Clint Meeting: Vision Realignment

Tuesday, April 15, 2025 8:56 PM

General notes about our product (Internal Use Only):

RMF Process:
1) Prepare – organization to manage security and privacy risks
2) Categorize – the system and information based on impact analysis
3) Select – the NIST SP 800-53 controls to protect the system
4) Implement – controls and document how they are deployed
5) Assess – controls to see if they are in place
6) Authorize – risk based decision to authorize the system
7) Monitor – control implementation and risks to the system

From the NIST SP 800-53 we are focusing on the areas that mention controls for Operating Systems
Picking out all the specific areas out of the document that has a large number of pages

RMF Step 4: Implementing Security Controls
- Operating System updates are essential for the Risk Management Framework (RMF) process, especially under System Maintenance and Configuration Management in:

RMF Step 3: Select Controls to Protect System
- NIST SP 800-53
  - SI-2 Flaw Remediation
  - CM-2 Baseline Configuration
  - CM-6 Configuration Settings

RMF Step 5: Assess Security Controls
- Based on the patch status within the report

RMF Step 7: Monitoring Security Controls
- Addressing new OS vulnerabilities as quickly as possible

Key things that we want to get from this meeting:
- Client's thoughts on the report that we sent
- What changes client would like to see
  - Would a good approach be to add the SL-2, CM-2, CM-6, etc.
- What output will the client be satisfied with? For us to say "Here is what we have" and for the client to say "this is an acceptable product"
- Let them know about the Cyber Range handover, as well as the presentation
  - Do they want / need to be there for that stuff?
  - How will we successfully transition this project over when the quarter comes to an end?

Documents to have on hand for the meeting:

NIST.SP.800-53r5

OS_Patch_Compliance...

--
Meeting notes

Robert -
Question 1

Generic statements (we detected this version was behind, here is a reason why you want to update, multiple hosts per each page
- You've got what looks like a working project, the next step will be, starting to iron it down to a more specific output goal
- Ease of use factors

From Roberts perspective, we have a working project, successful coalition of data into a working project
Done the basic steps

Focusing on to present: focusing the vulnerability language to be more specific to a vulnerability. More specific about what our findings are. More specific to benefit the AI side.

Provide client outline of the presentation

On one slide of the presentation, what are the next steps.

CVE's being discontinued
- What is the fall back?

Send clients the presentation outline for what we are going to do (what we *think* we are going to do) for our final presentation