Security, Identity and Cybersecurity Services

Microsoft Defender for Identity (MDI)

Importance of Response Planning

Liju Varghese
Sr. CSA-Engineering

Microsoft

Conditions and Terms of Use

Microsoft Confidential

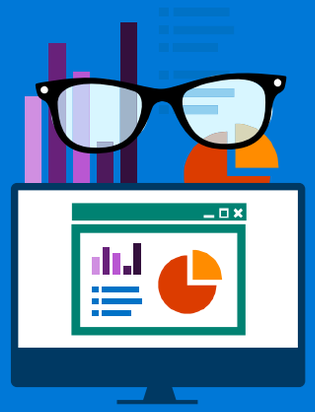
This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

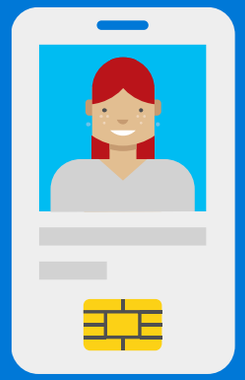
Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

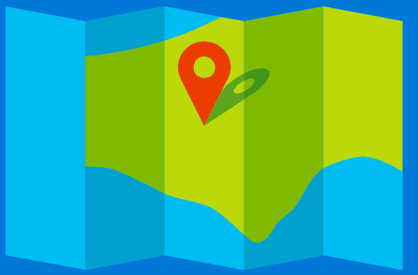
How do I respond to credential theft?



Deploying a threat detection solution requires a solid understanding of the threats that the solution detects and being prepared to respond to them



Credential theft attacks are unique because the adversary is using legitimate identities within the environment



Knowledge of the risk and impact along with a planned and established response plan is crucial when attacks are identified

What is an incident response plan?

"The primary objective of an Incident Response (IR) plan is to manage a cybersecurity event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs."

-McKinsey&Company "How good is your cyber incident-response plan?" December 2013

Why is a response plan needed?

- If you assume compromise, you assume Defender for Identity (MDI) will find something.
- If you do not have a response plan, what do you feel could, would, or will happen?
- A well-established response plan will prepare you to address findings in a positive manner.
- Response plans guide you through:
- Identifying the severity of the incident
- Quickly understanding the risk to the organization
- Identification of the correct people to investigate, resolve and report on the issue
- An agreed upon way to navigate organizational structures
- A structured process for communicating to internal and external audiences

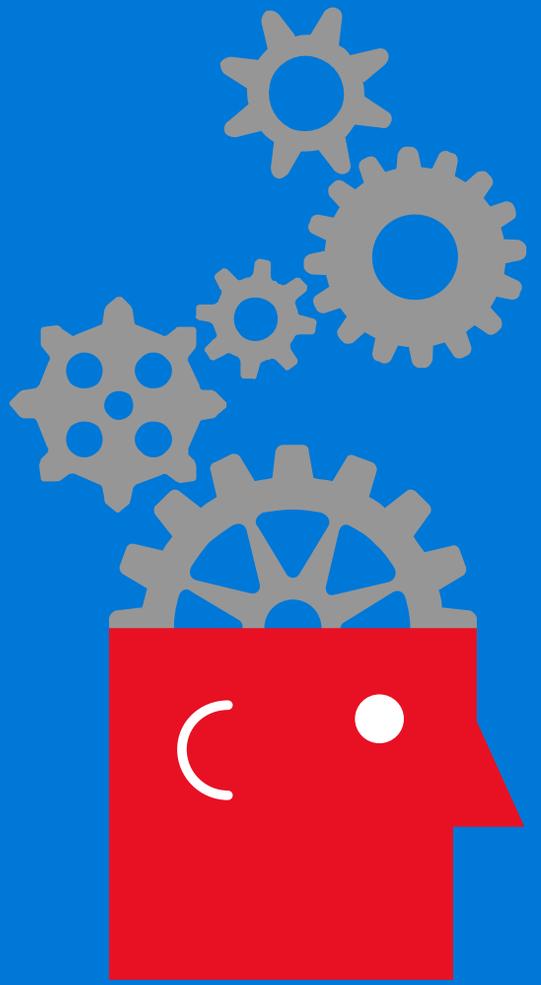
Why most incident response plans fail?

- Documentation may be out of date, too generic and not useful for guiding specific activities during a crisis
- Plans are not coordinated with across business units
- Decision making is often based on institutional knowledge of the organization and relies on one or two “go to” people

Fortunately, these scenarios can all be successfully addressed with a well-prepared and thought-through incident response plan

Improved decision making

When decision rights have been delegated and carefully planned, an organization can quickly respond to a breach at the appropriate scale or escalation level based on the value at stake



Internal coordination

Incident response is an issue that involves many departments, and not just IT

Effective planning and coordination must incorporate all business functions across the organization (e.g. Corporate Communications, Legal, Compliance and Audit, Business Operations, etc.)

Coordination ensures greater agility during an incident.

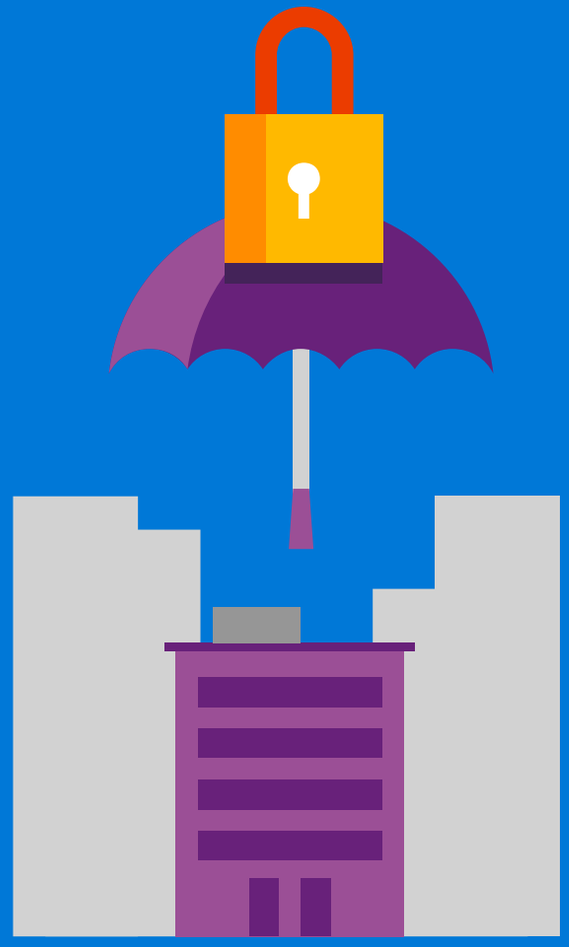
External coordination

Effective incident response plans should include coordination with important third-parties who can assist with investigation and remediation (e.g. law enforcement, incident response services, forensic experts, etc.)

Unity of effort

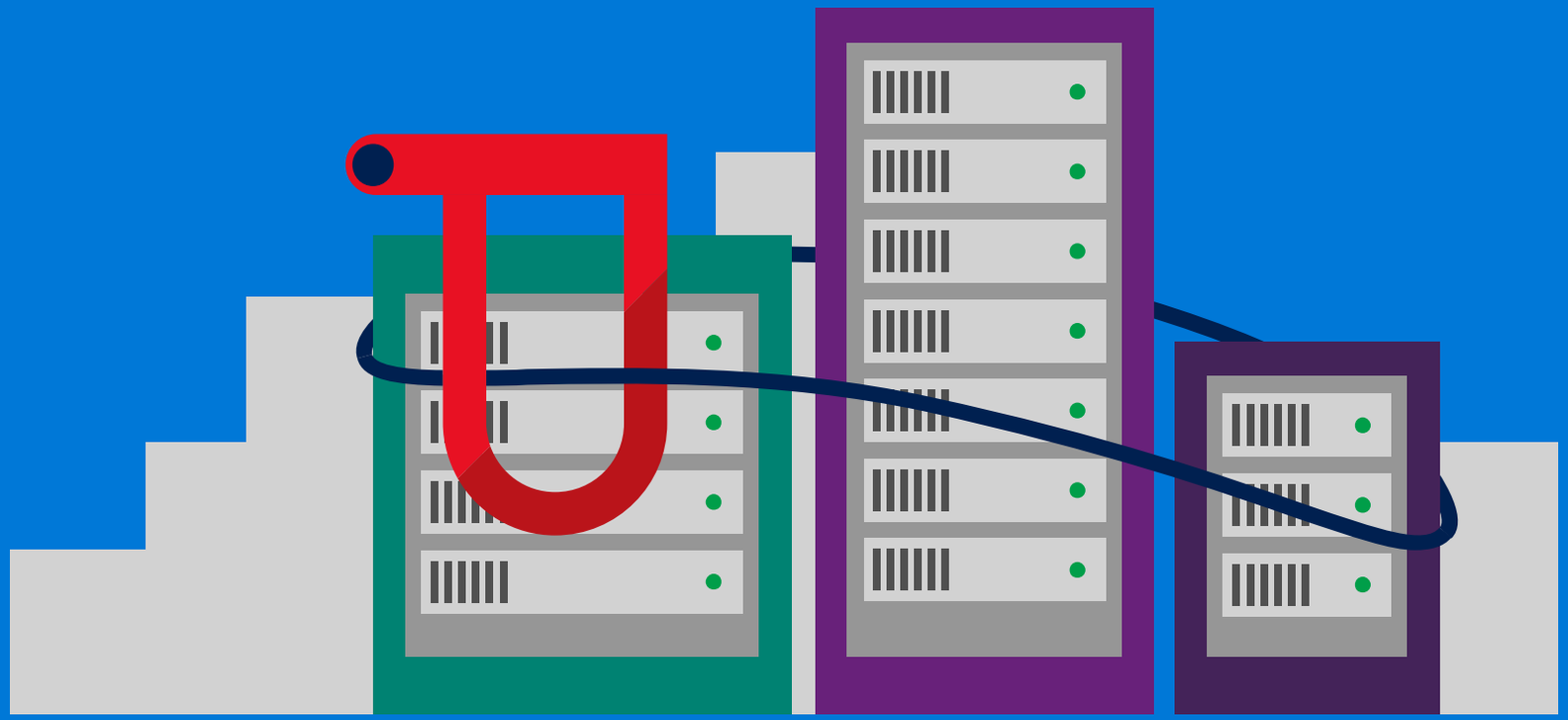
Efficient incident response plans should establish clear roles and responsibilities across the organization

Unclear responsibilities can lead to delays in decision making and risk greater damage to the organization



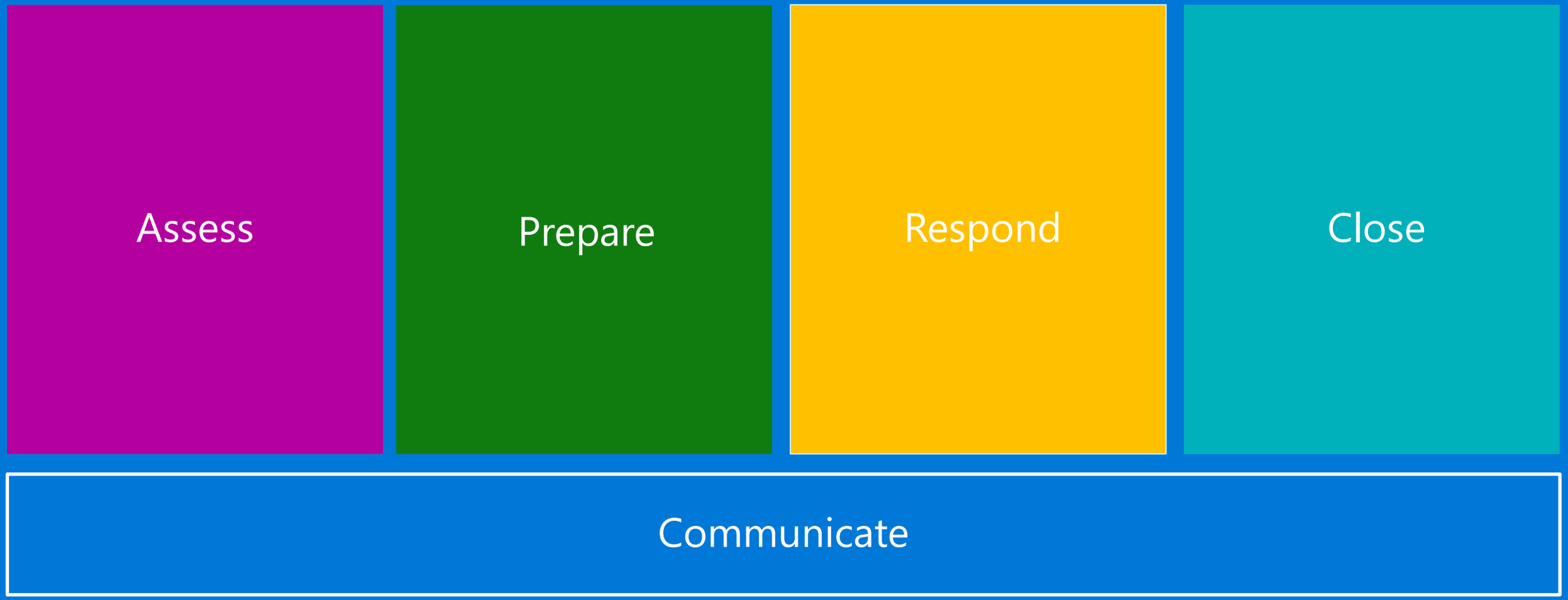
Damage limitation

Well-built incident response plans help ensure that minor events do not escalate into major incidents

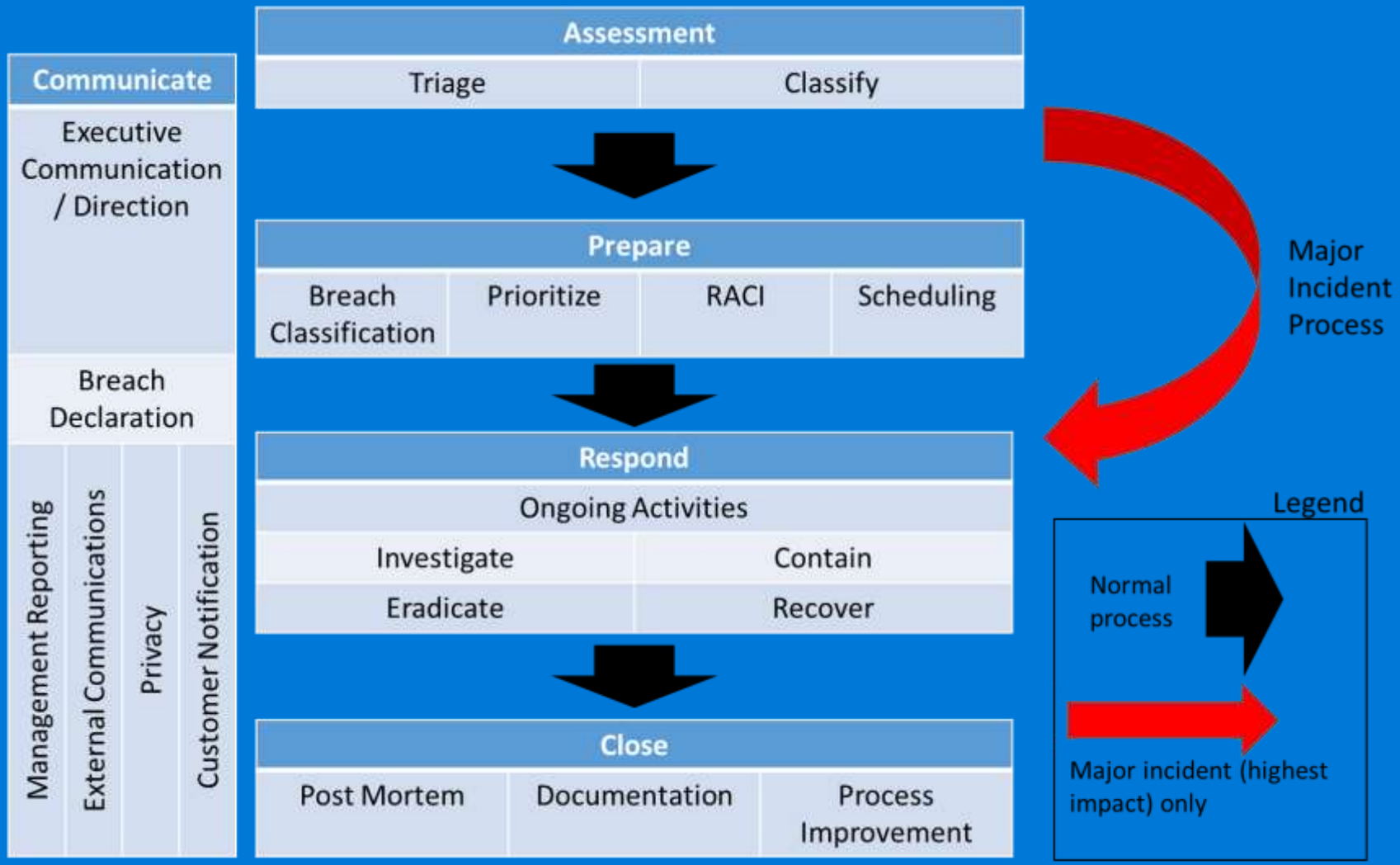


Components of a response plan

Components of a response plan



Security incident response process



RACI: Responsible, Accountable, Consulted, Informed

Assess

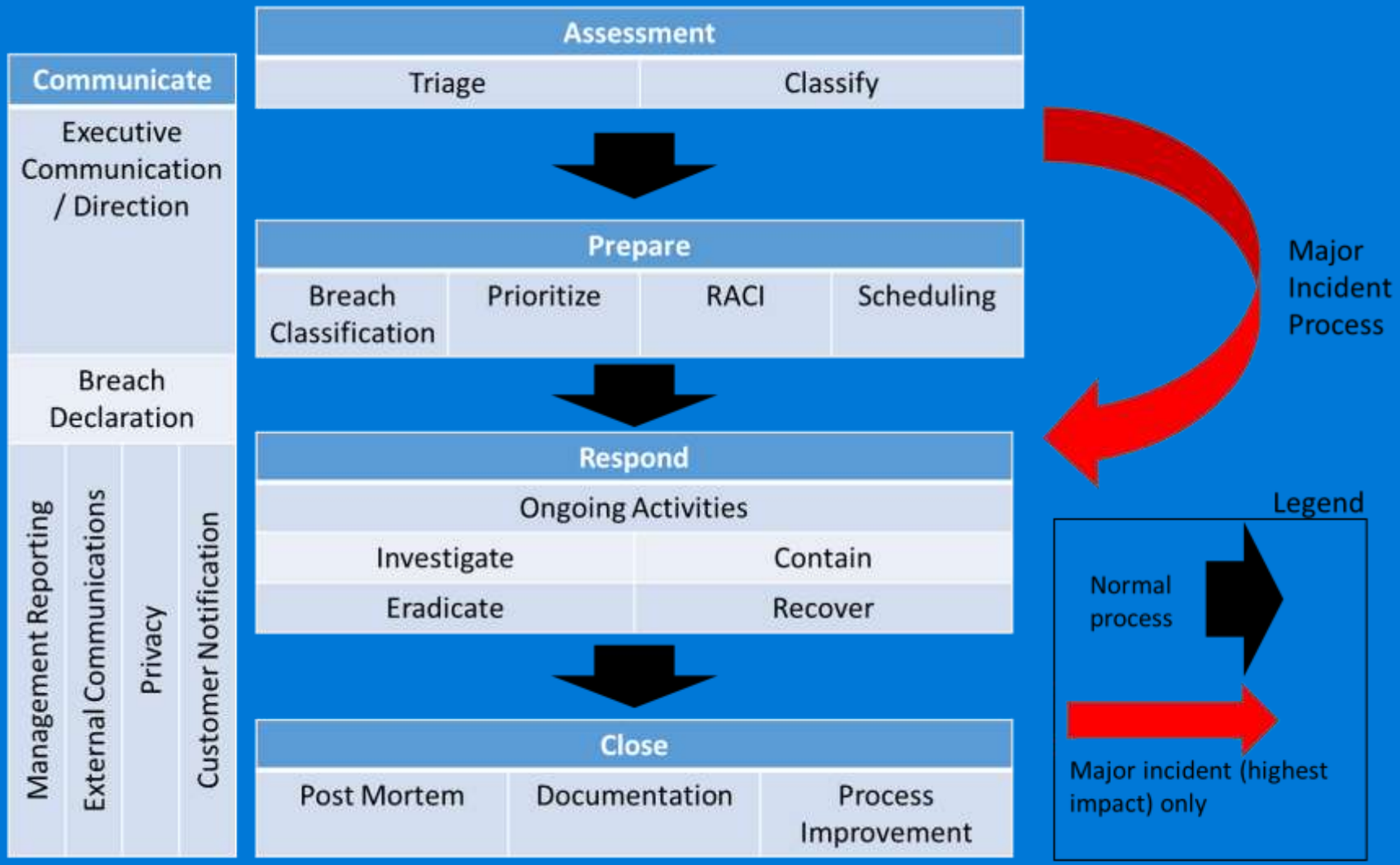
Triage

- The act of “triaging” an event is to determine if the event is an actual security incident and if so, its criticality.
- In summary:
- Every escalation may not be a critical security incident
- Each event should be reviewed to determine its organizational risk (criticality)

Classify

- The classification of an incident focuses on defined classifications that indicate the overall impact to the business.
- Everything that fits the *security incident* definition MUST go through the classification process.
- While Microsoft supply default classifications, customer ultimately determines their own classifications.

Major incident management process



Major (critical) incident management

- In case of a major incident, actions to communicate and contain will take precedence over activities such as scheduling, RACI, and even eradication
- This does not mean that scheduling, the RACI or eradication are not important
- Major incident management provides a quick response process if the situation dictates

Prepare

Prioritization

- Before an appropriate response to a security breach can be defined, the team must have a comprehensive understanding of the response priorities.
- For example:
- If an adversary is able to compromise an asset that will impact customer licensing, the top priority may be system integrity.
- If the compromised system is used to store customer personally identifiable information, the highest priority may be to identify the extent of any unauthorized access across the data sources, depending on the context.
- If the compromised system is used to deliver authentications services, restoration of reliable service may be the top priority.

Prioritization example

Success Element	Priority (1 being High, 6 being Low)
Minimize customer impact	1
Address legal or regulatory risk	4
Media coverage	5
Restoring operations quickly	3
Execute remedial actions	2
Identify actors involved in the breach	6

Communicate

Executive communications and reporting

- Notification to executive leadership is often appropriate and necessary.
- Executive(s) can aid in determining the total impact (both financial and otherwise) of a security incident to the business or the entire organization.
- Leadership provides guidance on the response (for example, who notifies customer(s), public relations actions, early legal involvement, etc.).
- Provides legitimate-power coverage for expedited authority chains (for example, quick decision-making for major incidents).

Security incident declaration

- The security incident declaration involves communicating out both internally and externally the nature, impact and response to the security incident.
- The declaration will often be governed by notification laws or compliance requirements.
- It is critical to be aware of the requirements and exceptions to these laws before declaring a breach. For example, laws may permit delayed notification for certain circumstances such as when a law enforcement agency determines that notification would impede a criminal investigation.

External communications

- The security team and executive leadership shall be responsible for providing guidance regarding all communication with third parties and what information is being disseminated internally among organizations.
- Given the sensitivities surrounding these types of events, no entity should engage internal or external third parties without the approval of leadership and security incident response teams.

Respond

Investigate

- The triage of a security escalation should yield the following:
- Preliminary scope of the incident
- Impact across various services
- Severity of the incident at minimum

Investigation steps

1. Acquire, organize and preserve evidence in a manner that is reasonably forensically sound (from an investigative versus a law enforcement perspective), given circumstances of the incident.
2. Iteratively reassess and revise the scope, impact and severity of the incident as more facts are uncovered.
3. Periodically check regulatory requirements regarding compliance and privacy.
4. Identify possible root cause for the incident.
5. Assess containment, eradication and remediation options with the operations team to reduce the impact of the incident.
    a. Security incident response team will conduct the investigation in conjunction with the IT incident management process to take advantage of existing communication channels, resources and operating rhythm of each team.
    b. Each of the five stages of the Investigate phase are iterative in nature and can be optional depending on multiple factors.

Containment

- The containment phase is centered on protecting systems from further risk associated with the incident through system isolation.
- Containment and remediation:
  - In case of a security incident, the team in consultation with the IT Operations teams and SMEs will develop an appropriate remediation and containment plan to reduce the impact of the incident in a timely fashion.

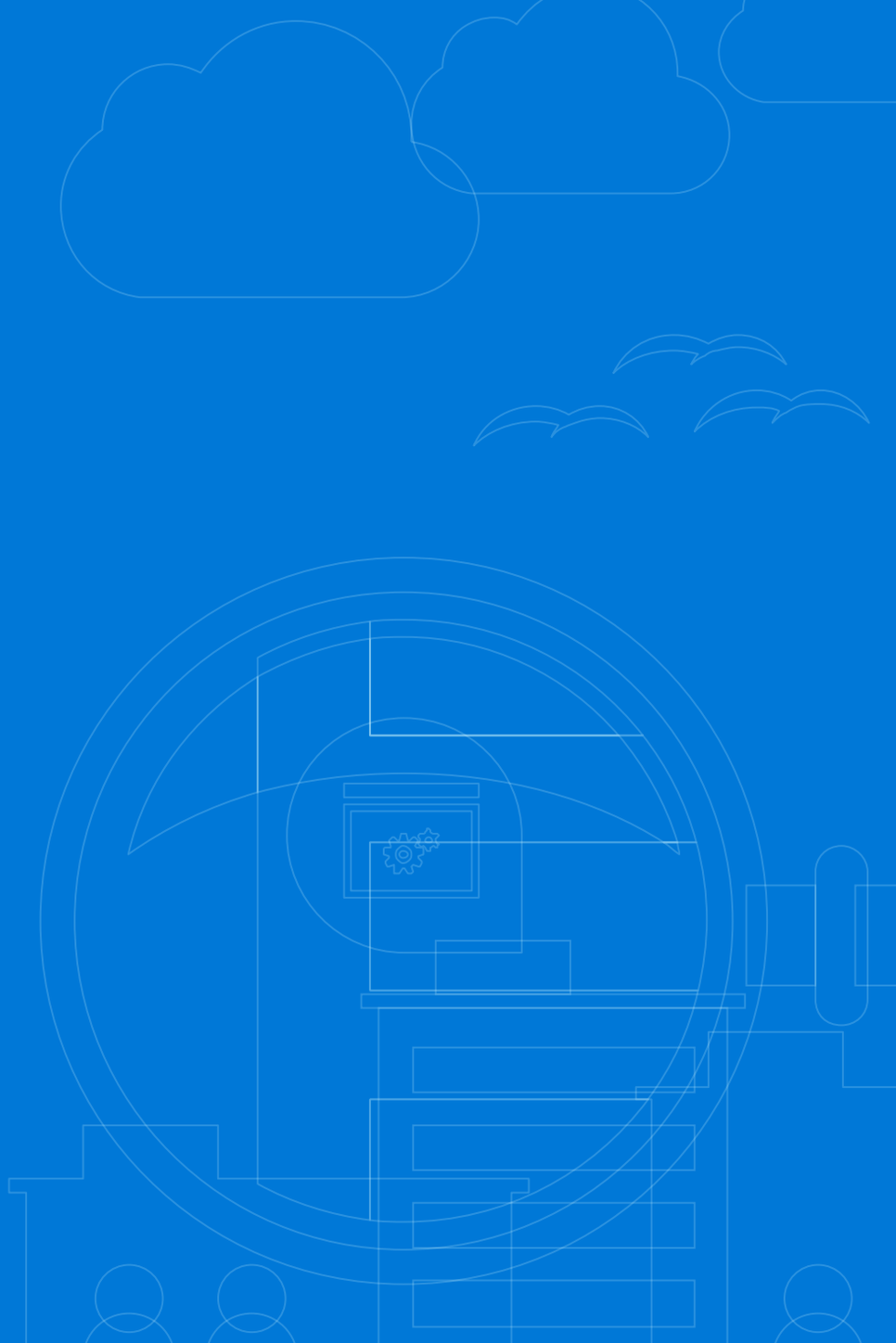
Eradication

- Eradication is the process an organization completes to regain control of resources that have been compromised by a security incident.
- The process of *eradicating* may be different for each security incident. Some may have defined processes, while others may be determined as an organization is confronted with a new issue.

Recovery

- Recovery is the process of returning resources and/or systems to a safe running state with technical operations reporting as normal.
- This does not mean that services to stakeholders have been fully recovered.
- Steps need to be taken to ensure that services are at full, normal capacity and available for stakeholders. These steps may include:
- Communications to stakeholders indicating they may proceed with normal system(s) use, or in some cases, engage systems per refined security protocols
- Verification steps to ensure services have been fully restored for stakeholders
- Escalation and de-confliction process have been established in the case when recovered services cannot be accessed as expected or needed

Close



Post mortem

- A post mortem session brings the entire Security Incident Response Team together to review how the incident response process worked during a response to a security incident.
- During the post mortem the following items are reviewed:
- The problem
- Who actively participated
- Detailed timeline
- Root cause
- How things were handled
- The eventual solution
- Further prevention techniques
- Gaps in the process
- Lessons learned
- What needs to be updated in the Security Incident Response Plan

Documentation

- The documentation phase covers more than just updating documentation. It also includes:
- Ensuring all tickets related to the incident have been properly closed
- Ensuring all details captured during each phase of the incident response were properly captured and included in a post incident review with appropriate properties
- Tracking and validating any and all updates to the Security Incident Response Plan document

Process improvement

- The closure of an incident always offers an opportunity for process improvement.
- Customers should use this opportunity to update any gaps that were identified during the incident response and, if necessary, new processes are defined for the future.

Questions & Answers


Microsoft