# REDSEAL AND INCIDENT RESPONSE

As attacks have evolved in sophistication in recent years, the information security industry has responded by developing more and more preventative technologies. Unfortunately, between attacker ingenuity and unwitting employees, organizations are realizing that while their protection efforts are necessary, they still can't prevent all attacks. To stay in business, organizations need to be able to respond quickly to incidents and minimize (or prevent) loss. And that requires making sense of a huge amount of data from a variety of sources.

## PREPARATION AND DETECTION

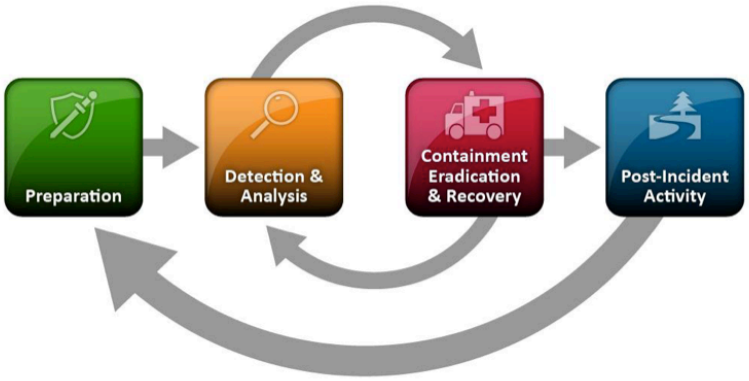
To address the issue, many organizations begin with Security Information and Event Managers (SIEMs), a solution designed to help with all this data. SIEMs take in information from all the sources that are monitoring your network and its environment and look for anomalies. These sources may include:

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

In order to sift through this data and determine if your network is experiencing an incident, a SIEM depends on rules you create. Called *correlation rules*, these are in the form of, "IF this happens, AND we see this, AND we see that – we have an incident."

But even with your correlation rules, SIEMs report many more "incidents" than you can respond to. And many of these incidents are not particularly relevant. These are *false positives*.

So, although your SIEM has reduced your data to a more manageable amount, the volume is still too high for your team to look into all reported incidents. You need to do some analysis to identify the most serious and relevant of these.




**NIST Incident Response Lifecycle**

# REDSEAL AND INCIDENT RESPONSE

## ANALYSIS

The analysis phase is when the members of your team personally evaluate each reported incident and 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?” Unfortunately, this analysis can’t be fully automated. It requires human judgement based on investigation, expertise and familiarity with your network and its normal operations.

## CONTAINMENT and ERADICATION

Once you’ve determined that you’re dealing with a real incident that requires a timely response, it is time to act. First, you must locate the affected device, then 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 eradicate the problem from your network, removing any malware or unauthorized access.

## POST-INCIDENT ACTIVITY

As the urgency decreases and your network is no longer in danger, you have time to research, reflect and discuss. You’ll need to figure out 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.

## THE MISSING ELEMENT: NETWORK CONTEXT

As you work to identify, analyze and contain network incidents, what you’ve lacked is a full understanding of what’s in your network and how it all connects – network context. 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 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.

RedSeal provides all this information to make the job of incident response faster and easier.

### Preparation and Detection

At the earliest stages of this process, RedSeal adds an understanding of your full network (including virtual and cloud-based networks) to your SIEM. The network context RedSeal brings allows you to create more effective correlation rules, refine them, and reduce false positives. RedSeal’s knowledge of your network helps you create rules like: IF high value asset AND attack depth is 0, THEN you have an incident.

# REDSEAL AND INCIDENT RESPONSE

## Analysis

As your team examines reported incidents to evaluate the need for response, the top questions are usually the same. You begin with an IP address where the incident is supposed to be occurring and ask:

- Where is this IP address?
- What's 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 requiring pouring over potentially outdated network maps and tracking down machines. RedSeal automates this discovery process. With just one query, RedSeal can tell you:

- Where the IP address is
- What's on it
- What your policy is with regard to it
- Its sub group

Then, RedSeal can identify all "targets" reachable from that IP address – and provide detailed information on each one, including:

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

## Containment and Eradication

Once you've identified that you have a real incident that could be harmful to your network, RedSeal makes it easier for you contain it. RedSeal can provide the exact, detailed path intruders could take to reach each target. It can show you which paths are open and which are closed.

Once you decide 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 you reflect and plan for the future, you may want to update your policies. You can model those policies in RedSeal, so a future correlation rule could simply be: IF policy violation, THEN incident.

With RedSeal, you'll have the network context 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.