Incident Response Steps and Frameworks for SANS and NIST

cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide

What is Incident Response?

Incident response is a plan for responding to a cybersecurity incident methodically. If an incident is nefarious, steps are taken to quickly contain, minimize, and learn from the damage.

Not every cybersecurity event is serious enough to warrant investigation. Events, like a single login failure from an employee on premises, are good to be aware of when occurring as isolated incidents, but don't require man hours to investigate. Your cybersecurity team should have a list of event types with designated boundaries on when each type needs to be investigated. From there, you should have customized incident response steps for each type of incident.

The Importance of Incident Response Steps

A data breach should be viewed as a "when" not "if" occurrence, so be prepared for it. Under the pressure of a critical level incident is no time to be figuring out your game plan. Your future self will thank you for the time and effort you invest on the front end.

Incident response can be stressful, and IS stressful when a critical asset is involved and you realize there's an actual threat. Incident response steps help in these stressing, high pressure situations to more quickly guide you to successful containment and recovery. Response time is critical to minimizing damages. With every second counting, having a plan to follow already in place is the key to success.

The Two Industry Standard Incident Response Frameworks

Introduced in no particular order, NIST and SANS are the dominant institutes whose incident response steps have become industry standard.

NIST

NIST stands for National Institute of Standards and Technology. They're a government agency proudly proclaiming themselves as "one of the nation's oldest physical science laboratories". They work in all-things-technology, including cybersecurity, where they've become one of the two industry standard go-tos for incident response with their incident response steps.

The NIST Incident Response Process contains four steps:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

SANS

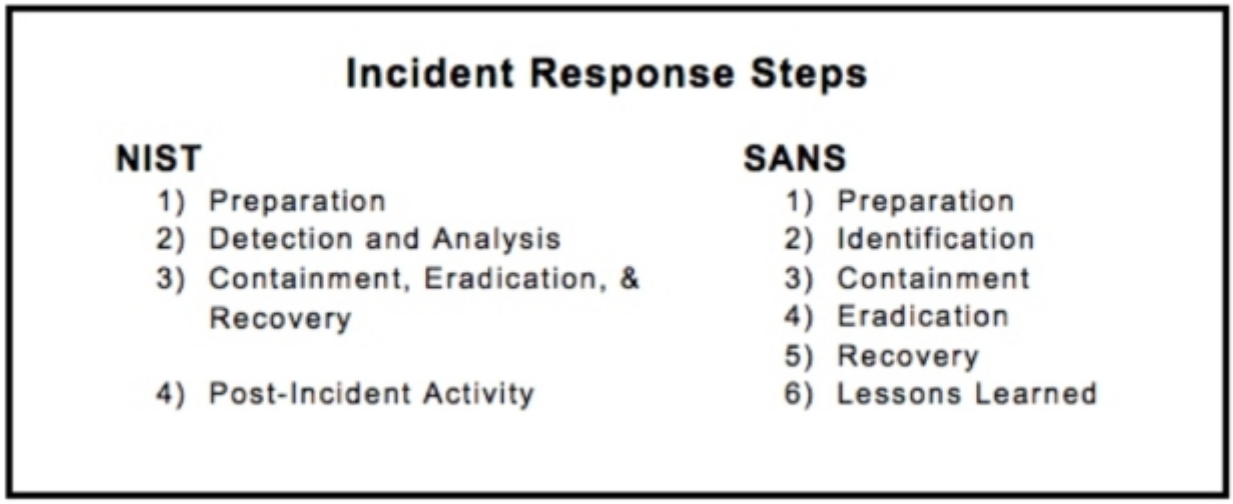
SANS stands for SysAdmin, Audit, Network, and Security. They're a private organization that, per their self description, is "a cooperative research and education organization". Though more youthful than NIST, their sole focus is security, and they've become an industry standard framework for incident response.

The SANS Incident Response Process consists of six steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

The Difference Between NIST and SANS Incident Response Steps

With two industry standard frameworks, there's a chance you're familiar with one but not the other. So let's do a walk-through of their similarities and differences. First, here's a side-by-side view of the two processes before we dive into what each step entails.



Placed side-by-side in a list format, you can see NIST and SANS have all the same components and the same flow but different verbiage and clustering. Let's walk through what each of the steps entail to get into the nuanced differences of the frameworks.

For consistency, NIST steps will always be presented on the left and SANS on the right during the steps side-by-side comparisons.

Step 1) Preparation = Step 1) Preparation

Preparation is key to rapid response. We beat this drum earlier when discussing the importance of having incident response steps.

This step is similar for both NIST and SANS. In this step you compile a list of all your assets, including but not limited to: servers, networks, applications, and critical endpoints (like C-level laptops). After you've compiled your asset list, rank them by level of importance. Then monitor their traffic patterns so you can create baselines to be used for comparisons later.

Create a communication plan, with guidance on who to contact, how, and when based on each incident type. Don't forget to get buy-in from everyone on this contact list to prevent hiccups or finger pointing later.

Determine which security events, and at what thresholds, these events should be investigated.

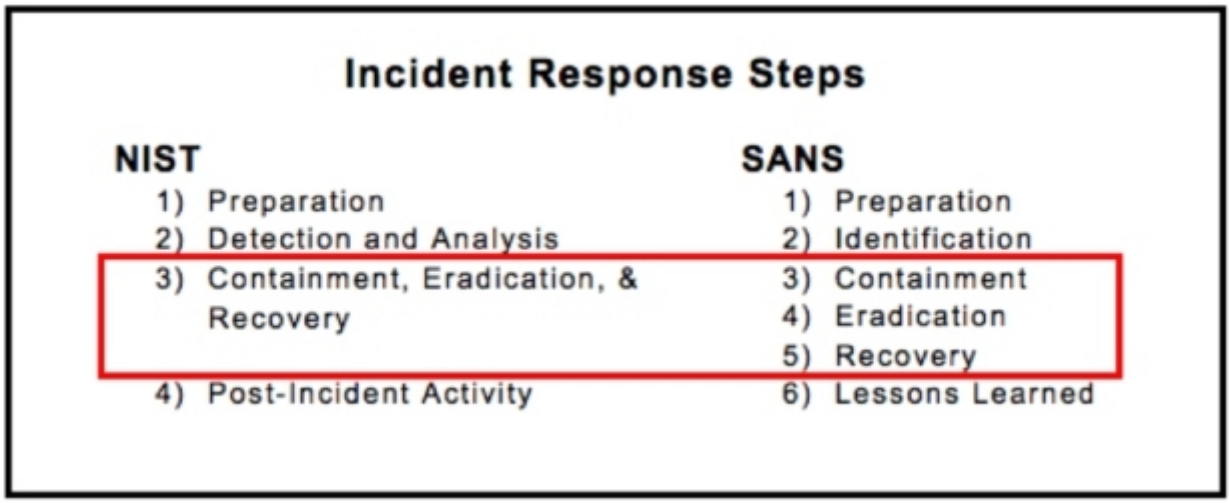
Then create an incident response plan for each type of incident. It can be improved through security event simulations, where you identify holes in your process, but it will also be improved after actual events (more on that later). The point is, get a process in place.

Step 2) Detection and Analysis = Step 2) Identification

Again, this step is similar for both NIST and SANS, but with different verbiage.

At this point in the process, a security incident has been identified. This is where you go into research mode. Gather everything you can on the the incident. Then analyze it. Determine the entry point and the breadth of the breach. This process is made substantially easier and faster if you've got all your security tools filtering into a single location.

Step 3) Containment, Eradication, & Recovery = Steps 3-5) Containment. Eradication. Recovery.



Here is where NIST and SANS kind-of part ways in their similarities before agreeing again on the final step. NIST views the process of containment, eradication, and recovery as a singular step with multiple components. SANS views them as their own independent steps.

Containment aims to stop the bleeding. Here is where you patch the threat's entry point.

Eradication aims to remove the threat. If the threat gained entry from one system and proliferated into other systems, you'll have more work on your hands here.

Recovery aims to get the system operational if it went down or simply back to business as usual if it didn't.

Step 4) Post-Incident Activity = Step 6) Lessons Learned

NIST and SANS are in agreement again in their last step, if not in verbiage, in spirit.

This step provides the opportunity to learn from your experience so you can better respond to future security events. Tempting as it may be to skip, with your never ending to-do list, this step is strongly recommended.

Take a look at the incident with a humble but critical eye to identify areas for improvement. Then go add those improvements to your documentation.

No process is perfect for absolutely every possible scenario. Some scenarios can't even be fathomed until they've occurred. The threat landscape is also ever-evolving so your incident response process will naturally need the occasional update. Remember, your future self will thank you.

The Incident Response Steps Poll

In an informal Twitter poll on a personal account, one of us got curious and asked people where their incident response guidance comes from. Check out the result:

While not a statistically significant poll, 69% of respondents use NIST or SANS. Not surprising since they're industry standards, but it scratched our curiosity itch.

Which Incident Response Steps Framework is Better?

Ah, to be definitely told an answer. No such chance here. It really does come down to personal preference. Does it make more sense to you to break containment, eradication, and recovery into their own steps or keep them grouped in a single step? Let your answer to that question guide you to the right choice.

Both are popular and have supporters. Regardless of which you choose, both NIST and SANS have incident handling checklists available to get you started. Just remember to customize them to your specific needs and company's environment...and before you're in the midst of an incident response.