A Network Operator’s Guide to Detection and Response

Bob Rotsted

NSRC Volunteer

About Me

- I’m an NSRC volunteer based in San Francisco, CA
- I’ve been building and using intrusion detection systems since 2007
- I’ve been to Fiji once and am keen to go again

NSRC
Network Startup Resource Center

Suva, Fiji 2018

Summary

- You’ve limited resources, prioritize threats that are important to your organization.

- Detection requires alert tuning, validation and institutional context to be effective.

- Detection is not enough. Consider how you will contain threats and prevent them from occurring again.

You’ve received some security alerts, what now?

Scenario: Ransomware detected by firewall

- Your organization recently upgraded the firewall and the new firewall produces security alerts.

- Your team receives many alerts daily suggesting that there are virus infected machines on your network.

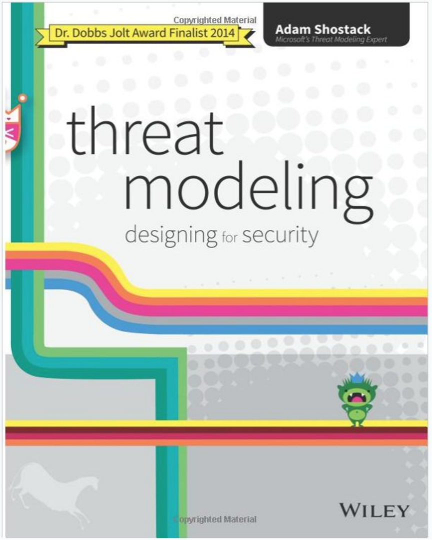
- **You’re concerned that ransomware could infect computers on the network and cause harm to your organization.**

Step 1: Is this alert important?

- Are you responsible for the infrastructure that triggered the alert?
- Will responding improve your security posture?
- Do you have a plan for responding?
- **If your answer is, “No” you may not need to do anything!**

Capability: Organizational Threat Model

- What are you trying to protect?
- Why do you need to protect it?
- Who are you protecting it from?
- How might it be attacked?



Threat Modeling: Designing for Security
Provides practical advice about how to threat model.

Capability: IPAM and Asset Management

- **Document your IP Addressing Scheme** - When investigating an alert, knowing the role of an IP address (eg. guest network, building control network, etc.) will accelerate your ability to determine if a threat is important or not.

- **Asset Management System -** Documenting the IP/Hostname and owner of important infrastructure on your network will make it easy to know who to contact for remediation of a security breach.

Step 2: Validate the threat

- Have you seen this alert before? Was it a true positive?
- Do you understand how it was generated and why?
- How will you find out more information?

Capability: Incident tracking system

- **Document your incidents -** Keeping a log of the validation and remediation steps taken during the investigation of an alert or incident can inform future response action and provide evidence in the event of legal action.

- **Control access to documentation** - Security incidents commonly involve sensitive information like people’s names and details about vulnerabilities in your organization’s infrastructure. Ensure that this information is kept private to prevent inadvertent disclosure.

Capability: Audit logs

- **IP to Identity -** Radius accounting, VPN authentication, DHCP lease, NAT translations, etc.

- **Authentication -** SSH, RDP, LDAP, SAML

- **Network Metadata** - Flow logs (Netflow, Zeek, Argus), Firewall ACL logs, DNS query logs, etc.

Capability: Centralized Log Collection

- **Use reliable transport** - There are many scenarios where logs can get lost in transit. Using a logging agent (eg. FluentD, Logstash, etc.) will minimize the chance that logs are lost in transit.

- **Establish a Retention Policy** - Collecting your logs in a centralized place make it easier to enforce a data retention policy across all your important datasets. This will ensure you’ve got logs when you need them most.

- **Using a search engine** - You can store your logs in a search engine (eg. Elastic, Humio, Stackdriver) to make them easy to access. Search engines commonly charge per gigabyte indexed; this option can be expensive if pursued commercially.

Step 3: Take action or not?

- **If the threat is real** - you'll want to contain it and document it. Consider how you might prevent a threat from spreading or gaining access to sensitive information.

- **If you're unsure if the threat is real** - you may still want to contain it until you can determine otherwise. Consider how this may affect your user. How disruptive will it be to your environment?

- **If it's not a threat** - you'll want to document it, modify the detection logic to tune out this specific instance of the alert and move on.

Capability: Centralized Alerting

- **An easy way to tune alerts** - False positives are common in commodity detections that come from commercial products. You will want a way to filter false-positive events before they page your team in the middle of the night.

- **Escalation management** - Your team may only handle part of a remediation process. You will want a way to hand off to other teams when you need their help.

- **Notification** - If you have alerts that are critical you want to ensure that your team is notified of them promptly. You will want a way to escalate an alert and trigger a phone call, push notification or SMS to ensure that the team receives the alert.

Capability: Network Access Control (NAC)

- **Network Isolation** - One of the best ways to contain a threat is to isolate it from the network. Network access control (NAC) can provide a centralized way to enforce network isolation when you find a threat on your network.

Capability: Incident Response Plan

- Who will respond when an alert fires?
- What hours will responders keep? Will there be an on-call rotation?
- How will a responder validate an alert?
- Who needs to be notified if a breach occurs?

Summary

- You’ve limited resources, prioritize threats that are important to your organization.
- Detection requires alert tuning, validation and institutional context to be effective.
- Detection is not enough. Consider how you will contain threats and prevent them from occurring again.

Questions?