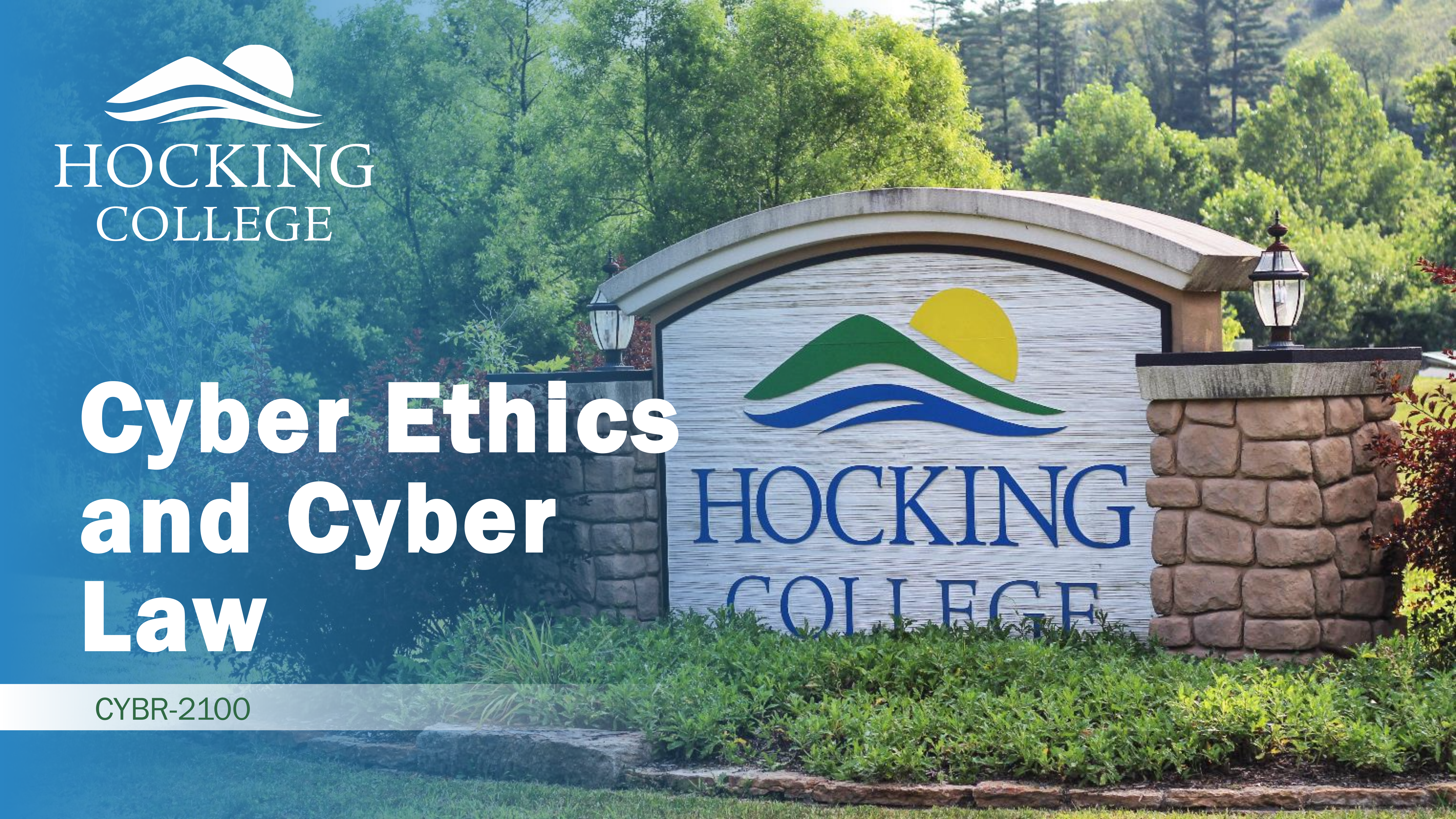
HOCKING
COLLEGE

Cyber Ethics and Cyber Law

CYBR-2100



HOCKING COLLEGE

Incident Response & Evidence Notes

Week 4 - B

Incident & Evidence Notes

Outcomes: Explain the NIST lifecycle in plain language; (2) Write a 1-page Incident & Evidence Note that is complete but minimum necessary; (3) Make a risk-based containment recommendation and justify it.

Why this matters:

Security teams face legal/ethical boundaries during incidents. You'll learn to recognize common cybercrime patterns, act within authorization, and capture minimum, defensible evidence that respects privacy and due process. Our goal: help without harm—to users, to investigations, and to rights.

Ethical Lens:

Minimize harm and professional responsibility. Practice minimum necessary collection and proportional containment . Protecting individuals' privacy rights, sticking to authorization, document truthfully, preserve evidence integrity.

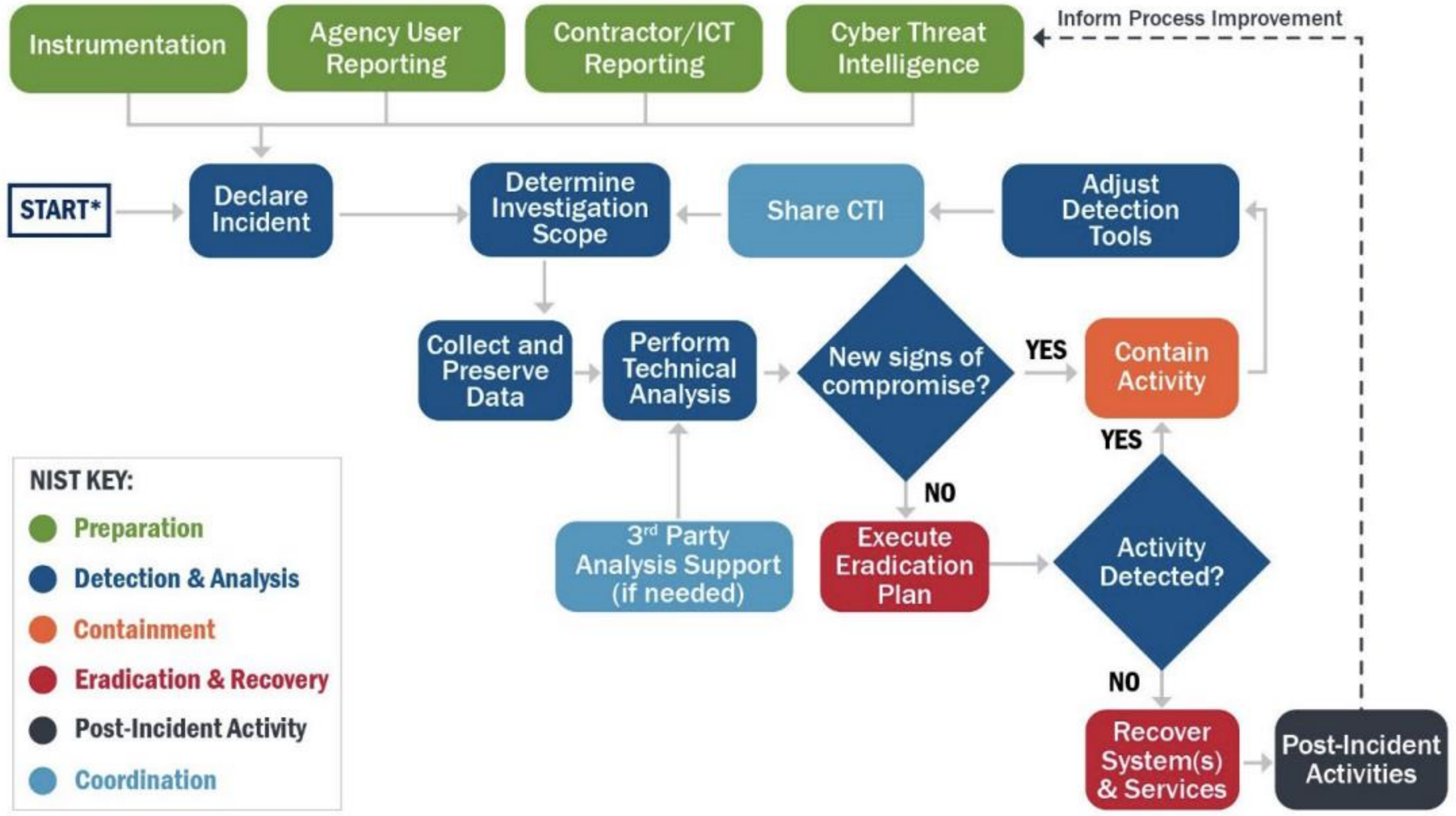
HOCKING
COLLEGE

NIST Cybersecurity Framework (CSF)

- Preparation
- Detection/Analysis
- Containment
- Eradication
- Recovery
- Lessons Learned.

HOCKING
COLLEGE

Incident Response Lifecycle



Instrumentation

Agency User Reporting

Contractor/ICT Reporting

Cyber Threat Intelligence

Inform Process Improvement

START*

Declare Incident

Determine Investigation Scope

Share CTI

Adjust Detection Tools

Collect and Preserve Data

Perform Technical Analysis

New signs of compromise?

YES

Contain Activity

YES

NO

3rd Party Analysis Support (if needed)

Execute Eradication Plan

Activity Detected?

NO

Recover System(s) & Services

Post-Incident Activities

NIST KEY:

- ● Preparation
- ● Detection & Analysis
- ● Containment
- ● Eradication & Recovery
- ● Post-Incident Activity
- ● Coordination

Figure 1: Incident Response Process

- https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

HOCKING COLLEGE

NIST Cybersecurity Framework (CSF) 2.0

- Govern (GV): The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- Identify (ID): The organization’s current cybersecurity risks are understood.
- Protect (PR): Safeguards to manage the organization’s cybersecurity risks are used.
- Detect (DE): Possible cybersecurity attacks and compromises are found and analyzed.
- Respond (RS): Actions regarding a detected cybersecurity incident are taken.
- Recover (RC): Assets and operations affected by a cybersecurity incident are restored.

NIST Cybersecurity Framework (CSF) 2.0

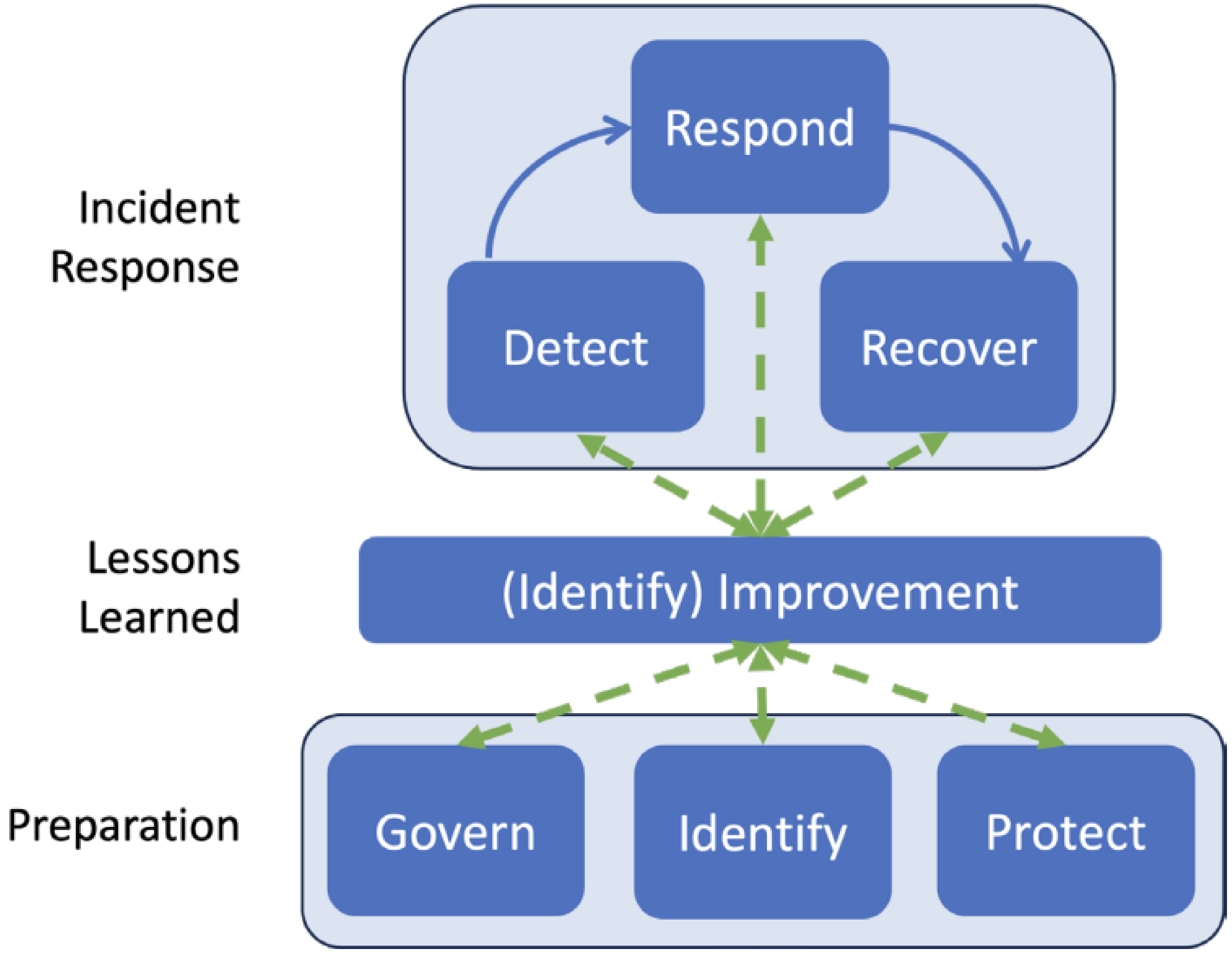


Fig. 2. Incident response life cycle model based on CSF 2.0 Functions

HOCKING
COLLEGE

CSF 2.0 - Govern

- How leadership sets expectations for risk, privacy, and incident authority.
- Context and policy layer that shapes every incident decision, including notification and data handling obligations.
- It answers:
  - *Who can approve what?*
  - *What legal/privacy obligations apply?*
  - *Who gets notified?*
- It sets out the authorization, scope, and privacy constraints.

HOCKING
COLLEGE

CSF 2.0 - Identify

- Know what you’re defending (accounts, devices, apps) and what risks you accept.
- Maps out:
  - What systems are in scope
  - Where logs live
  - Who owns what
  - What “critical” means

CSF 2.0 - Protect

- Safeguards that lower incident frequency/impact
- Including:
  - MFA
  - Role-based access
  - Allow-listed admin tools
  - Email authentication
  - Backups
- Can reduce number of incidents, to teams can focus on higher impact events
- Controls can also slow attackers (harder lateral movement)

HOCKING
COLLEGE

CSF 2.0 - Detect

- Monitoring and analysis to find anomalies and declare incidents.
- Monitoring includes:
  - Networks
  - Endpoints
  - Auth attempts
  - Email/web services
  - Service-provider activity
- Declaring an incident is part of detection
- Don’t wait for certainty before declaring

HOCKING
COLLEGE

CSF 2.0 - Respond

- Highlights documenting what happened, preserving integrity/provenance, and estimating magnitude
- Incident & Evidence Note is a component of this
- Covers:
  - Investigating
  - Deciding containment strategy
  - Recording actions
  - Coordinating communications.

HOCKING
COLLEGE

CSF 2.0 - Recover

- Restore assets and operations, and prevent attack recurrence
- Explain clearly what you’re doing and why during recovery (to leadership/users)

HOCKING
COLLEGE

Roles

- Speak in roles
- Write clean handoffs to next in line

- Declarer: confirms/declares incident; opens ticket; sets initial scope.
- Coordinator/Incident Manager: assigns owners, tracks actions, escalates.
- Comms: who informs stakeholders (and what you can/can’t share).
- Technical Owner(s): do the captures within authorization.
- Legal/Privacy Liaison: checks policy, retention, breach notice rules.
- Use these words in your note (owner/handoff/next step).

HOCKING
COLLEGE

Incident Preparation

- Before incidents occur put in place clear policy, roles, and plans so you're ready to act fast.
- When to declare an incident
  - Adverse activity meets your incident criteria
  - Don't wait for absolute certainty
- Evidence collection and handling procedure
  - Acquire → Preserve → Document → Avoid alteration → Store promptly.
  - Follow playbook for common events, tools to use,
- Who to notify and who not to notify in the event of a computer security incident.
  - Within the company, who needs to be notified, and what information does each person need to have?
  - Under what conditions should the company contact major customers and suppliers?
  - When should the authorities be contacted?

HOCKING
COLLEGE

Eradication and Incident Follow-Up

- Before eradication: ensure all necessary evidence is collected/logged and verify backups are clean.
- Eradication
  - Before the IT security group begins eradication efforts, it must collect and log all possible criminal evidence and then verify all backups are current, complete, and free of malware.
- Incident Follow-Up
  - An essential part of follow-up is to determine how the organization's security was compromised so that it does not happen again.
  - A formal incident report documents a detailed chronology of events, the root cause and the impact of the incident.
  - Policy updates and improvements

HOCKING
COLLEGE

Evidence Recording

- Incident log: A chronological diary of the incident: who did what, when, why, and with what authorization. Think “timeline of actions & decisions.” It’s about people + time + rationale. New owner adds a line to this after handoff.
- Evidence inventory: A catalog of artifacts you collected: each file/log/screenshot with ID, description, hash, storage location, and why it was collected. Think “index of objects and their integrity.”
- Chain of custody: A movement ledger for each evidence item: every hand-off/access (From → To, date/time UTC, purpose, signature/ID). Can be kept separately or in the inventory (a per-item custody log)
- Artifacts: The actual files
- Incident & Evidence Note: 1 page summary, points to items in inventory and references custody.
- Note: These are all append-only, retains all prior entries and they cannot be modified. If something is wrong, add a correction.

HOCKING
COLLEGE

Authorization & scope

- Do only what’s approved
- Stay inside the ticket/tasking/role
- No “curiosity clicks”
- No out-of-scope scans
- Must explicitly state in incident log – who authorized, to do what, on which assets, and when (time window).

HOCKING
COLLEGE

Evidence Collection

	Legal	Not Legan
Ethical		
Not Ethical		

Minimum Necessary Evidence Collection

- Collect only what's needed for the purpose of investigating/containing incident
- Avoid content collections or bulk grabs unless explicitly approved
- Request expansion only if necessary
- Less collected = fewer people exposed and faster review. Less is ethically more!
- Capture:
  - Single malicious email .eml (full headers+body) — shows source path & indicators (SPF etc..
  - Targeted Auth logs (±15–30 min) — correlates user/time without over-collection, context, enough to test hypothesis
  - Process list and network statistics — confirms live behavior near event
- Ignore:
  - Full mailbox exports — bulk content/PII; over-collection, privacy risk, not needed/slows analysis
  - Full-day logs — privacy risk; slows analysis.
  - Passwords/tokens in notes — creates new exposures, don't copy secrets
  - Campus-wide packet capture

HOCKING
COLLEGE

Chain of Custody

- Organizations should document all details of a security incident as it happens
- So evidence is trustworthy (accurate, could be used in criminal cases)
- A complete record of specific actions taken and all conversations in a logbook
- Who captured/handled what, when, storage location, and any changes for each item.
- Maintain chain of custody rows:

[ItemID] | [Description] | [From/To] | [UTC time] | [Location] | [Action/Purpose] | [Signature/ID].

- Tip: write custody rows as you capture; don’t add them later
- Use UTC for each row!

HOCKING
COLLEGE

Redaction & Evidence Storage

- Blur/box PII/creds/tokens
- Label all edits/redactions ("brightness adjusted, PII redacted").
- Do not share in chats/email
- Store in restricted evidence path
- Log access to case files
- Hashing is cryptographic identifier of a file. Not encryption!
- The same file will have the same hashing, a slightly different file has a different hash.
- Used to identify any changes to evidence
- Record SHA-256 for saved artifacts. In read/append only manifest.

HOCKING
COLLEGE

Screenshot Redaction

- Header: UTC, page/app title, URL/source, context
- Body: Relevant pane only; visible redaction boxes; note any edits.
- Footer template:

UTC Time • Source/URL • Captured by [name] • Case ID • Hashing SHA-256 • Redactions • Edits

HOCKING
COLLEGE

Containment Trade-offs

- Containment without chaos: choose responses that limit damage and preserve proof.
- Select containment based on asset criticality and impact
- Preserve evidence while limiting harm
- Avoid knee-jerk wiping which destroys context.

Choose the lightest control that manages risk (asset criticality + user impact + evidence value):

- Soft: revoke sessions/tokens/access; reset password; block compromised domains; disable account; additional user monitoring for 48hr
- Medium: network-isolate host (reduces spread; if authorized delay isolation to capture volatile data first)
- Hard: rebuild/wipe (only with approval; document thoroughly first)

- When to isolate: active malicious process, data exfiltration signs, or you can’t safely reset/revoke without the host cooperating. Grab one volatile snapshot first (authorized).
- When to reimage: only when analysis indicates persistence or high-risk malware *and* you’ve saved necessary artifacts; document pre-wipe evidence and all approvals.

HOCKING
COLLEGE

Weekly Reflection

Purpose:

- Practice ethical first-hour incident choices that respect privacy, policy, and evidence integrity.

Write (≈350–500 words):

- What I learned (6–8 sentences): Summarize the NIST incident lifecycle and why minimum necessary matters; tie to the eBook's harm-prevention theme.
- How I'll apply it (1 paragraph): A realistic campus or small-business scenario—list two items to capture and one to avoid with justification (scope/consent).
- Muddiest point (3–4 sentences): One precise question on chain of custody, redaction, or containment trade-offs.
- Portfolio note (2–3 bullets): What you'll publish and why it matters.
- AI use: Allowed with disclosure (add AI Use Note).

- Assessment:
  - Understanding (30) • Application (30) • Muddiest Point (20) • Portfolio Note (10) • Clarity & Mechanics (10)

HOCKING
COLLEGE

First-Hour Priorities

- Act within authorization. Write authorization line first.
- Capture minimal targeted evidence:
  - E.g. one malicious email .eml; 15–30 min auth window; one process/ports log
- Avoid trying to ”prove it” through ongoing monitoring/privilege escalation
- Record custody rows as you go not later, ensures accuracy, integrity, usability.
- Make a containment recommendation (soft/med/hard) + one-sentence why.

HOCKING
COLLEGE

Incident & Evidence Note

- Real world: One shared note per incident links to logs. For CYBR-2100: Write a complete note including all info.
- Timestamp & Context (UTC) — who told you what, when.
- Authorization — who approved which actions on which assets.
- Actions you took — One line for each step, any commands/tools used, stick to facts
- Evidence Inventory — exact file/log paths; hashes (if file); why it's minimum necessary.
- Chain of Custody — intake rows, storage location; handlers/times etc.
- Redaction — what you removed (PII/creds) and how.
- Next Step — recommended containment/recovery handoff (to which role?)

HOCKING
COLLEGE

Incident & Evidence Note - Template

- Incident #
- Timestamp (UTC) & Context: [YYYY-MM-DD HH:MM UTC] — Initial incident declaration: notified by [name/role] that [summary]. Ticket created with [IncidentID].
- Authorization: [Name/role] approved [actions] on [asset(s)] for [time window].
- Actions Taken: Ran [cmd/tool] on [host]; collected [log path]; isolated [asset] per approval
- Evidence Captured: Item [path or file] — SHA-256: [hash] — Why: [reason tied to hypothesis/window]
- Chain of Custody: Stored at [location]; access: [names/times]; transfer records kept.
- Redaction: Removed [PII/creds]; method [blur/box]; Note: unredacted copy should still be retained.
- Next Step: Recommend [containment/recovery] (handoff to [team]).

HOCKING
COLLEGE

What not to include

- No credentials, passwords, tokens, API keys in notes/screen grabs
- Avoid bulk content/payloads
- Rationale: minimum necessary keeps evidence defensible and respectful of privacy.
- No speculation/accusations; write observations only until verified
- No Proof of Concept/exploit steps unless authorized and via secure channel
- No creeping scope: don’t escalate privileges to “confirm” compromise unless expressly approved

How to spot a Phishing attack?

- Look-alike domains and mismatched Return-Path are classic signs.
- Look-alike IT notices: “password check,” “mailbox quota,” “MFA reset.”
- Payroll/financial lures: “update direct deposit,” “past-due tuition.”
- Timely action required: “be the first to…” creates urgency
- Doc-share baits: fake “shared syllabus” links.

HOCKING
COLLEGE

What happens if someone clicks?

What user thinks they're doing: registering or validating for a legit event.

What actually happens:

- They land on a page (remote or an attached HTML form) that looks official.
- They type their username/password.
- The credentials get posted to the attacker.
- The attacker tests those credentials immediately
- If MFA isn't enabled—or if the attacker tries push-fatigue—they may get in and set mailbox rules, pull data, or try VPN/ShareDrive.

HOCKING
COLLEGE

What triggers a phishing incident?

- Email auth flag
- User reports
- IdP detections (unfamiliar sign-in properties, impossible travel, sudden password-only attempts)
- Multiple recipients hit simultaneously by similar mail

HOCKING
COLLEGE

Email Authentication Protocols

- SPF (Sender Policy Framework) = “Is this IP allowed to send mail for that domain?”
  - Does the sending server’s IP match what the domain’s DNS says is allowed to send?
  - Result: spf=pass -> allowed
  - Spf=fail -> Not allowed, strict policy
  - Spf=softfail-> not allowed byt sender’s policy asks for leniency
- DKIM (DomainKeys Identified Mail) = “Did the sender’s domain cryptographically sign this?”
  - Sender’s server cryptographically signs parts of the message with a private key; receivers fetch the public key from DNS and verify
  - Result: dkim=pass means the signature checks out
  - Dkim=fail often signals tampering/spoof
- DMARC (Domain-based Message Authentication, Reporting & Conformance): “What policy should receivers follow if SPF/DKIM fail?”
  - Policy that requires alignment between the visible From: domain and SPF/DKIM.
  - If alignment fails and policy says p=reject, receivers may drop or quarantine; result: dmarc=pass/fail

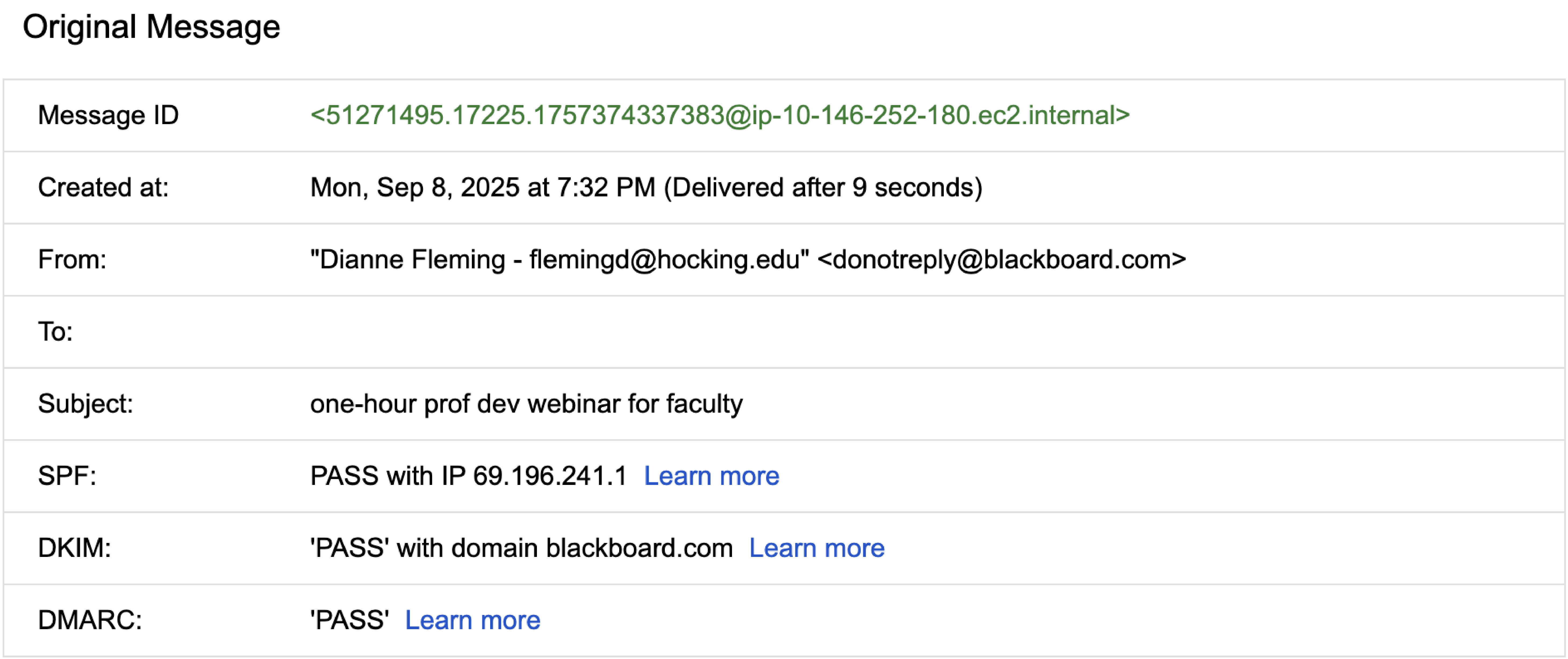
https://abnormal.ai/blog/what-is-an-email-header

Email Authentication Protocols

- Forwarding & mailing lists can break SPF and sometimes DKIM
- Some phishers also DKIM-sign compromised accounts, so a pass is not innocence.
- Alignment matters: DMARC wants From: domain to align with SPF or DKIM.
- Treat these results as clues, not verdicts. You still need other evidence to tell the story.
- If SPF fails but the email came through a known forwarder, be cautious; collect the email and correlate with other signals before recommending containment.
- You don’t need to decode these just quote the results from headers and explain what they imply (spoof vs. likely legit).
- Header hint: dmarc=fail with policy p=quarantine or p=reject strengthens the case it’s phish.

HOCKING
COLLEGE

Email Validation: SPF/DKIM/DMARC



Original Message

Message ID	<51271495.17225.1757374337383@ip-10-146-252-180.ec2.internal>
Created at:	Mon, Sep 8, 2025 at 7:32 PM (Delivered after 9 seconds)
From:	"Dianne Fleming - flemingd@hocking.edu" <donotreply@blackboard.com>
To:	
Subject:	one-hour prof dev webinar for faculty
SPF:	PASS with IP 69.196.241.1 Learn more
DKIM:	'PASS' with domain blackboard.com Learn more
DMARC:	'PASS' Learn more

HOCKING
COLLEGE

Email Validation: SPF/DKIM/DMARC

```
Return-Path: <donotreply@blackb0ard-mail.support>
Received: from mx2.hocking.example (10.12.34.21)
  by mailhub.hocking.example with ESMTP id 3F7A4C201
  for <alex.lee@hocking.example>; Mon, 08 Sep 2025 23:32:22 +0000 (UTC)
Received: from edge-smtp07.sender-net.example (198.51.100.27)
  by mx2.hocking.example with ESMTPS id 3F7A4C200; Mon, 08 Sep 2025 23:32:22 +0000
Received: from app01.blackb0ard-mail.support (203.0.113.78)
  by edge-smtp07.sender-net.example with ESMTP id 9C1D2E0
  for <alex.lee@hocking.example>; Mon, 08 Sep 2025 23:32:07 +0000
Authentication-Results: mx2.hocking.example;
  spf=pass smtp.mailfrom=donotreply@blackb0ard-mail.support;
  dkim=pass header.d=blackb0ard-mail.support;
  dmarc=fail (p=reject) header.from=blackboard.com
From: "Blackboard Learn" <donotreply@blackboard.com>
Reply-To: "Support" <support@blackb0ard-mail.support>
To: Alex Lee <alex.lee@hocking.example>
Subject: one-hour prof dev webinar for faculty – registration update
Date: Mon, 08 Sep 2025 23:32:05 +0000
Message-ID: <20250908.233205.9c1d2e0@app01.blackb0ard-mail.support>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8

<html>
<body>
  <p>Join us Wed 2:00–3:00 PM ET. Confirm your <b>teaching account</b> before joining.</p>
  <p><a href="https://learn-webinar.blackb0ard-mail.support/login">Registration</a></p>
</body>
</html>
```

HOCKING COLLEGE

Email Validation: Minimum Lines Example

From: "Blackboard Learn" <donotreply@blackboard.com> ← brand the user trusts

Reply-To: support@blackb0ard-mail.support ← different domain

Authentication-Results:

spf=pass smtp.mailfrom=donotreply@blackb0ard-mail.support

dkim=pass header.d=blackb0ard-mail.support

dmarc=fail (p=reject) header.from=blackboard.com ← alignment FAIL (spoof)

Body:

Join us Wed 2:00–3:00 PM ET. Confirm your teaching account before joining:

Registration: https://learn-webinar.blackb0ard-mail.support/login

HOCKING
COLLEGE

Email Validation Analysis

- Display-name spoofing: Set the display name to “Blackboard Learn” so the inbox shows a familiar name, even if the address or domain is different.
- DMARC misalignment spoof: Put From: donotreply@blackboard.com in the header but actually send from a different domain the attacker controls (e.g., blackb0ard-mail.support). If the brand’s DMARC policy is weak (p=none) or receivers are lenient, the message might still be delivered—even though alignment fails.
- Account compromise (harder but nastier): Attackers steal credentials from a real vendor or partner and send from the legitimate domain with valid DKIM/SPF. In that case, auth checks can pass because the sender really is permitted—your clue comes from the content and links, not auth failures.

HOCKING
COLLEGE

What other evidence do we have?

Web proxy:

- A traffic bouncer for web browsing.
- Logs outbound HTTP/HTTPS from devices: time, source IP, destination host, URL path, status, bytes.
- Can spot a GET request to a fake login page followed by a POST (i.e. credentials being sent).

Identity Provider (IdP):

- The service that proves identity for SSO
- Sign-in logs record each login attempt: timestamp (UTC), user, result (success/fail), auth factor (password vs MFA), client IP/location, device ID, app being accessed, client OS/browser, and risk flags (e.g., *impossible travel*)
- It’s minimal (no message content) and can be used to tell user and attacker apart.
- Password-only attempts right after the click = harvest signal.

HOCKING COLLEGE

IdP Logs

What to inspect:

- Timing
- Result + Factor: SUCCESS/FAIL and factor=Password/MFA
- Client IP: campus NAT / known ranges vs unfamiliar IP
- Device: known device ID / “compliant” vs blank/unknown
- Client app: what app the login targeted (VPN, ShareDrive, Email, etc.)
- Risk/Signals: *Unfamiliar sign-in properties*, *Impossible travel*, etc.
- Client OS/Browser: “Windows/Chrome” vs odd combos

IdP Logs Example

```
2025-09-08T23:20:12Z user=alex.lee result=SUCCESS factor=MFA(method=push)
  client_ip=198.51.60.10  location="Campus-NAT"
  device="WIN10-ALee-Laptop" device_state=Compliant client_os=Windows10 client_browser=Chrome
  app="Email" risk=Low

2025-09-08T23:33:27Z user=alex.lee result=FAIL factor=Password
  client_ip=198.51.100.54  location="Unfamiliar"
  device="-" client_os=Linux client_browser="Chrome/125"
  app="VPN" risk=High signals="[UnfamiliarSignInProperties]"

2025-09-08T23:33:58Z user=alex.lee result=FAIL factor=Password
  client_ip=198.51.100.54  location="Unfamiliar"
  device="-" client_os=Linux client_browser="Chrome/125"
  app="ShareDrive" risk=High signals="[UnfamiliarSignInProperties]"

2025-09-08T23:40:12Z user=alex.lee result=SUCCESS factor=MFA(method=push)
  client_ip=198.51.60.10  location="Campus-NAT"
  device="WIN10-ALee-Laptop" client_os=Windows10 client_browser=Chrome
  app="Email" risk=Low
```

HOCKING
COLLEGE

Phish Containment

- Recommend **soft containment**; escalate only if you see host persistence or lateral movement
- Preserve, then protect.
- Minimize blast radius with targeted actions
- Rationale matters. In your note, write the why for each containment step!

- Soft: reset password; revoke sessions/tokens; block look-alike domain/email; shorter session lifetimes .
- Medium: isolate the PC if network intercept shows active malware on that asset, only after snapshot of volatile data.
- Hard: rebuild only if needed and approved.

HOCKING
COLLEGE

Note Example

Incident #HC_IR_101

2025-09-08T23:35:00Z —Notified by student Alex Lee that a “Blackboard webinar” email looked suspicious and included a login link. Ticket created.

Authorization:

IR Manager (J. Smith) approved collection of one email (.eml) and Identity Provider (IdP) sign-in lines for alex.lee between 23:20Z–23:50Z. No other assets authorized.

Actions Taken:

- 23:38Z — Exported the reported message as raw .eml (headers + body intact).
- 23:40Z — Exported IdP sign-in events for alex.lee within approved window 23:20–23:50Z (single user, narrow window)
- 23:41Z — Calculated SHA-256 for both artifacts; recorded evidence inventory and chain-of-custody.
- 23:45Z — Completed analysis; prepared recommendation (soft containment).

HOCKING
COLLEGE

Note Example (cont.)

Evidence Captured:

Item ID: EV-001

Description: Phishing email (.eml; headers+body)

SHA-256: ????????

Collected: 23:38Z

Collector: Name Here

Location: /incident/HC_101/Artifacts/EV-001_Original_Email.eml

Why: Shows DMARC alignment failure (brand in From is blackboard.com; authentication passes for attacker's look-alike domain), plus a look-alike login link. This establishes spoof and a possible credential-harvest lure.

Note Example (cont.)

Item ID: EV-002

- Description: IdP sign-in log (23:20–23:50Z)
- SHA-256: ??????
- Collected: 23:40Z
- Collector: Name here
- Location: ???
- Why: Shows password-only fails from unfamiliar IP/device right after phish email; MFA successes bookend.

Note Example (cont.)

Chain of Custody:

Time (UTC)	ItemID	From	To	Location/Path (logical)	Purpose/Action	Sign/ID
23:38Z	EV-001A	Collector	Evidence	\evidence\HCL-101\02_Artifacts\EV-001A…	Intake; added; hashed	JD
23:40Z	EV-002A	Collector	Evidence	\evidence\HCL-101\02_Artifacts\EV-002A…	Intake; added; hashed	JD
23:45Z	EV-001A	Evidence	IR Manager	(same)	Review only for decision	KM

Note Example (cont.)

Redaction:

List any redactions made to evidence and why.

e.g. Redact non target user information on IdP evidence log. Filter csv to do this.

Next Step:

Recommend soft containment due to [likely attack vector/impact]

Actions include: resetting user alex.lee password, revoke tokens/sessions, and block *.blackb0ard-mail.support in email/web filters.

Monitor for 48h for additional attempts on the account.

Handoff to IdP Manager for decision

HOCKING
COLLEGE

In-Class Activity With Prompt

Task (≈1 page, bullet-friendly)

- Write an Incident & Evidence Note from a short prompt (log + email excerpt) provided in class. Keep it factual and concise.
- Phishing Exercise Prompt: TBD
- Assessment
  - Preparation & Participation (20) • Apply Ethics & Law (40) • Collaboration & Professionalism (20) • Deliverable Quality (20)

HOCKING COLLEGE

Portfolio Artifact

- Sections:
  - My First-Hour Priorities (3–5 bullets): What you capture vs. avoid (with why).
  - Incident & Evidence Note (final): Paste your refined note.
  - Integrity & Privacy Controls (short paragraph): Hashing, storage location, redaction policy.
  - Evidence Links: Upload or link the in-class note and reflection PDF.
  - Reflection (3–4 sentences): Trade-offs you'd revisit next time.
  - AI Use Note (if used).
- Do not include: PII, credentials, or exploit steps.
- Assessment:
  - Ethical & Legal Accuracy (40) • Evidence & Artifacts (20) • Reflection & Growth (20) • Presentation & Mechanics (20)

HOCKING
COLLEGE

Remember

- First-hour discipline: act within authorization, capture the minimum necessary, and write notes others can trust.
- Privacy by default: narrow scopes and redact PII to reduce harm and review burden.
- Defensible evidence: integrity, storage, and chain of custody make artifacts usable later.
- Containment without chaos: choose responses that limit damage and preserve proof.

HOCKING COLLEGE