C-level*
  - *Finance*

Ensure

- Phone data is available

PHASE I DETECTION

Onsite Visitor

- Review physical breach methodologies

Phone (inbound)

- Identifies as law enforcement
  - *Ask for contact information*
  - *Note timestamp*
  - *Escalate to EMT*
- Identifies as law enforcement
  - *Ask for contact info*
  - *Note timestamp*
  - *Escalate to EMT*
- Wire transfer (unusual)
  - *Escalate to EMT*
  - *Consider cross-invoking direct financial loss template*

Email (inbound)

- Escalate to EMT
  - *Consider cross-invoking direct financial loss template*

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Confirm

- Reliability of contact data given
- Delegate tasks to EMT as appropriate
  - *Technical staff*
  - *GC*
  - *Compliance*
  - *External legal counsel*

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Decide On Appropriate Course Of Action

- Escalate to law enforcement
- Engage attacker
- Warn entire company
- Enact technical blocks

Evidence

- Do not destroy evidence
  - *Snapshots*
  - *Screenshots*
  - *Compliance*

Loss

- Data
- Funds
  - *Consider FI lockdown*
- Physical

PHASE IV POST-INCIDENT

Close

- Declare "all clear"

RCA

- Debrief personnel
- Review technical defenses

Forensics

- Secure evidence

Post-event

- Identify costs to recover or remediate
  - *Financial loss*
  - *Insurance*
  - *Law enforcement*
  - *Regulators*
- Further training if needed

Ransomware

eSENTIRE

PHASE 0 PREPARATION

Ensure all systems are up-to-date

- **Workstations, Servers (including internal and DMZ)**
  - *Patching, where possible.*
  - *Antivirus, anti-exploit (e.g. EMET), application whitelisting (e.g. AppLocker)*
  - *Restrict downloading of applications and payloads (network application control)*
- **Mobile Devices**
  - *MDM (patching, restricting applications, downloads)*

Ensure backups of critical systems and data are successful and available

- **Test regularly for content accuracy**
- **Back up important data offline**

Restrict Access

- **Enforce "least-privilege" access throughout filesystems**
- **Segment network**
  - *Restrict workstation-to- workstation access*
  - *Utilize jump box for important and critical parts of network*
- **Log access attempts to shares that get denied (early signs of infestation)**

Reduce Susceptibility Footprint

- **Reduce inbound vectors (e.g. personal email)**
- **Disable macros within Microsoft Office if not needed**
- **Use Microsoft Viewer software if editing of Office documents is not needed for all tasks (especially when viewing suspect documents)**
- **Improve/Harden upstream SMTP attachment scanning and quarantine**
  - *Block .zip, .exe, .js, .html*
  - *PTR/SPF records for anti-spoofing protection*

Training

- **Inoculate skepticism in end-users**
  - *Security Awareness Training*
  - *Phishing test campaigns*
  - *Weekly reminders/ postings*

Alerting

- **Implement behavior-based alerting when a certain threshold of files are modified**
- **Implement a Continuous Monitoring/Embedded Incident Response methodology**

PHASE I DETECTION

Formal Initiation of Event

- **Note timestamp and method of discovery**
- **Identify "patient(s) zero"**
  - *External*
    - *» FI*
  - *Workstation*
    - *» single or multiple?*
  - *Server*
    - *» single or multiple?*
  - *Mobile Device*
    - *» single or multiple?*
  - *Accounts*
    - *» single or multiple?*
  - *Blend of the above*

PHASE II CONFIRMATION/TRIAGE/ASSESSMENT

Initiate Event Data Cull if manpower permits, otherwise immediately move to PHASE III.

PHASE III MITIGATION/REMEDIATION/RESOLUTION

Contain

- **Is isolation possible?**
- **What is the impact of isolation?**
- **Is there a need for the BC/DR Plan to be put into effect?**
- **Method**
  - *Manual disconnect*
    - *» Cable*
    - *» Wireless*
    - *» Antenna disable (mobile device)*
  - *Switch port disable*
  - *Wireless controller access disable*

Identify

- **Breadth of the filesystem affected**
- **Impact and sensitivity of the files lost**

Analyze

- **Affected systems for possible multi-pronged/method attack**
- **Vestigial artifacts left on affected systems**
- **Network indicators**
  - *Payload transfer/droppers*
  - *Command and control channels/covert channels*
  - *Data loss/file extrusion*

Eradicate

- **Implement IP blocks (on firewall) if deemed appropriate**
- **Alert staff to indicators derived from attack**

Recovery

- **Initiate file recovery**
- **Verify backups not affected**
  - *Check shadow copies (system restore)*
- **Wipe affected systems**
  - *if needed*
  - *when convenient*
  - *and analytics completed*

PHASE IV POST-INCIDENT

Confirm "All Clear" Event

- **Note timestamp for formal records**

Update and Secure Documentation

Root Cause Analysis

- **Present findings to management**

Enhance Response Capabilities

- **Present findings to management**

Pragmatic Security Event Management Playbook

Purpose of Playbook

The eSentire Pragmatic Security Event Management Playbook aims to provide structure and guidance when responding to a variety of security events that require a concerted response. It lists the members of the security event management team (EMT) with contact information, describes the hierarchy, defines their responsibilities and provides a structure to deal with an evolving situation.

Each organization differs in culture, hierarchy, critical data and systems. As such, it is critical that this framework be modified to best reflect the actions to take when an event necessitating action occurs. No "one size fits all" security event management program exists.

The first 24 hours after a security event is identified are critical to restore functionality, identify and mitigate threats; identify the appropriate blend of forensic analysis to perform versus returning to fully operational ("all-clear") status and to comply with fiduciary and legal responsibilities. The Pragmatic Security Event Management Playbook is intended to guide the EMT through the "fog of war" during an event to ensure that crucial steps are not missed and that steps to event resolution are agreed upon in advance.

Executive Summary

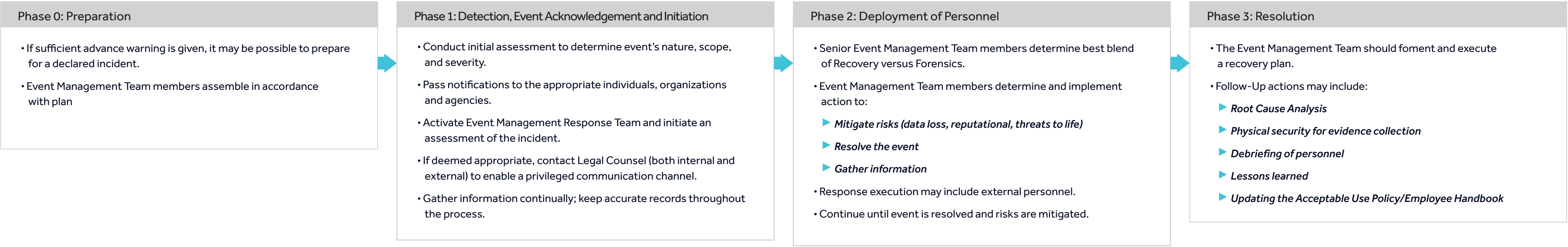
The overall purpose of this document is to provide guidelines to protect, preserve and ensure the availability, integrity and confidentiality of the company's information and network assets, regardless of format. In order to accomplish this goal, the program has the following objectives:

- Within a predefined framework, control and manage unauthorized access or computer attack incidents
- Permit for the timely investigation of incidents, given the defined priority (taking into account each event's severity)
- Take all measures as appropriate to contain and control damage to customers (including employees) resulting from the security incident and to preserve evidence related to the incident
- Return to normal operating conditions as quickly as possible by mitigating ongoing computer attacks or by executing a timely recovery
- As appropriate, notify the regulatory and law enforcement authorities and affected parties of the security event in accordance with applicable law

Event Response Priorities

1. Ensure the safety of staff.
2. Fulfill key fiduciary responsibilities and legal obligations.
3. Protect public, shareholder and investor confidence.
4. Resume business operation as soon as feasible.
5. Ensure financial loss will not exceed tolerances.
6. As best as possible, fully document actions taken, with care taken to not destroy evidence, while maintaining a forensic chain of custody.

Four Phases of Event Management Team Operations



Phase 0: Preparation

- If sufficient advance warning is given, it may be possible to prepare for a declared incident.
- Event Management Team members assemble in accordance with plan

Phase 1: Detection, Event Acknowledgement and Initiation

- Conduct initial assessment to determine event's nature, scope, and severity.
- Pass notifications to the appropriate individuals, organizations and agencies.
- Activate Event Management Response Team and initiate an assessment of the incident.
- If deemed appropriate, contact Legal Counsel (both internal and external) to enable a privileged communication channel.
- Gather information continually; keep accurate records throughout the process.

Phase 2: Deployment of Personnel

- Senior Event Management Team members determine best blend of Recovery versus Forensics.
- Event Management Team members determine and implement action to:
  - ▶ *Mitigate risks (data loss, reputational, threats to life)*
  - ▶ *Resolve the event*
  - ▶ *Gather information*
- Response execution may include external personnel.
- Continue until event is resolved and risks are mitigated.

Phase 3: Resolution

- The Event Management Team should foment and execute a recovery plan.
- Follow-Up actions may include:
  - ▶ *Root Cause Analysis*
  - ▶ *Physical security for evidence collection*
  - ▶ *Debriefing of personnel*
  - ▶ *Lessons learned*
  - ▶ *Updating the Acceptable Use Policy/Employee Handbook*

Pragmatic Security Event Management Playbook Cont'd

eSENTIRE

Event Management Team (CORE)

Event Management Team Leader

- Lead event management team
- Activates event management organization
- Acts as incident commander in order to ensure a coordinated, timely and effective response to threats
- Coordinates assessment of threat/incident
  - ***Reviews event severity level***
    - ***Confirm***
    - ***Modify***
    - ***Escalate as needed***
- Acts as liason to executive team
  - ***Receives direction as appropriate***
- Ensures appropriate teams/personnel are assembled as appropriate to respond to event
- Declares completion of event
- Cotordinates root cause analysis post-event
- Participates in, and coordinates event management drills, exercises, training
- Ensures that event management response procedures are appropriate going forward

Facilities/Physical Security Representative

- Provides assessment of facility-related issues
  - ***Severity level***
- Coordinates facility-related response
  - ***Security of affected facilities***
  - ***Restore damaged facilities***
  - ***Obtain additional space if required***
- Provide intelligence and assessment of threats
- Liaise with external entities to gather/evaluate threats
- Coordinate physical security response associated with proposed/planned response
- Participates in root cause analysis post-event
- Participates in event management drills, exercises and training

Line of Business Representative **(one from each Line of Business)**

- Advise on the business impact of events
  - ***Severity***
  - ***Proposed response***
  - ***Recovery actions***
- Provide material as appropriate to public affairs/communications to permit crafting of stakeholder messaging as appropriate
- Participate in root cause analysis post-event
- Participate in event management drills, exercises and training

Event Team Coordinator

- Assist event management team leader
- Monitor events that could impact and/or require escalation to the event management team
- Gather information regarding threats/events with potential to affect company
- Make recommendations regarding:
  - ***Assembling the event management team***
  - ***Improving the event management process***
- Acts as Proxy for event management team leader when tasked by same
- Notify event management team as needed
- Activate event management command center
- Participates in root cause analysis post-event
- Assist in the design and coordination of event management drills, exercises and training

Compliance/Risk/Finance Representative

- Advises on financial aspects of proposed/planned response
  - ***Estimate costs to determine appropriate extent of response***
  - ***Allocate appropriate sources of funding to cover response activity***
  - ***Coordinates accounting for expenditurest***
- Help to develop effective response actions while minimizing financial impact
- Coordinate insurance issues (as appropriate)
- Advises on issues regarding regulation with financial impact (e.g. privacy)
- Participates in root cause analysis post-event
- Participates in event management drills, exercises and training

Human Resources Representative

- Advises on HR issues associated with proposed or planned response activities and severity level
- Coordinate employee and dependent support programs
- Acquire temporary personnel or arrange to redeploy personnel based on requirements
- Arrange for transportation/lodging for redeployed personnel
- Advise on compensation/benefits
  - ***Including medical, health risks, assistance and welfare***
- Participate in root cause analysis
- Participates in event management drills, exercises and training

Event Management Team Center Support Team Member

- Assists in setup of event management center
- Records event management team discussions
  - ***Prepares meeting minutes***
  - ***Tracks issues***
- Provide administrative support as needed
- Maintain all documentation created/received by event management team
- Record and document all actions with forensic-level detail
  - ***Activities, decisions, problems, inputs, follow-up, tasks, directives, chain of custody transfers***
- Record and document all actions with forensic-level detail
- Participate in root cause analysis
- Participates in event management drills, exercises and training

Technical CxO Representative (CIO/CTO)

- Advises on event's impact to IT
  - ***Severity level***
  - ***Proposed/planned response activities***
- Directs IT activities in support of proposed/planned response activity
- Advises on implications to business
  - ***Issues involving applications, data, business partners, integrators***
- Participates in root cause analysis post-event
- Participates in event management drills, exercises and training

Public Affairs/Relations and Corporate Communications Representative

- Coordinate communication
  - ***Media***
  - ***Employee***
  - ***Customer***
- Monitor media coverage of incident
- Advise on corporate communication aspects of response and recovery action
  - ***Company/brand image***
  - ***Severity level***
- Advises and briefs spokesperson
- Participate in root cause analysis
- Participates in event management drills, exercises and training

Corporate Legal Affairs/General Counsel Representative

- Advises on legal implications of proposed/planned response activities
- Advises on legal responsibilities that arise from event
- Advises on legal methods to contain event
- Advises on legal requirements for
  - ***Protection of records***
  - ***Disclosure***
- Advises on regulatory requirements
- Participate in root cause analysis
- Participates in event management drills, exercises and training

As Needed: Board of Directors Representative

- Advise/speak on behalf of board of directors
- Liaise with core team members where appropriate

As needed: External Vendors
(Applications, Integrators, ISP, Service Providers)

- Advise regarding specific aspects of services provided.
- Assist with forensics, information gathering and remediation (as relating to the service provided)

Event Management Contact List

eSentire Security Operations Center (SOC) – Incident Response

PHONE 1	1.866.579.2200 x3
PHONE 2: ESCALATION 1	+001.519.651.2200 x3
EMAIL	csirt@esentire.com
EMAIL	esoc@esentire.com

War Room Information

PHONE (INTL)	
PHONE (TOLL-FREE)	
LEADER PASSWORD	
PARTICIPANT PASSWORD	
URL	

Event Management Team Leader

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Event Team Coordinator

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Event Management Team Center Support Team Member I

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Event Management Team Center Support Team Member II

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Technical CxO Representative (CIO/CTO)

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Facilities/Physical Security Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Compliance/Risk/Finance Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Human Resources Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Public Affairs/Relations and Corporate Communications Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Corporate Legal Affairs/General Counsel Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

External Legal Counsel Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Line of Business Representative I

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Line of Business Representative II

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Line of Business Representative III

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Line of Business Representative IV

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

Board of Directors Representative

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

External Finance Contact I

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

External Finance Contact II

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

External Vendor I

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

External Vendor II

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

External Vendor III

NAME	
TITLE	
PHONE 1	
2: ESCALATION 1	
3: ESCALATION 2	
EMAIL	
SMS	

eSENTIRE