Security Lens Items

1. Who has access to view this data?
2. Are there authorization checks for the restore feature?
3. Are there validation checks for which computers can be restored?
4. Are these checks enforced server-side?
5. Is the untrusted data being HTML-encoded?How is each action logged?
6. What are the security related events that could be logged?
7. Who can see the fact this was detected?
8. Is the end-user notified at all?
9. How can we assure the correct device is affected?
10. Can other devices know about this event?
11. Do any existing roles or permissions change?
12. Can I call the API directly?
13. Can I assure we do validation on the UI and the server-side?
14. What happens if I give the API inconsistent, malformed or bad input? Too small/too large
15. How does the UI respond if I can manipulate the server to respond with errors?
16. Do error messages disclose too much information?
17. Can users call the API if the UI is hidden?
18. What happens if an endpoint is offline at various states?
19. What happens if the endpoint is a different version?