Incident Response Planning

As cyber attacks have become more sophisticated, organizations have responded by adopting more preventative technologies. Unfortunately, between attacker ingenuity and unwitting employees, organizations are realizing that protection efforts can't prevent all attacks.

To stay in business, organizations need to be able to respond quickly to incidents, contain them, and minimize (or prevent) loss. And that requires somehow making sense of a huge amount of data from a variety of sources. In spite of all the technology involved, this can be a time-consuming, manual task.

The missing element: Network situational awareness

What's been missing is a full understanding of what's in your network and how it all connects—network situational awareness. Without it, you struggle the same way a firefighter would struggle knowing only that a fire is happening— over there. No firefighter could go in without an area map, and individual building blueprints are an added plus. Like the firefighter, you need to know exactly where the problem is, how to get there, the nearby valuable assets (Is it near a gas station or a hospital? How about near your customer data?), and where it might move next.

The network situational awareness RedSeal gives you makes incident response faster and easier throughout the process: preparation and detection; analysis; containment and remediation; and post-incident activity.

Preparation and detection

Many organizations begin their incident response process with Security Information and Event Managers (SIEMs). SIEMs take in information from all the sources that are monitoring your network and its environment and look for anomalies.

These sources may include:

- Threat feeds
- End point information
- Event logs from different systems
- Data loss prevention information
- Network map information

In addition to SIEMs, organizations employ:

- User and behavior analytics
- Network traffic analysis
- Threat intelligence feeds
- Machine learning

But all this information results in many more “incidents” than you can respond to. And most of these incidents are not particularly relevant.

RedSeal sifts through reported incidents to identify the most critical. It augments the information you bring into your SIEM with an understanding of your full network (including virtual and cloud-based sections) and all the access paths in it. With the up-to-date model of your network RedSeal computes and maintains you’ll get a valuable and precise output about the location of each potentially compromised host.

Analysis

The analysis phase is when the members of your team personally evaluate each reported incident to identify the most serious and relevant. They look for answers to questions like: “Is this reported incident real?” “Do we have to do something about it?” “Do we have to do something NOW?” This has been a manual process. It requires human judgement based on investigation, expertise, and familiarity with your network and its normal operations.

RedSeal automates much of this process. By calculating every access path in your network, RedSeal shows you not just where the indicator of compromise is, but what an intruder can reach from there.
As your team examines reported incidents to evaluate the need for response, the top questions are usually the same.

You begin with the IP address where the incident is supposed to be occurring and ask:

- Where is this IP address?
- What applications are running on it?
- How important is it?
- Where can intruders go from there?
- Can they reach key data (the “crown jewels”)?

These are frequently challenging questions that require you to pour over potentially outdated network maps and track down machines. RedSeal automates this discovery process.

With just one query, RedSeal tells you:

- Where the IP address is located in your RedSeal model
- Where the IP address is physically located by switch and port
- The applications that are running on it
- What your access policy is with regard to it

Then, RedSeal identifies all “targets” reachable from that IP address – and provides detailed information on each one, including:

- Name
- Operating system
- Applications running
- Policy group
- Topology group

Containment and remediation

Once you've determined that you're dealing with a real incident that requires a timely response, it's time to act. After you locate the affected device, you take action to contain the incident and minimize damage and/or data loss.

You could take a variety of approaches, including:

- Unplugging affected equipment
- Creating a "honey pot" of fake, attractive-looking information and following its trail
- Increasing your monitoring to see what happens
- Changing rules in your firewalls to block access to key assets

Eventually, you need to contain the problem, neutralizing any malware or unauthorized access. RedSeal makes it easier for you contain incidents that could be harmful to your network. RedSeal provides the exact, detailed path intruders could take to reach each target. It shows you which paths are open and which are closed. When you're ready to contain the intrusion, RedSeal identifies which firewall you'll need to change, what its configuration file looks like and which line of that file you need to change.

Post-incident activity

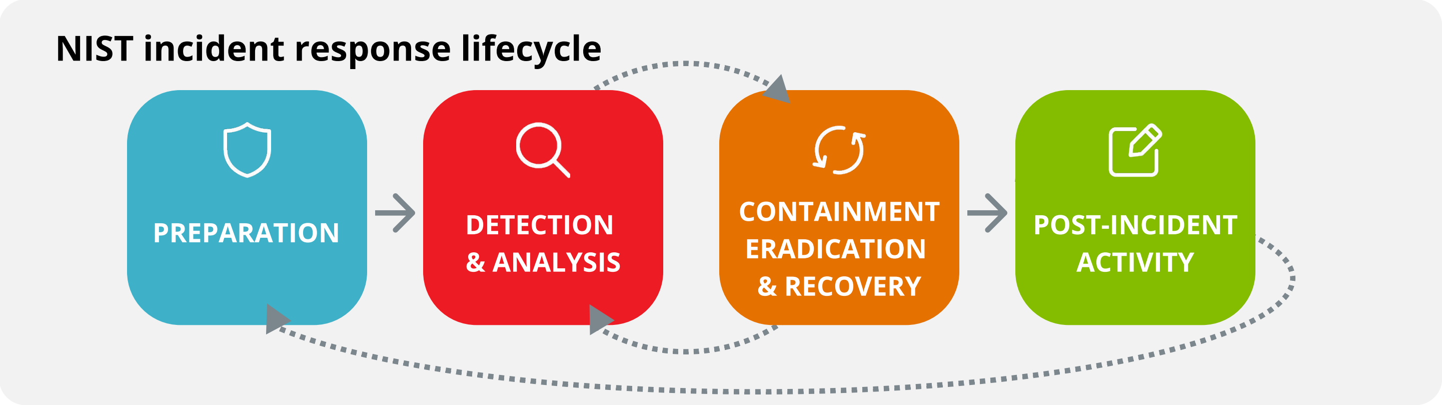
As the urgency decreases and your network is no longer in danger, you have time to research, reflect, discuss and identify needed changes. You can determine how the incident happened, how you can prevent something like it in the future, and, not least, what you will say to all the interested parties.

RedSeal hardens your network against future attacks by modeling all possible attack paths. You'll be able to find and block them before they're exploited. As you reflect and plan for the future, you may want to update your policies and enforce some segmentation. You can model policies in RedSeal and evaluate your segmentation—as it was implemented, not just how it was planned.

With RedSeal, you'll have the network situational awareness you need to automate many of the steps involved in responding to incidents. Your team will be able to focus on areas where their network and organizational knowledge can have the biggest positive impact.

The end result: Faster and more effective incident response.

NIST incident response lifecycle



RedSeal, a leader in network exposure management, offers proactive insights to close security gaps in hybrid environments. It creates a network digital twin for comprehensive visibility and protection. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency, boosts productivity, and reduces business risk.
www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169