Playbook: Identity and Access Compromise

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

TODO: Expand investigation steps, including key questions and strategies, for identity and access compromise.

1. TODO

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain

TODO: Customize containment steps, tactical and strategic, for identity and access compromise.

TODO: Specify tools and procedures for each step, below.

- TODO

TODO: Consider automating containment measures using orchestration tools.

Eradicate

TODO: Customize eradication steps, tactical and strategic, for identity and access compromise.

TODO: Specify tools and procedures for each step, below.

- TODO

Reference: Remediation Resources

TODO: Specify financial, personnel, and logistical resources to accomplish remediation.

Communicate

TODO: Customize communication steps for identity and access compromise

TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan.

In addition to the general steps and guidance in the incident response plan:

1. TODO

Recover

TODO: Customize recovery steps for identity and access compromise.

TODO: Specify tools and procedures for each step, below.

In addition to the general steps and guidance in the incident response plan:

1. TODO

Resources

Additional Information

1. "Title", Author Last Name (Date)