CHECKLIST

VULNERABILITIES

- [ ] How frequently are vulnerabilities unpatched when disclosed?
- [ ] Which vulnerabilities should you prioritize for remediation?
- [ ] How will you reduce the risk of similar vulnerabilities getting into your code base in the future?
- [ ] What are the specific kinds of vulnerabilities that scanning can identify and help to remediate?
- [ ] Are you reliably addressing your key vulnerabilities?
- [ ] How frequently are vulnerabilities fixed by disclosure time?
- [ ] How long do vulnerabilities live in code bases?
- [ ] Which vulnerabilities are most exploited?
- [ ] Are higher severity vulnerabilities patched quicker?
- [ ] How often do you see open source vulnerabilities in your ecosystem?
- [ ] How long does it take to fix vulnerabilities?
- [ ] Are systems and applications periodically scanned for common and new vulnerabilities?
- [ ] Are vulnerabilities reduced to an acceptable level for release?
- [ ] Has the severity of discovered vulnerabilities changed over time?
- [ ] Which percentage of overall vulnerabilities are high risk?
- [ ] Which vulnerabilities must one remediate in order to have a clean scan under PCI DSS standards?
- [ ] Are you better equipped to prioritize your vulnerabilities for remediation?
- [ ] Does your ics vendor respond to vulnerabilities that are provided to it?
- [ ] Do you expect the chosen provider to perform remediation for discovered vulnerabilities?
- [ ] What happens when vulnerabilities are discovered?
- [ ] Why have so few vulnerabilities been reported that were introduced in later versions?
- [ ] Is the median lifetime of vulnerabilities decreasing in newer versions?

CHECKLIST

- [ ] What types of vulnerabilities are associated with web resources?
- [ ] How do you manage vulnerabilities?
- [ ] Which vulnerabilities represent the greatest threats?
- [ ] What percentage of remediated vulnerabilities are actually high risk?
- [ ] How do you inform affected parties about vulnerabilities on large scale?
- [ ] What percentage of exploited or high risk vulnerabilities were actually remediated?
- [ ] Who is responsible for remediating vulnerabilities?
- [ ] What percentage of exploited or high risk vulnerabilities are remediated?
- [ ] Which percentage of overall vulnerabilities are high risks?
- [ ] Do you see a reduction in vulnerabilities introduced into your digital environment?
- [ ] What vulnerabilities were identified that you were unable to patch or mitigate?
- [ ] Are vulnerabilities being exploited in the wild?
- [ ] How to test for buffer overflow vulnerabilities?
- [ ] NOTES: