PONDURANCE

Follow the NIST Cybersecurity Framework by Asking the Right Questions



Step 1: Identify

Making sure you can see every nook and cranny of your organization.



- ☐ What assets do you have (data, devices, cloud and on-premises infrastructure, software and networks, etc.)?
- ☐ What risks and vulnerabilities do the assets carry?
- ☐ What are their priority levels?
- ☐ What are your specific plans to protect them?
- ☐ Have you conducted a comprehensive vulnerability assessment?

Step 2: Protect

Taking a risk-based approach to protecting your organization is an ongoing effort.



- ☐ How often do you review identity and access management controls?
- ☐ Are your endpoints equipped with up-to-date antivirus software?
- ☐ Are you creating regular secure backups?
- ☐ Is your asset inventory updated monthly?
- ☐ Are systems and software updated and patched based on vulnerability scan results and as directed by vendors?

Step 3: Detect

Detecting incidents as soon as possible is crucial for a fast recovery.



- ☐ Do you have full visibility into data, devices, logs, cloud-based and on-premises system infrastructure, software and networks?
- ☐ Are you monitoring for potential threats and incidents across all environments 24/7?
- ☐ Do you have staff to maintain and monitor logs that record events like changes to systems or accounts?
- ☐ Do you have security tools in place to help like a SIEM to aggregate logs and look for deviations from normal behavior?
- ☐ Do you test and fine-tune your detection mechanisms regularly?

Step 4: Respond

Responding with a plan in place is crucial so you can eradicate the breach quickly.



- ☐ Have you contained the threat by isolating or shutting down the affected systems, networks, servers, databases, and devices to prevent further spread to your network?
- ☐ Are you preserving evidence while it's available including logs, memory dumps, audits, network traffic reports, and disk images?
- ☐ Did you patch the entry point to ensure the attacker cannot regain access?
- ☐ Have you determined if any sensitive information has been breached or any data loss has occurred?
- ☐ Have you engaged with your legal team to examine any compliance or regulatory risks to determine potential violations?

Step 5: Recovery

Recovering begins almost immediately after the incident happens and could overlap with your response.



- ☐ Have you collected all necessary forensic evidence?
- ☐ Are systems fully restored to normal operations?
- ☐ Did you restore system images, restore data from backups, or replace compromised controls like passwords?
- ☐ Have you conducted a post-incident analysis and reporting with evidence from the incident?
- ☐ Have you captured lessons learned to reduce the risk of a future incident?

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204

Copyright © 2021 Pondurance

PONDURANCE

Follow the NIST Cybersecurity Framework by Asking the Right Questions



Step 1: Identify

Making sure you can see every nook and cranny of your organization.



- ☐ What assets do you have (data, devices, cloud and on-premises infrastructure, software and networks, etc.)?
- ☐ What risks and vulnerabilities do the assets carry?
- ☐ What are their priority levels?
- ☐ What are your specific plans to protect them?
- ☐ Have you conducted a comprehensive vulnerability assessment?

Step 2: Protect

Taking a risk-based approach to protecting your organization is an ongoing effort.



- ☐ How often do you review identity and access management controls?
- ☐ Are your endpoints equipped with up-to-date antivirus software?
- ☐ Are you creating regular secure backups?
- ☐ Is your asset inventory updated monthly?
- ☐ Are systems and software updated and patched based on vulnerability scan results and as directed by vendors?

Step 3: Detect

Detecting incidents as soon as possible is crucial for a fast recovery.



- ☐ Do you have full visibility into data, devices, logs, cloud-based and on-premises system infrastructure, software and networks?
- ☐ Are you monitoring for potential threats and incidents across all environments 24/7?
- ☐ Do you have staff to maintain and monitor logs that record events like changes to systems or accounts?
- ☐ Do you have security tools in place to help like a SIEM to aggregate logs and look for deviations from normal behavior?
- ☐ Do you test and fine-tune your detection mechanisms regularly?

Step 4: Respond

Responding with a plan in place is crucial so you can eradicate the breach quickly.



- ☐ Have you contained the threat by isolating or shutting down the affected systems, networks, servers, databases, and devices to prevent further spread to your network?
- ☐ Are you preserving evidence while it's available including logs, memory dumps, audits, network traffic reports, and disk images?
- ☐ Did you patch the entry point to ensure the attacker cannot regain access?
- ☐ Have you determined if any sensitive information has been breached or any data loss has occurred?
- ☐ Have you engaged with your legal team to examine any compliance or regulatory risks to determine potential violations?

Step 5: Recovery

Recovering begins almost immediately after the incident happens and could overlap with your response.



- ☐ Have you collected all necessary forensic evidence?
- ☐ Are systems fully restored to normal operations?
- ☐ Did you restore system images, restore data from backups, or replace compromised controls like passwords?
- ☐ Have you conducted a post-incident analysis and reporting with evidence from the incident?
- ☐ Have you captured lessons learned to reduce the risk of a future incident?

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204

Get the full cybersecurity roadmap for your organization with our latest eBook.

Get the Practical Cybersecurity eBook

Copyright © 2021 Pondurance