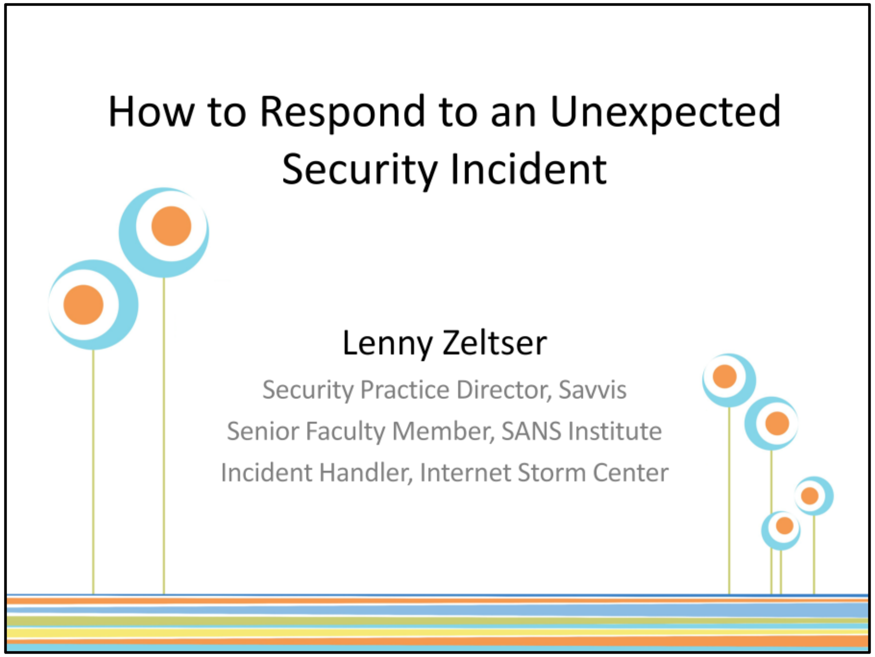


How to Respond to an Unexpected Security Incident

Lenny Zeltser

Security Practice Director, Savvis

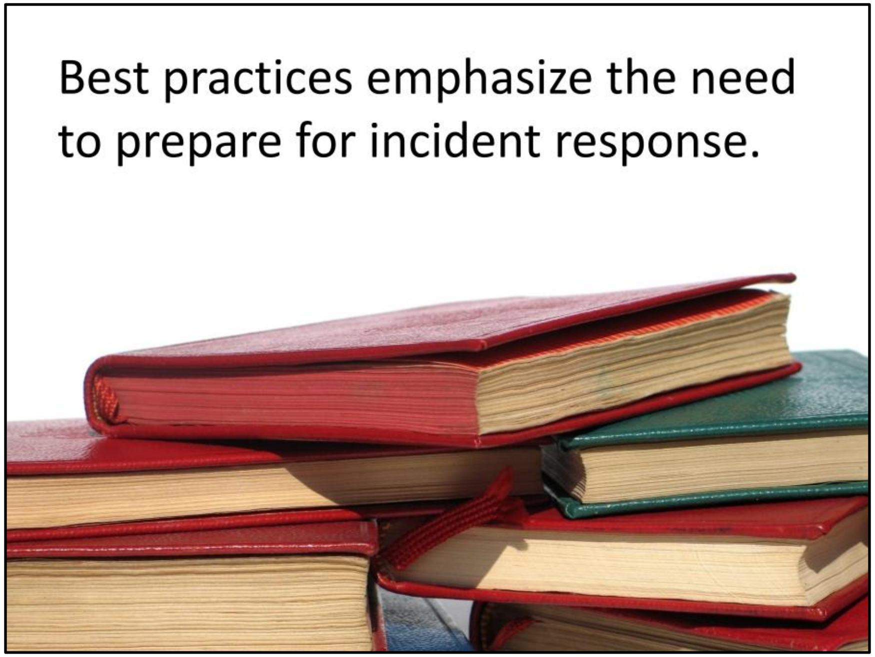
Senior Faculty Member, SANS Institute

Incident Handler, Internet Storm Center

What if a security incident catches you unprepared? In such situations, stress leads to mistakes and poor decisions made in the spur of the moment. In this talk, Lenny Zeltser discusses the questions an incident responder should ask to gain control of the situation quickly and assertively.

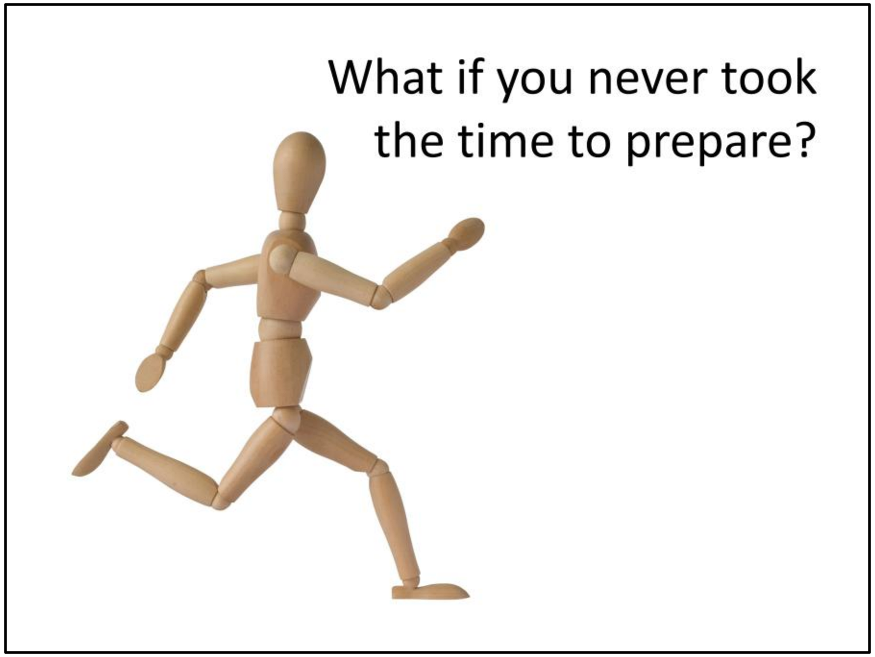
Lenny Zeltser leads the security consulting practice at Savvis, helping customers manage information security and address IT risks. He is also a Board of Directors member at SANS Technology Institute, a SANS faculty member, and an incident handler at the Internet Storm Center. Lenny frequently speaks on information security and related business topics at conferences and private events, writes articles, and has co-authored several books.

Lenny is one of the few individuals in the world who've earned the highly-regarded GIAC Security Expert (GSE) designation. He also holds the CISSP certification. Lenny has an MBA degree from MIT Sloan and a Computer Science degree from the University of Pennsylvania. For more information about his personal projects, see http://zeltser.com and http://twitter.com/lennyzeltser.



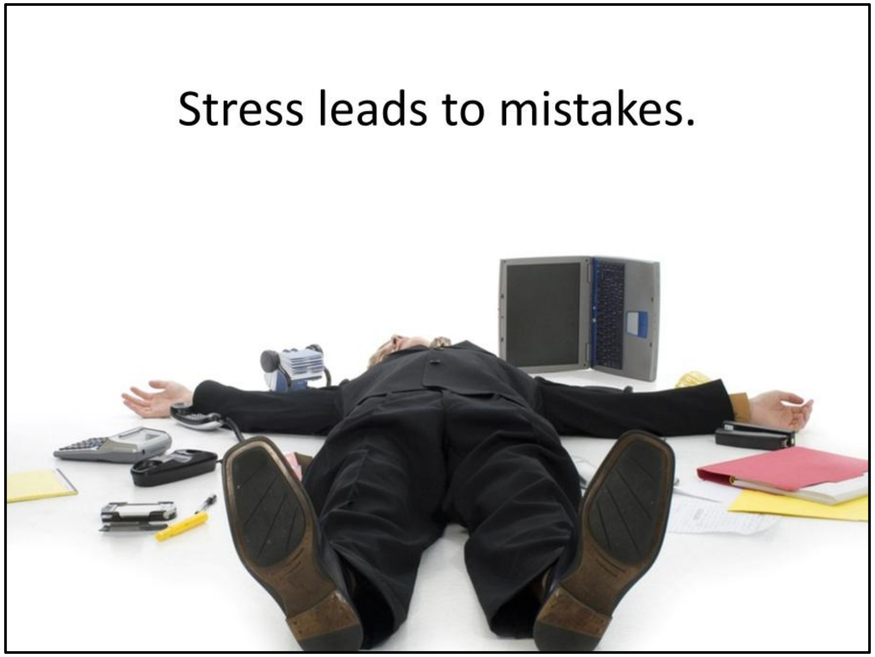
Best practices emphasize the need to prepare for incident response.

“Best practices” emphasize the need to prepare for incident response before the security breach occurs. Build the toolkit, train the staff, test restore capabilities, document roles and responsibilities... Indeed, that is the right approach to handling security incidents in a controlled manner.



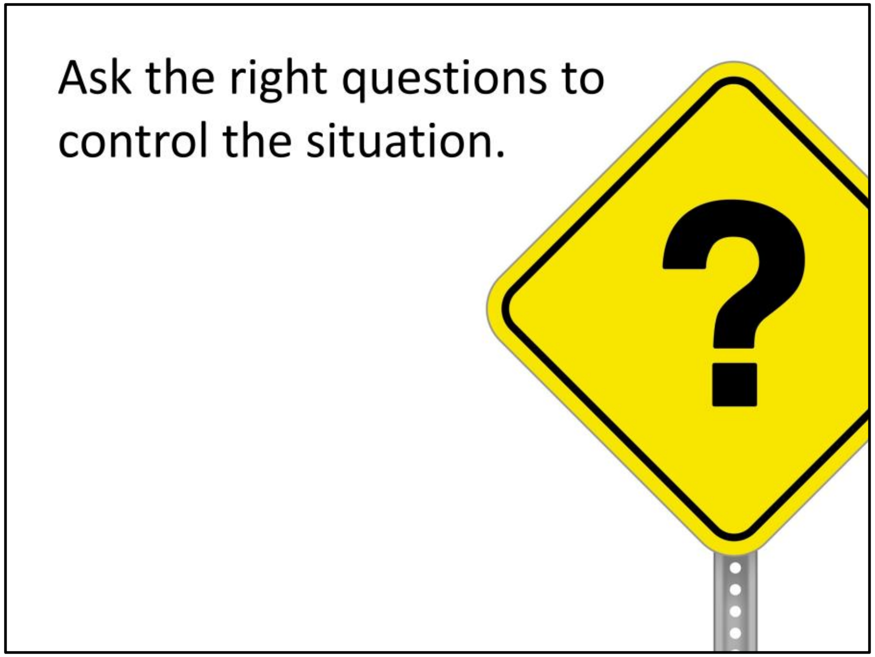
What if you never took the time to prepare?

What if you never found the time to prepare? In today's reactive world, you wouldn't be alone. Security incidents are often unexpected, and organizations are often unsure how to proceed when faced with them.



Stress leads to mistakes.

Dealing with security incidents is often high-pressure. The stress leads to mistakes and poor decisions made in the spur of the moment. Since small and mid-sized companies rarely have a dedicated incident response staff, the responders frequently lack the confidence and expertise that comes from handling the breaches routinely.

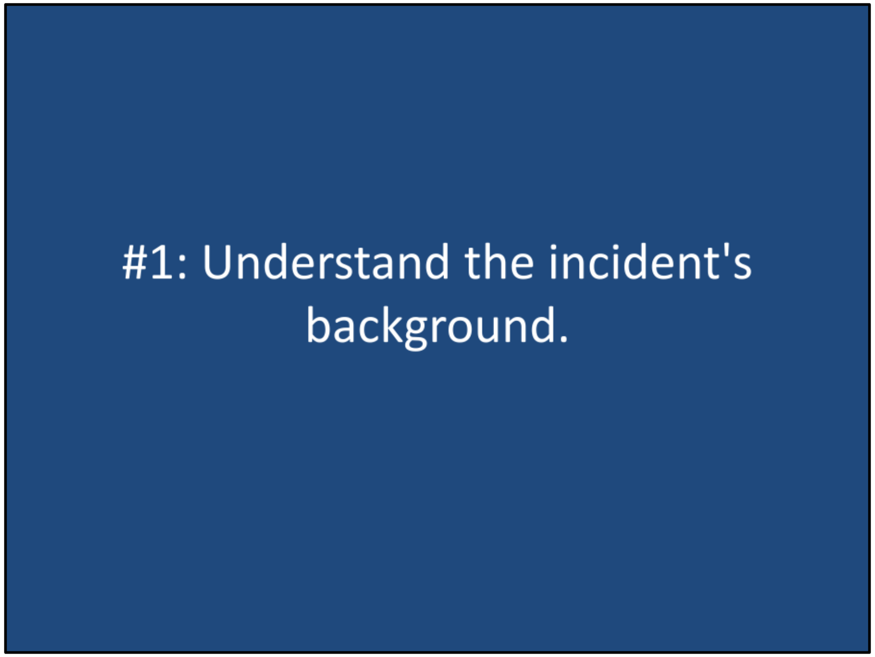


Ask the right questions to control the situation.

This talk discusses the questions an individual should ask when responding to a security incident. By having a list of such questions in advance, the incident handler will be able to take control of the situation quickly and assertively. I'll guide you through the questions worth asking, and will point you to "cheat sheets" that will offer additional useful questions.

To accomplish this, I suggest going through the following steps to become familiar with the situation, assign the appropriate responsibilities, and plan the next set of actions:

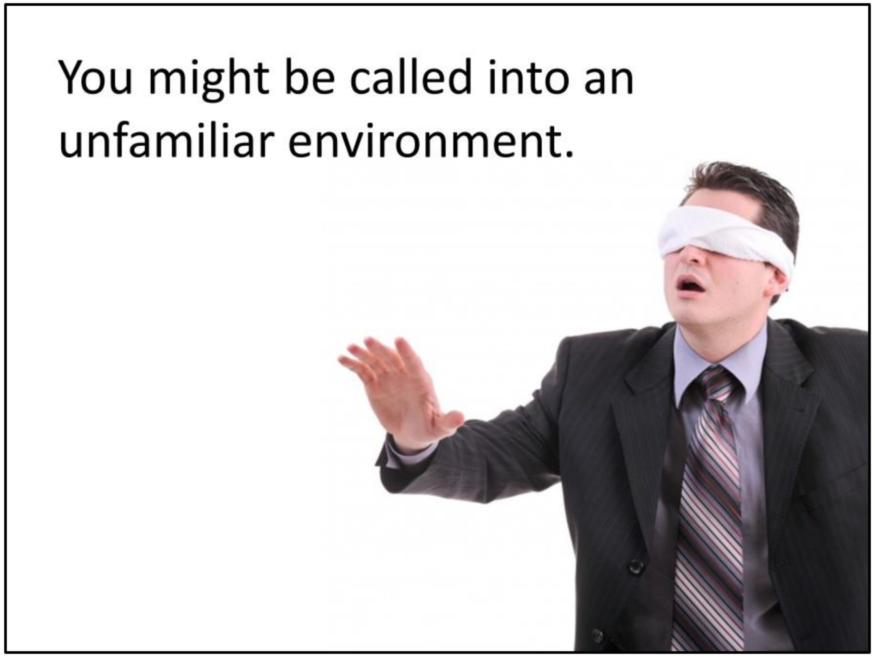
1. Understand the incident's background.
2. Define communication parameters.
3. Assess the incident's scope.
4. Review the initial survey's results.
5. Decide how to proceed with incident response.



#1: Understand the incident's background.

When first called onto the scene, the responder needs to understand the incident’s background.

Consider this scenario: Your phone rings at 1am. “We have a problem. We think our web server got hacked.” You, the incident handler, are asked to assist with the situation, so that the company can determine what happened and how to recover from the breach. Where do you start?

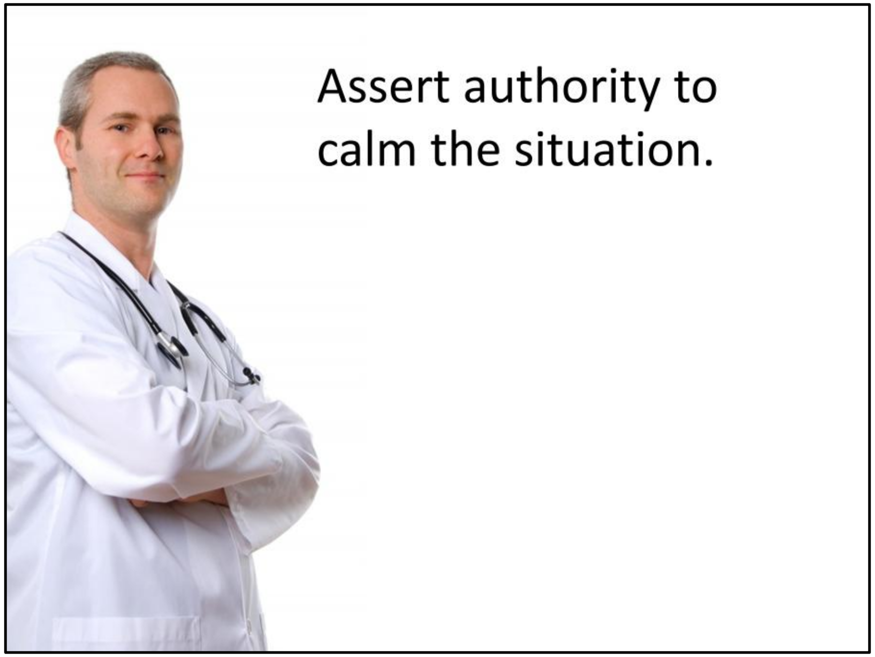


You might be called into an unfamiliar environment.

The first challenge of responding to an incident that appears out of the blue is that you may be called into an environment that you don’t know.

If you’re an external consultant, maybe you’ve never seen the details of your client’s infrastructure until now. Even if performing incident response as part of an internal team, you might be getting involved with people in an unfamiliar department. Or, maybe you’ve never had the opportunity to familiarize yourself with the network layout, its systems and devices, and the corresponding business processes that may be affected by the incident.

At this stage, it feels like you’re walking into the situation blindfolded.

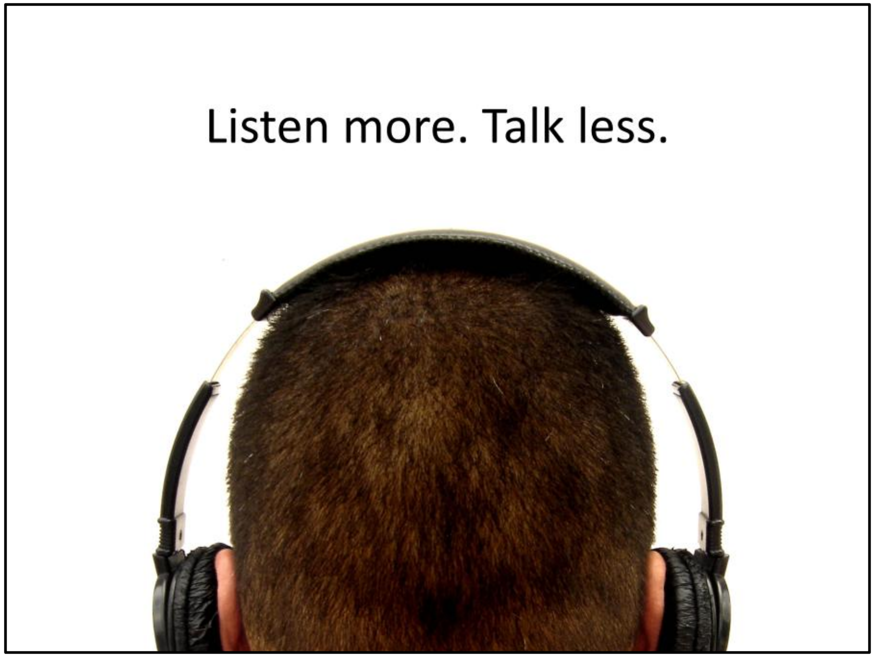


Assert authority to calm the situation.

Take a deep breath. Accept that the environment may be unfamiliar to you, yet remain confident that soon you'll get a handle on the situation. When people observe you being composed, they'll calm down too. Then, start by understanding people's impressions about what happened.

Did you notice that even during regular check-up exams, doctors often carry a stethoscope and wear a white coat? In part, this is to project an image that people have come to expect of a confident doctor: a knowledgeable professional who will find and diagnose any problem.

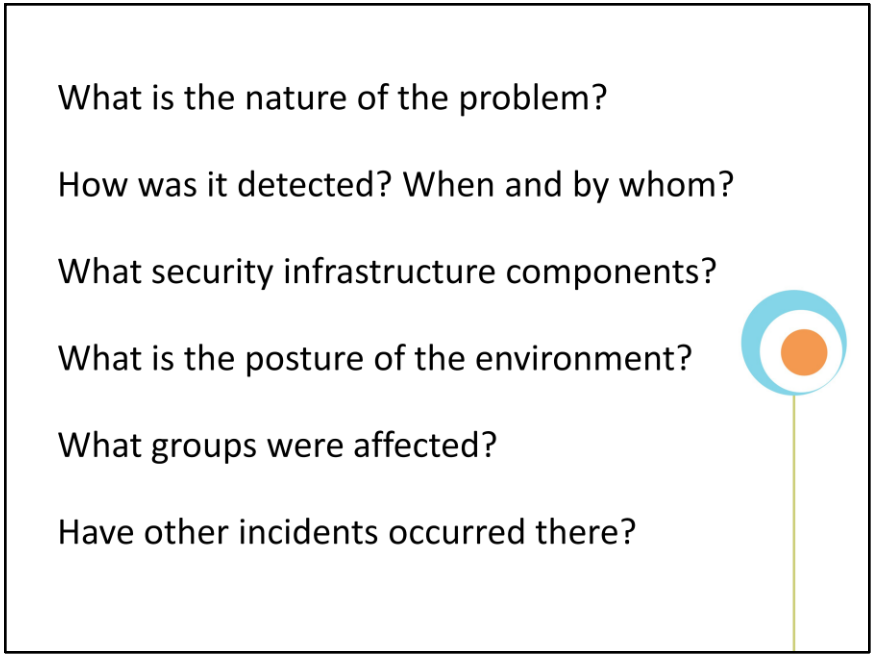
As an incident handler, you'll rarely need a stethoscope, but you can project confidence by the clothes you wear, the bag you carry and perhaps more importantly, by your posture, your voice, and the manner in which you ask the right questions.



Listen more. Talk less.

Listen to system names, business terms, applications, and other details people will mention in their answers. Take notes. It’s OK to take the time to listen, and hold off forming opinions or making recommendations until you’ve gotten some sense of what you will be dealing with. At this stage, listen more—talk less.

I remember a study that explored the situations under which doctors are likely to be sued for malpractice by their patients. It turns out that those doctors who take a few extra minutes to listen to the patients’ concerns were significantly less likely to end up in court. I suspect the same principle applies to other professions: if we pay attention to the concerns of the parties involved in the situation, we will all come out ahead.



What is the nature of the problem?

How was it detected? When and by whom?

What security infrastructure components?

What is the posture of the environment?

What groups were affected?

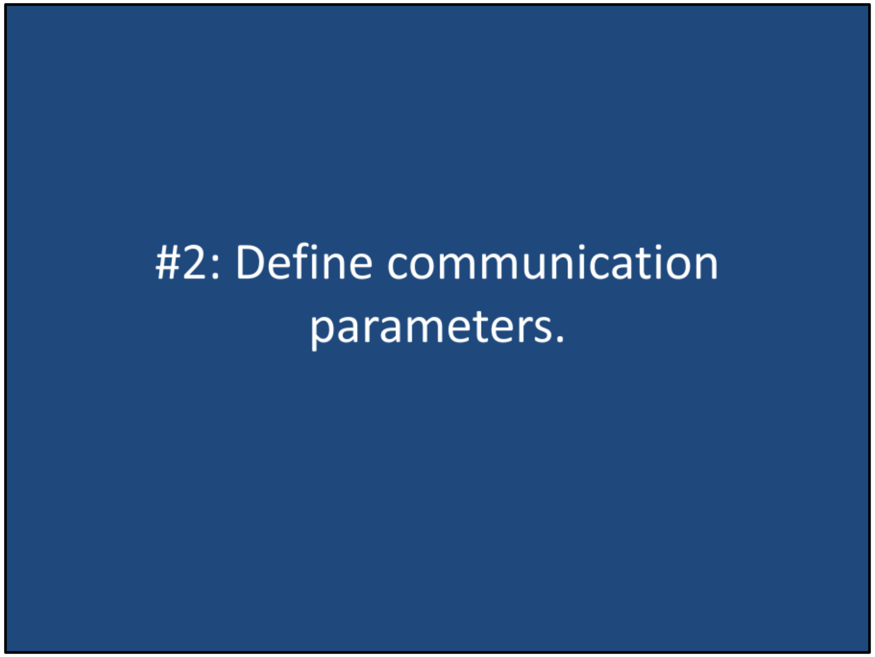
Have other incidents occurred there?

To assess the general nature of the problem you're being asked to tackle, make use of the questions summarized on this slide.

It's OK to ask open-ended questions, such as "What's the nature of the problem, as observed so far?" Then, inquire about the specifics: "How was the problem initially detected? When? By whom?" "What security infrastructure components exist in the affected environment? (e.g., firewalls, anti-virus, intrusion detection systems, etc.)"

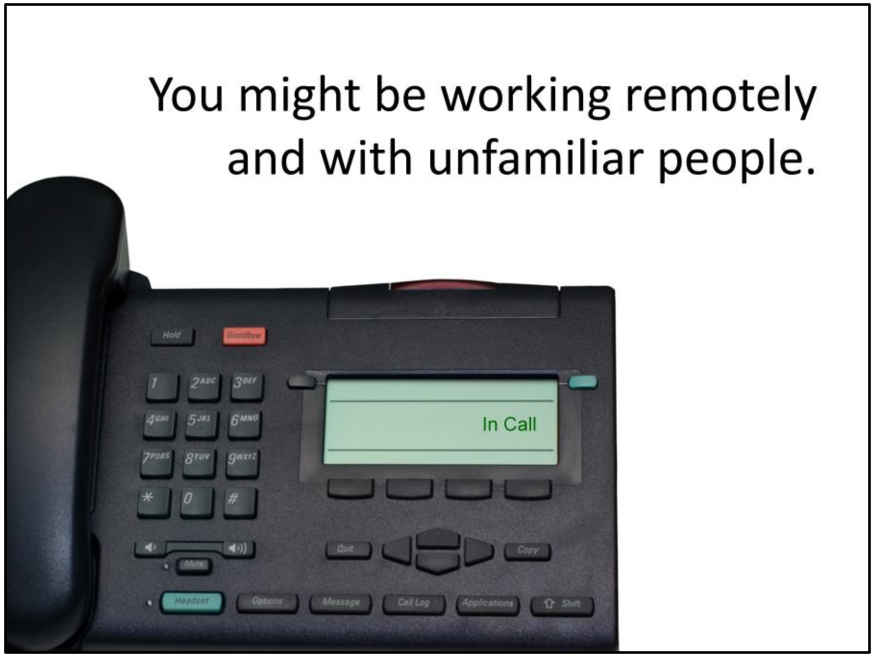
Get a sense for the overall security posture of the environment. Ask, "When was a security assessment conducted there? What were the results? What security incidents have occurred in the environment over the last two years?"

Also, get a sense for the business units that may have been affected by the incident and for the groups with which you may need to interact. Find out whether they are aware of the problem.



#2: Define communication parameters.

Once you've understood the background of the situation, focus on defining communication parameters for the incident response effort: who will be talking to whom, how, and for what purpose.



You might be working remotely and with unfamiliar people.

Hold
Goodbye
In Call
Quit
Copy
Headset
Options
Message
Call Log
Applications
Shift
Mute

In many cases, the handler begins participating in the incident remotely as part of a conference call. Even if you are located in the same room as many of the initial team members, others might be in remote locations, joining the conversation remotely.

Consider what communication mechanisms you could use to maintain contact with the team and ensure effective communications within the primary response team, as well as with business users, administrators in the field, and other groups.

If possible, communicate using the medium that is least likely to have been compromised. For instance, if the breach may have affected the email system, don’t rely on email. When in doubt, go out of band.

Understand who has what responsibilities. Assign roles.

Bad things happen when people make assumptions about who will do what when responding to the incident. Instead, assume that people don't know what to do and assign roles. If you don't have such authority, find out who does and explain to that person the importance of clearly assigning responsibilities for investigating the incident, collecting data, interacting with external groups, and so on.

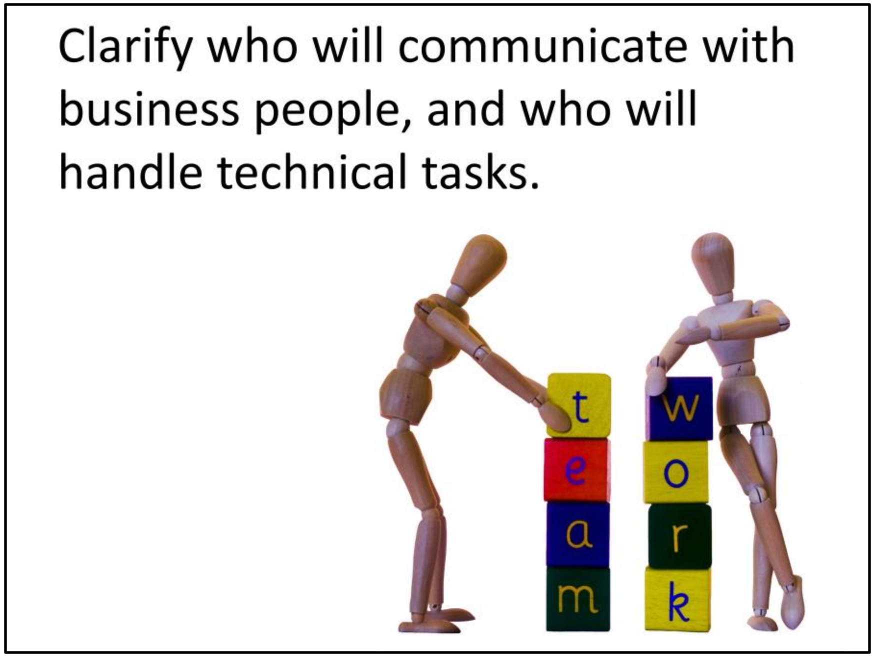
In many incidents, no one knows who is in charge. If you feel comfortable, and if you believe you are authorized to do so, take charge. Groups in crisis often appreciate someone taking control, if they believe the person is competent. The questions you're asking and the manner in which you do that, can demonstrate your skills and convince your team members of your abilities to lead this stage of the effort.

Keep in mind that while the incident handler may be in charge of coordinating incident response, this person rarely has the authority to make business decisions regarding affected IT resources. Find out who the business decision maker is, and keep that person in the loop.

Consider how the group will interact with other teams.

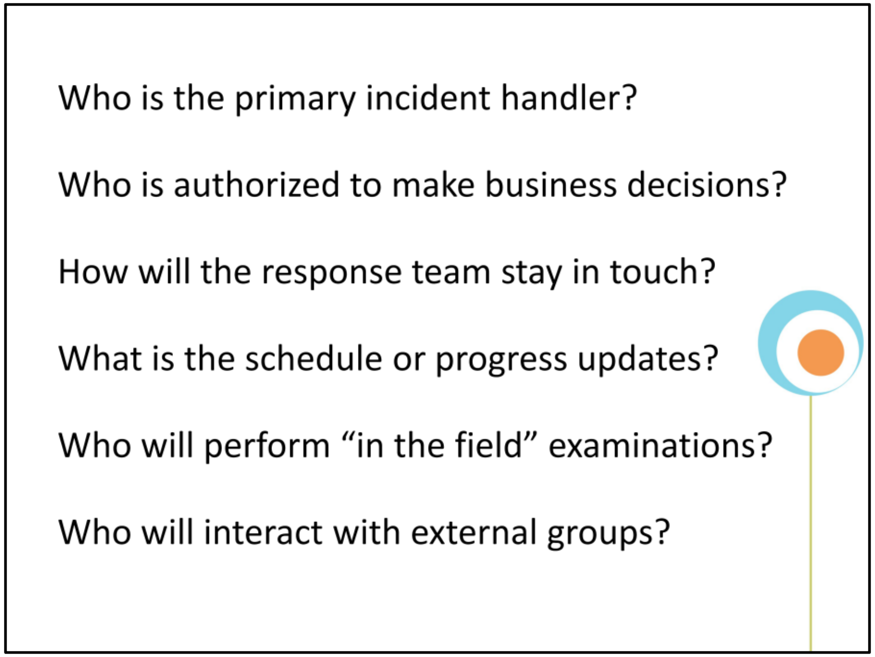
When considering which teams should be kept in the loop regarding the incident, don’t forget legal, executive management, public relations, as well as the business owners of the infrastructure affected by the incident. You’ll need to balance the benefits of distributing incident-related information on need-to-know basis with the benefits of getting input from these groups.

It is a good idea to schedule periodic and regular updates of your progress with the external teams, especially executives, so they understand where the organization in handling the situation. Stick to the schedule, say meeting once every two hours, even if you have nothing new to report; even that can be an important and stress-relieving communication to the parties who don’t directly handle incident-related tasks. Of course, such updates are time-consuming. Depending on the number of people available to you, assign the update task to someone who cannot assist with technical aspects of incident response, but has strong communication skills.



Clarify who will communicate with business people, and who will handle technical tasks.

It is often useful to assign two people to coordinating incident response: one person’s responsibilities are to handle communications with business people within the affected organizations. This allows the other—typically more technical person—to focus on the technical aspects of examining the situation.



Who is the primary incident handler?

Who is authorized to make business decisions?

How will the response team stay in touch?

What is the schedule or progress updates?

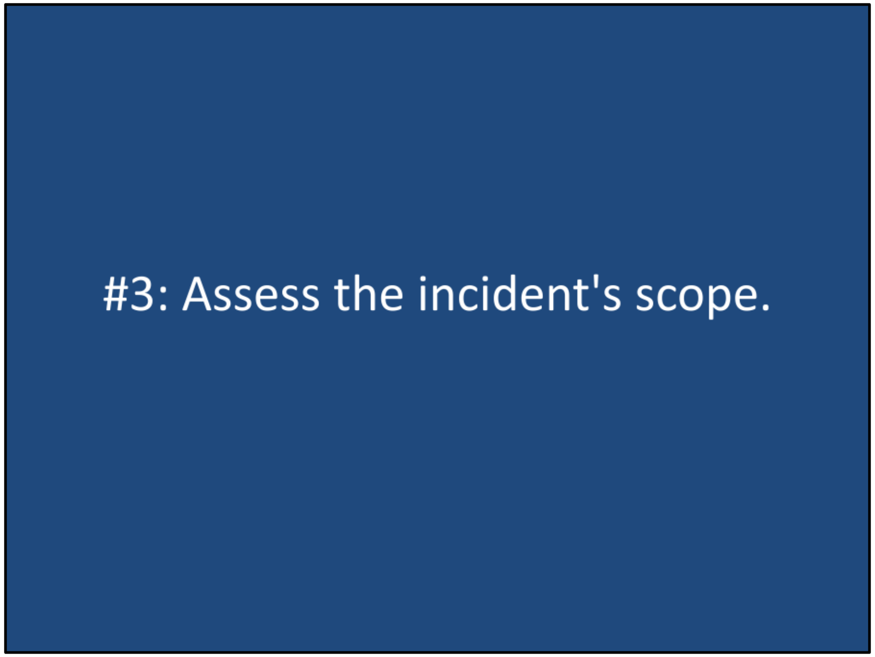
Who will perform “in the field” examinations?

Who will interact with external groups?

To define communication parameters for incident handling steps, first clarify who is in charge of coordination tasks, and who is authorized to make business decisions regarding affected IT resources.

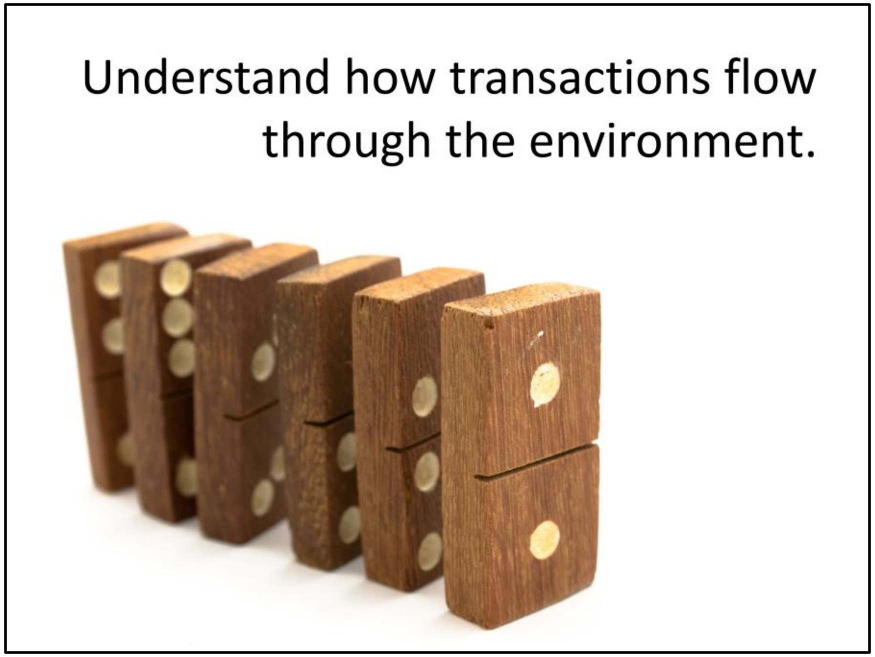
Also, decide how the team will stay in touch during the hours, days, maybe even weeks of the incident handling process. Make sure that the right contact details are available.

Determine when communications will occur and who will need to receive what information. Also, assign specific responsibilities to the individuals participating in incident response.



#3: Assess the incident's scope.

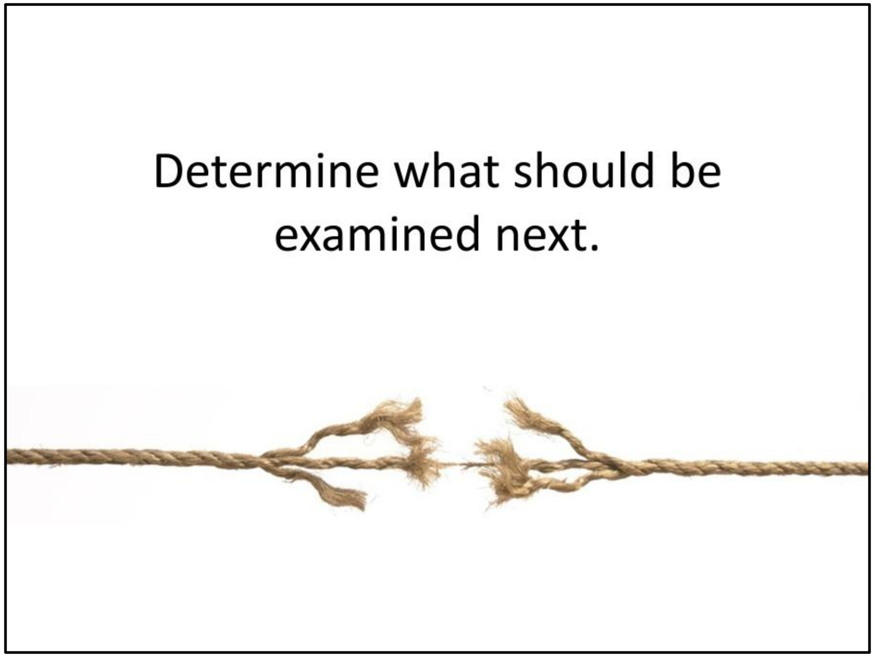
Once you have a good idea of the responsibilities of the members of the incident response team, take some time to drill into the details known about the situation so far.



Understand how transactions flow through the environment.

Consider a compromised web server. How does data flow through it? What kind of data is it? What access does the affected server has to other infrastructure components?

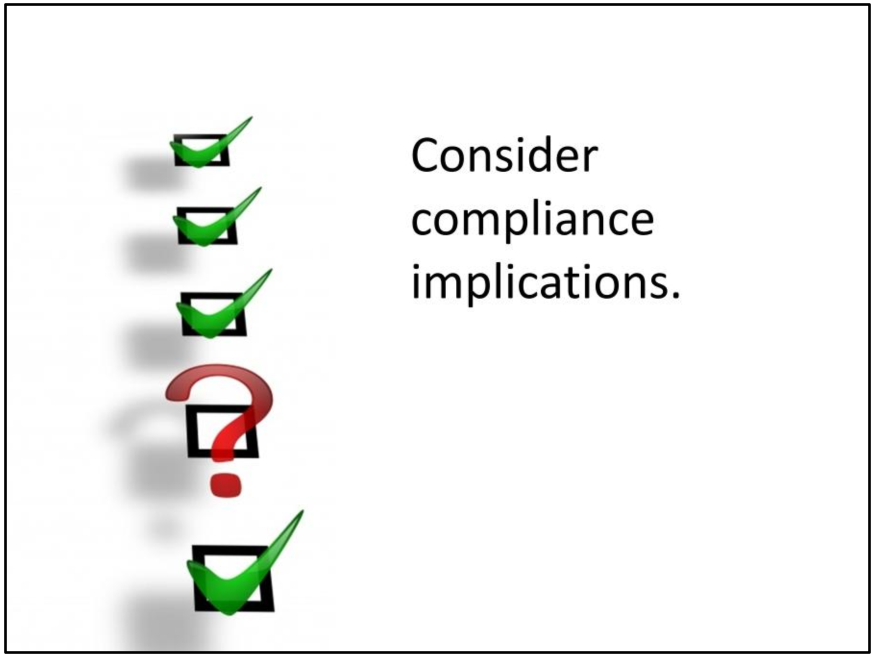
You’re looking for resource dependencies, as well as for the systems or applications that have access to applications in other security zones. For instance, if the compromised server has a script that logs into the database on another network, then the scope of the incident may be wider than initially believed.



Determine what should be examined next.

Once you have a general sense of the incident’s scope, consider what systems or applications you should examine next. Your human resources will likely be limited, so pick where you’ll focus your efforts carefully.

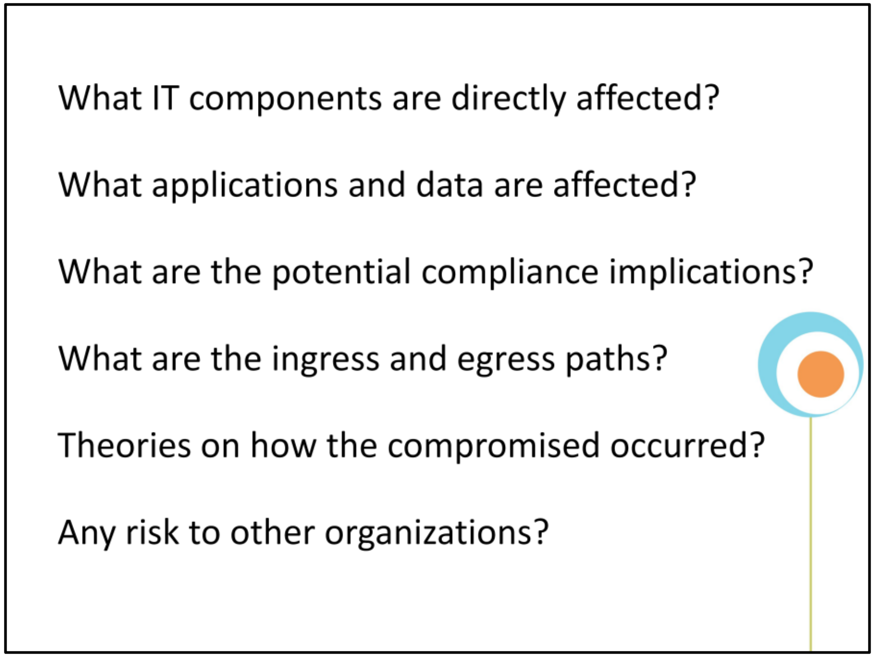
A system that’s particularly fragile, or an application that stores particularly sensitive data are good candidates for the resources you should examine sooner, rather than later.



Consider compliance implications.

In the modern world, awareness for the need to stay compliant with laws, regulations, and contractual obligations is high. This means that every incident should be evaluated with respect to the organization’s compliance requirements. As an incident handler, you may not be aware of what these requirements are, but you should ask the team questions about compliance, and if relevant, make sure executive management understands potential compliance implications.

Once you have a general sense for the compliance requirements (say, GLBA or PCI), understand the nature of the data involved in the incident and how it might (or might not) be relevant to compliance.



What IT components are directly affected?

What applications and data are affected?

What are the potential compliance implications?

What are the ingress and egress paths?

Theories on how the compromised occurred?

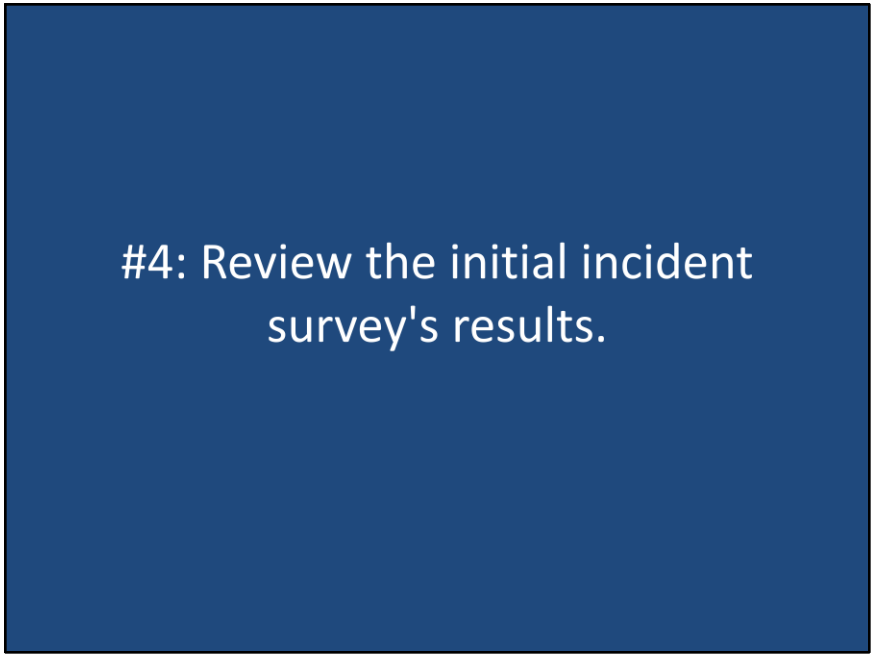
Any risk to other organizations?

As you assess the scope of the incident, ask questions about IT infrastructure components that may have been affected, including applications and the data that flows in them. Consider what compliance implications the incident may help, and make sure the appropriate executives within the organization are involved.

Also, at this stage you are starting to formulate theories about how the compromise may have occurred. To do this, ask about the possible ingress points into the environment: How is the firewall configured? What VPN links or private connections exist? How do administrators, customers, partners access the environment?

Next, get a sense for how sensitive information might leave the environment. Find out about the egress paths, and what controls exist to limit data leakage. When forming theories about the incident’s nature, ask for feedback from the people familiar with the affected environment.

Lastly, consider whether the compromised environment poses risks to other organizations and take the appropriate measures.

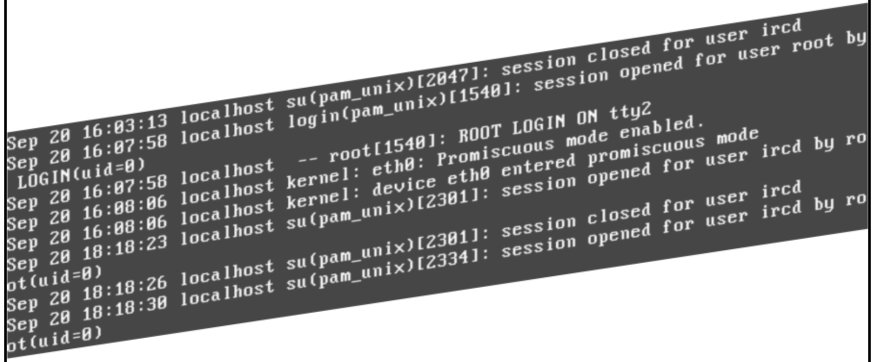


#4: Review the initial incident survey's results.

As this stage, you’ve developed a good sense for the affected environment and the incident’s scope, and are starting to formulate theories about how the incident may have occurred and what implications it may have for the organization.

To deepen you understanding of the situation, review the findings that have led the organization to believe that the incident occurred and that it may be security related.

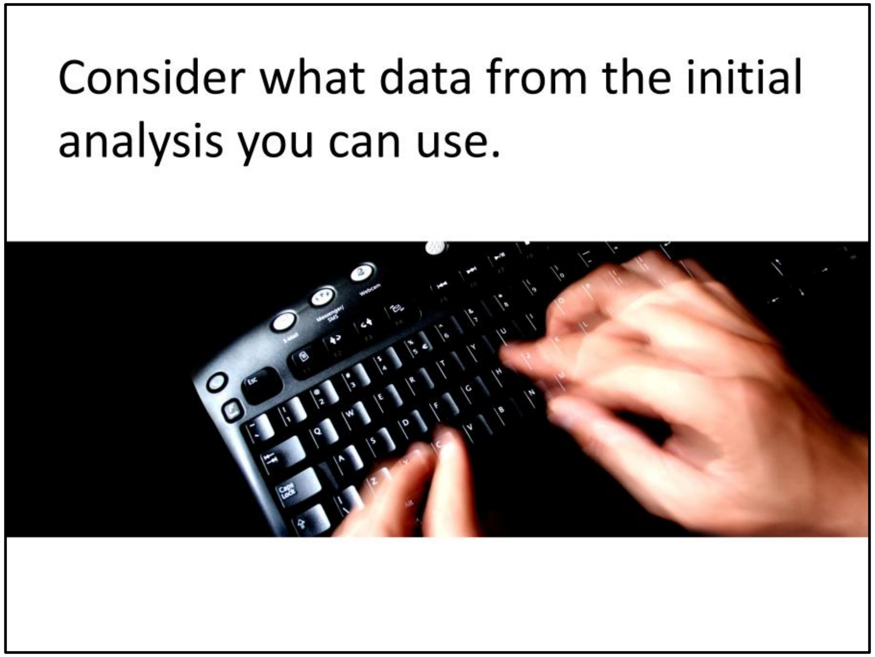
Understand what events and alerts were observed so far.



```
Sep 20 16:03:13 localhost su(pam_unix)[2047]: session closed for user ircd
Sep 20 16:07:58 localhost login(pam_unix)[1540]: session opened for user root by
 LOGIN(uid=0)
Sep 20 16:07:58 localhost  -- root[1540]: ROOT LOGIN ON tty2
Sep 20 16:08:06 localhost kernel: eth0: Promiscuous mode enabled.
Sep 20 16:08:06 localhost kernel: device eth0 entered promiscuous mode
Sep 20 18:18:23 localhost su(pam_unix)[2301]: session opened for user ircd by ro
ot(uid=0)
Sep 20 18:18:26 localhost su(pam_unix)[2301]: session closed for user ircd
Sep 20 18:18:30 localhost su(pam_unix)[2334]: session opened for user ircd by ro
ot(uid=0)
```

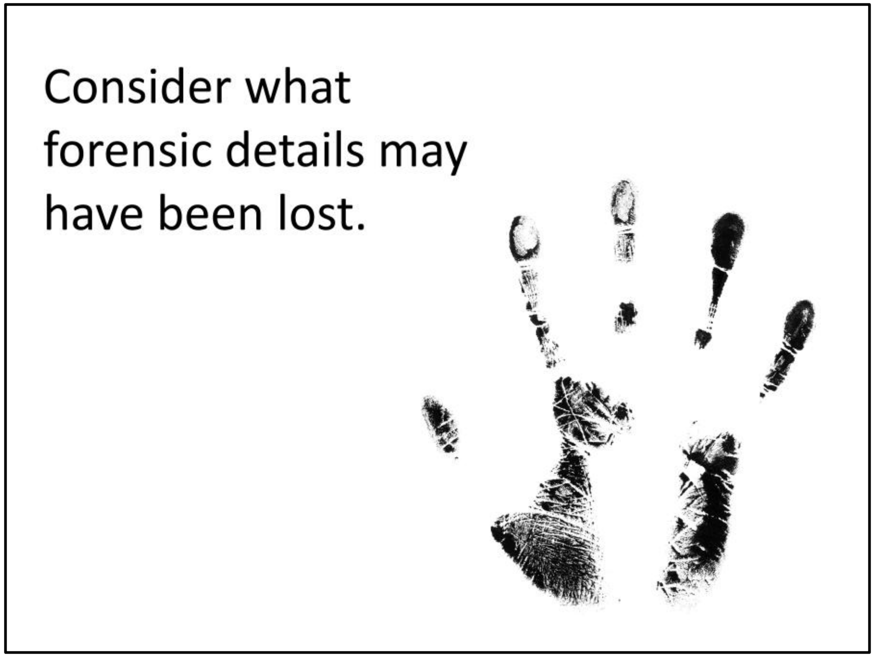
Chances are, before you got called into the situation, someone from the organization have observed events that led him or her to believe that a security incident may have occurred. Find out what events were observed and understand the basis for the conclusions of the initial observers or responders.

Ask about system, application, firewall, IDS, and other relevant events that may have been observed.



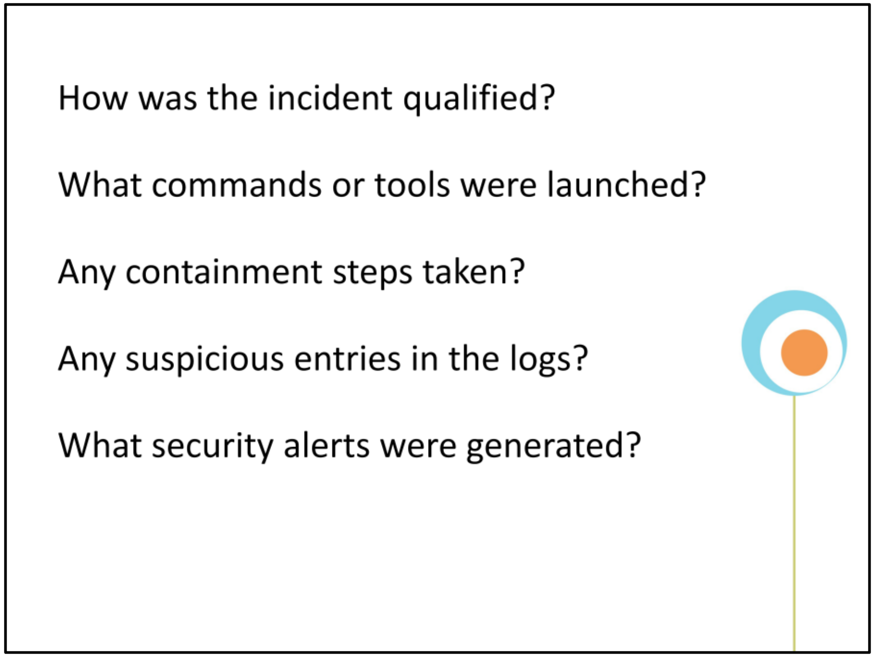
Consider what data from the initial analysis you can use.

In many incidents that involve servers, the system administrator has looked around to investigate the initial problem report and to qualify the incident as being security-related. To do so, the administrator probably looked at the system’s processes, applications, scheduled jobs, network connections, and so on.



Consider what forensic details may have been lost.

Recognize that whenever a person examines the system, the system’s state gets modified. This means that when the system administrator performed an initial survey to qualify the incident, he or she may have inadvertently removed details that would have helped during the incident’s examination or forensic analysis. Ask what tools were used during the survey and what commands were executed on the affected systems. This will help you get a sense for the kind of information that may have been lost.



How was the incident qualified?

What commands or tools were launched?

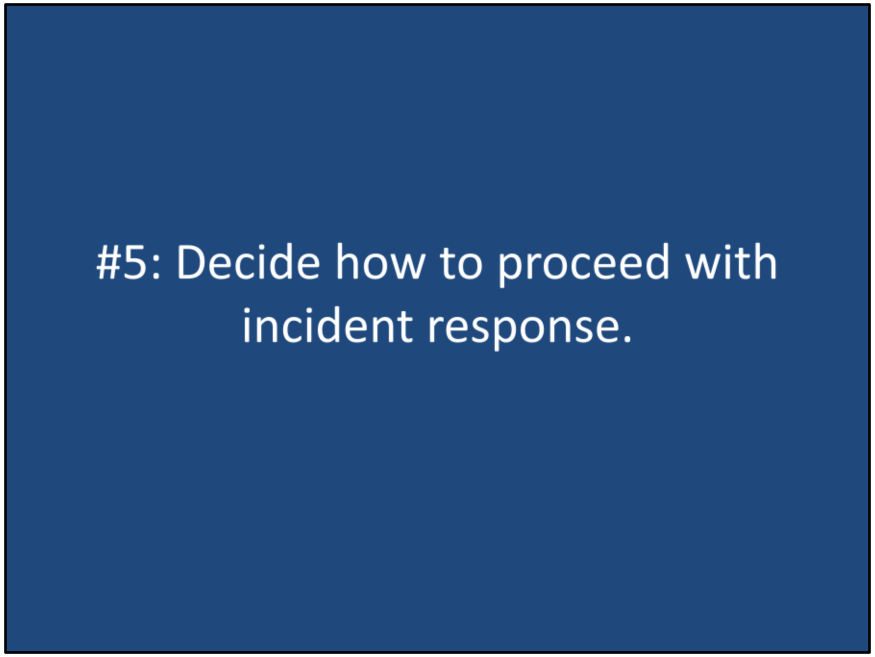
Any containment steps taken?

Any suspicious entries in the logs?

What security alerts were generated?

As you review the findings of the initial survey of the situation, which was probably performed before you got involved, understand how the incident was qualified. Ask questions about the tools that were used and the alerts or log entries that were observed. Also, understand what information from the affected systems may have been lost as part of the initial analysis.

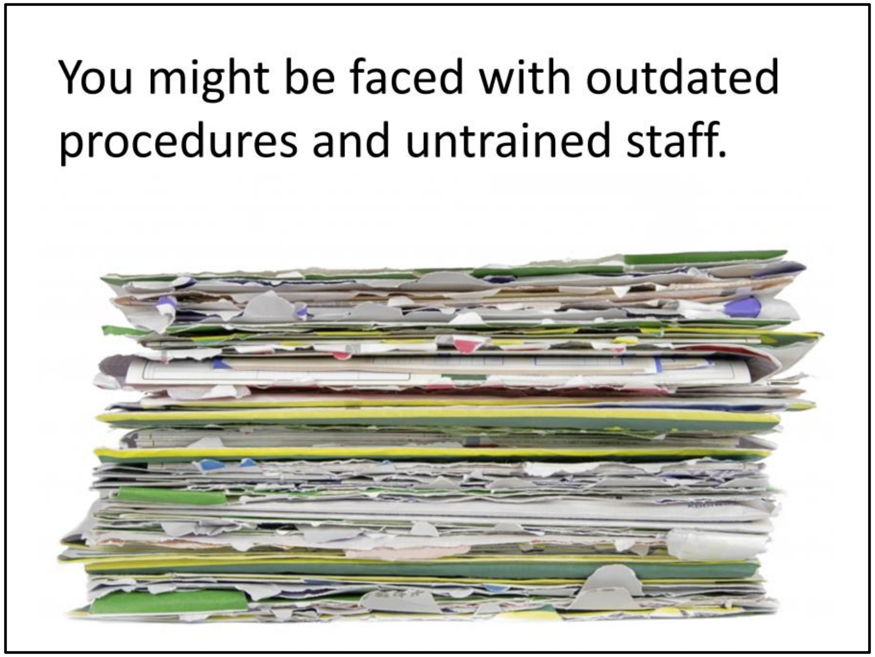
It's also important to understand what steps were taken so far to contain the problem. Even before you got involved, someone may have terminated the suspicious process, rebooted the system, or unplugged it from the network. Knowing what was performed will help you assess the current risk to the infrastructure and will assist in planning the next incident response steps.



#5: Decide how to proceed with incident response.

Now that you have a good understanding of the current situation, you are ready to decide how to proceed with the more formal incident response steps. These are often based on the incident handling steps advocated by NIST and SANS, which involve:

1. Preparation: Gather and learn the necessary tools, become familiar with your environment.
2. Identification: Detect the incident, determine its scope, and involve the appropriate parties.
3. Containment: Contain the incident to minimize its effect on neighboring IT resources.
4. Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.
5. Recovery: Restore the system to normal operations, possibly via reinstall or backup.
6. Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.

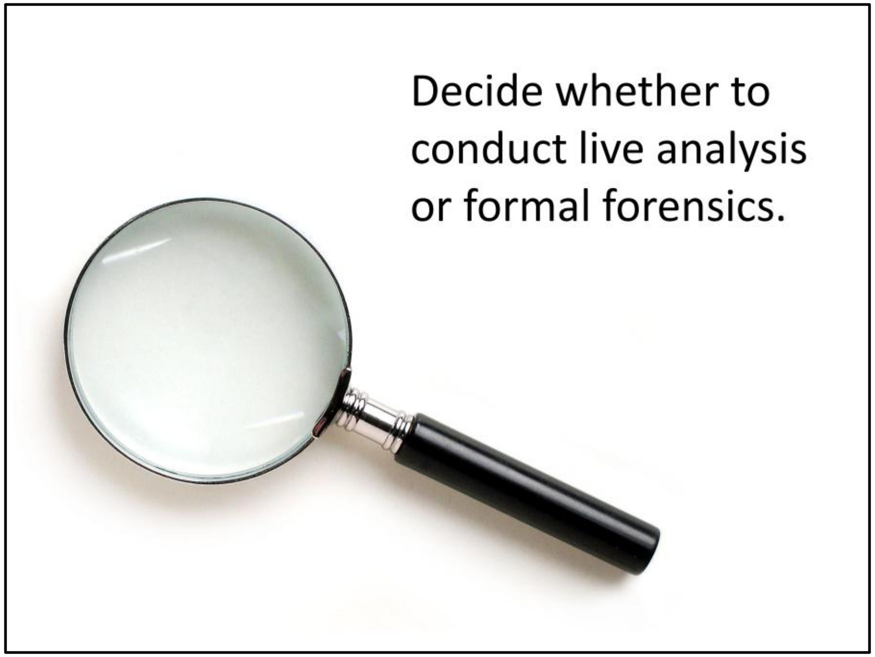


You might be faced with outdated procedures and untrained staff.

Check whether the organization has documented an incident response plan, in the form of policies, procedures, or check lists.

Many companies have never gotten around to documenting their incident response plans, or never formulated the plans to begin with. Even if the documents exist, don’t assume that they are up-to-date, or that the staff has read them or is trained to follow them.

Find out the reality of the situation: understand what specific incident response requirements are in place, and who among the incident handling team members is capable of performing which tasks.



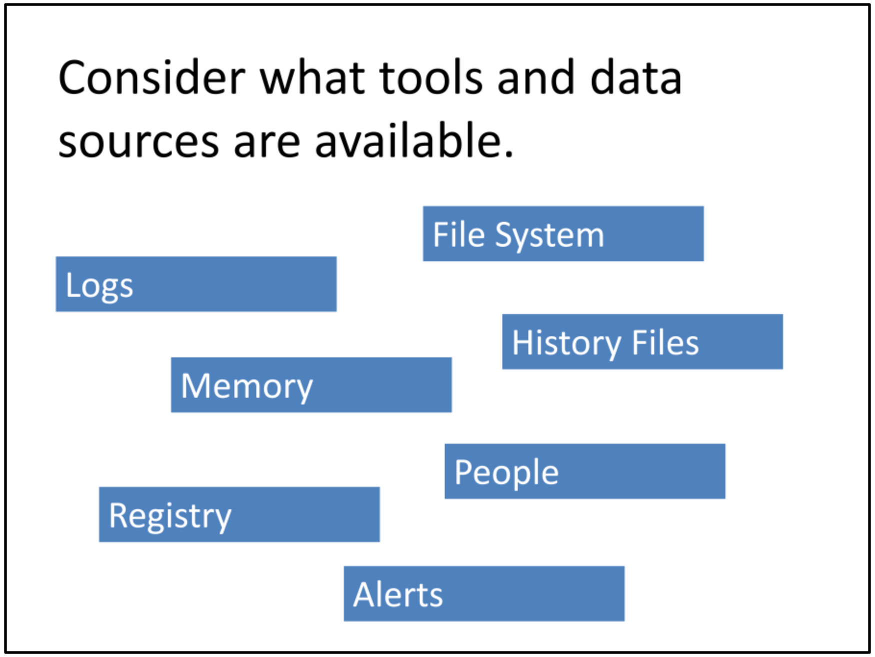
Decide whether to conduct live analysis or formal forensics.

The team now needs to make an important decision. Should the subsequent analysis follow formal forensics methodology, or should the team perform live analysis of the affected systems?

Formal forensic approaches take the time and care to examine the affected systems in a way that leaves a few footprints as possible on it, collecting data so that it could, if necessary, be used as evidence in court. These approaches are well-documented, though typically require forensics training and specialized tools.

Many organizations now chose to forego formal forensics in favor of a faster and less formal approach that analyzes the system live, as its running, without necessarily shutting it down, cloning its drive or using forensically-sound tools. Live analysis tends to be faster than forensics and focuses on performing an examination that’s “good enough” to return the organization to business as soon as possible.

Find out which business executive is authorized to decide between forensics and live analysis approaches, and understand how the team should proceed. It is often wise to document this decision in writing.

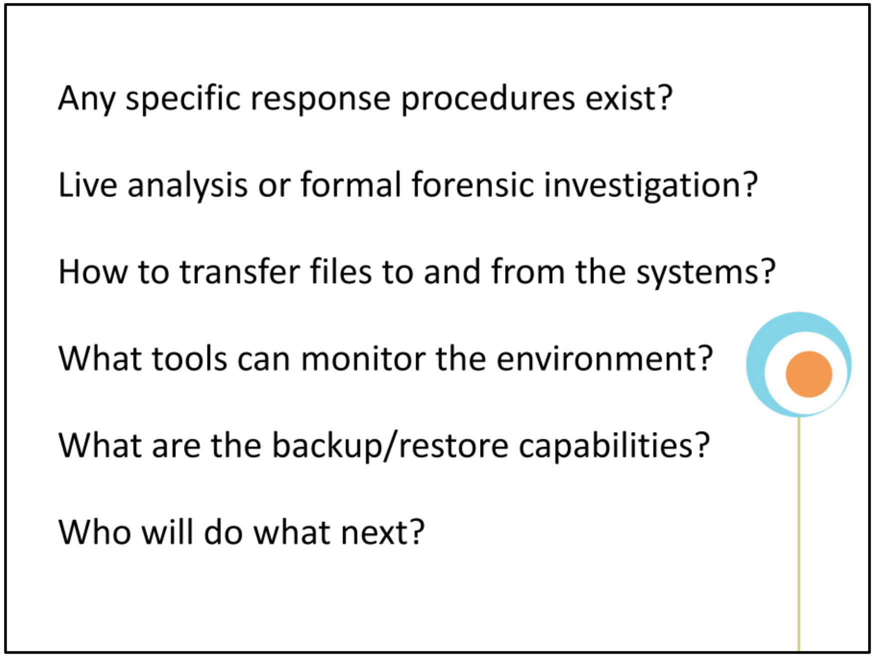


Consider what tools and data sources are available.

- File System
- Logs
- History Files
- Memory
- People
- Registry
- Alerts

Understand what tools and data sources are available to you for further understanding the scope of the incident and devising a recovery plan. Some environments are rich with visibility, in the form of system logs, application logs, firewall logs, IDS alerts, network sniffer records and so on. Less mature environments may have very few data sources, and may even require you to prepare tools like network sniffers on the fly.

In many incidents you'll want to increase the monitoring of the affected environment to assess whether its being actively used by an attacker. Consider what tools may assist you in that task.



Any specific response procedures exist?

Live analysis or formal forensic investigation?

How to transfer files to and from the systems?

What tools can monitor the environment?

What are the backup/restore capabilities?

Who will do what next?

As you plan your next steps, understand whether specific processes have been define and assess whether it’s realistic to follow them. In the worst case, you’ll need to think on your feet and make decisions as the situation develops.

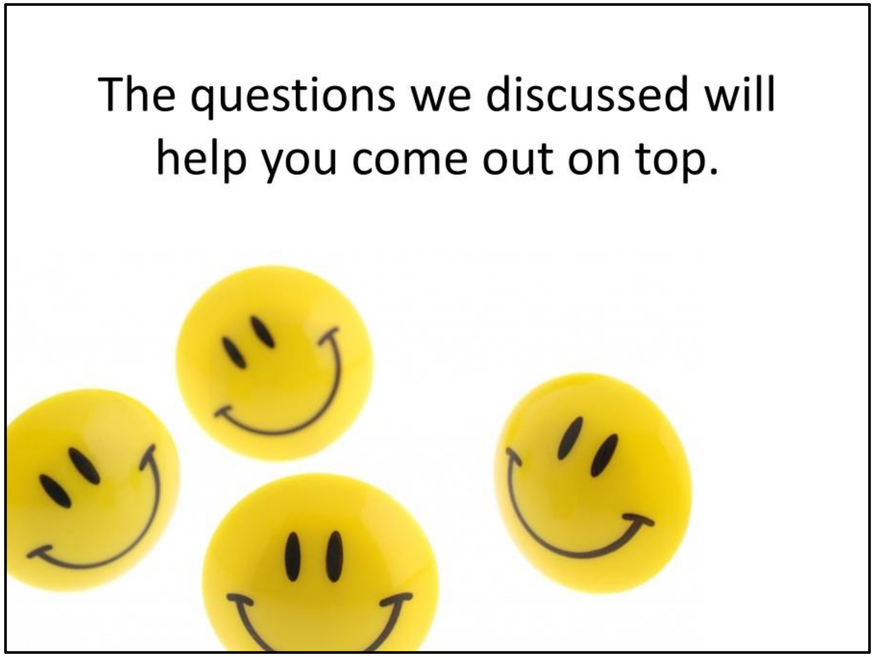
Once you know whether you should proceed with formal forensic analysis or whether live analysis is a good start, determine what tools you can and should use to better understand the problem.

Also, consider how you will transfer log files from the affected environment and how you will put the necessary tools into that environments. Back-end infrastructure might be segmented from the networks to which you or administrators have easy and unrestrained access. Transferring files to and from locked-down environments is often difficult and time-consuming; be prepared for that challenge.

As you plan your next steps and consider how you’ll return to normal business operations, understand what backup-restore mechanisms are in place to recover the system’s state. Don’t assumes that if even backup procedures exist, they are being followed or have been tested.

Incidents will happen, whether you’re prepared or not.

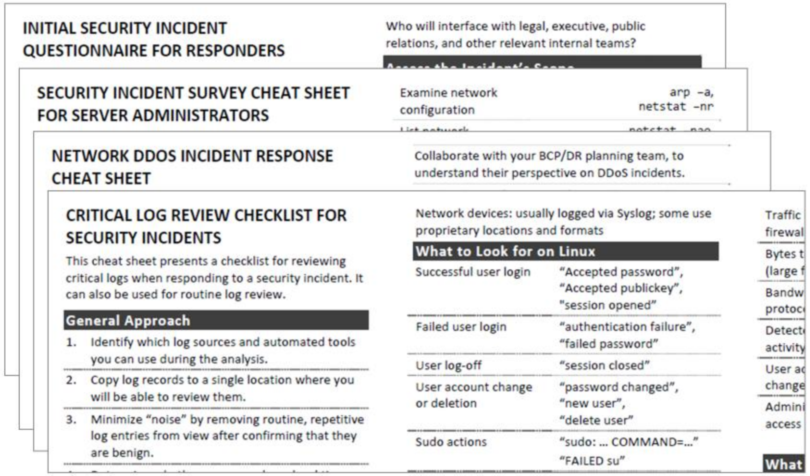
In this presentation, we discussed a number of challenges facing a responder when he or she enters the scene of a security incident. Despite the best of intentions, many organizations are not as prepared for handling such situations as they would like to be. Of course, those who are better prepared, will have an easier time minimizing the damage and handling the situation faster and less painfully.



The questions we discussed will help you come out on top.

My approach to taking control of an incident, regardless of the organization’s state of preparedness, involves having a list of questions to ask at the onset of the incident. We discussed many of these questions in the earlier slides.

I prepared a few “cheat sheets” that might help you.



INITIAL SECURITY INCIDENT QUESTIONNAIRE FOR RESPONDERS

Who will interface with legal, executive, public relations, and other relevant internal teams?

SECURITY INCIDENT SURVEY CHEAT SHEET FOR SERVER ADMINISTRATORS

Examine network configuration	`arp -a,`
	`netstat -nr`

NETWORK DDOS INCIDENT RESPONSE CHEAT SHEET

Collaborate with your BCP/DR planning team, to understand their perspective on DDoS incidents.

CRITICAL LOG REVIEW CHECKLIST FOR SECURITY INCIDENTS

This cheat sheet presents a checklist for reviewing critical logs when responding to a security incident. It can also be used for routine log review.

General Approach

1. Identify which log sources and automated tools you can use during the analysis.
2. Copy log records to a single location where you will be able to review them.
3. Minimize “noise” by removing routine, repetitive log entries from view after confirming that they are benign.

Network devices: usually logged via Syslog; some use proprietary locations and formats

What to Look for on Linux

Successful user login	“Accepted password”, “Accepted publickey”, "session opened”
Failed user login	“authentication failure”, “failed password”
User log-off	“session closed”
User account change or deletion	“password changed”, “new user”, “delete user”
Sudo actions	“sudo: … COMMAND=…” “FAILED su”

Traffic firewal

Bytes t (large f

Bandw protoc

Detect activity

User ac change

Admini access

What

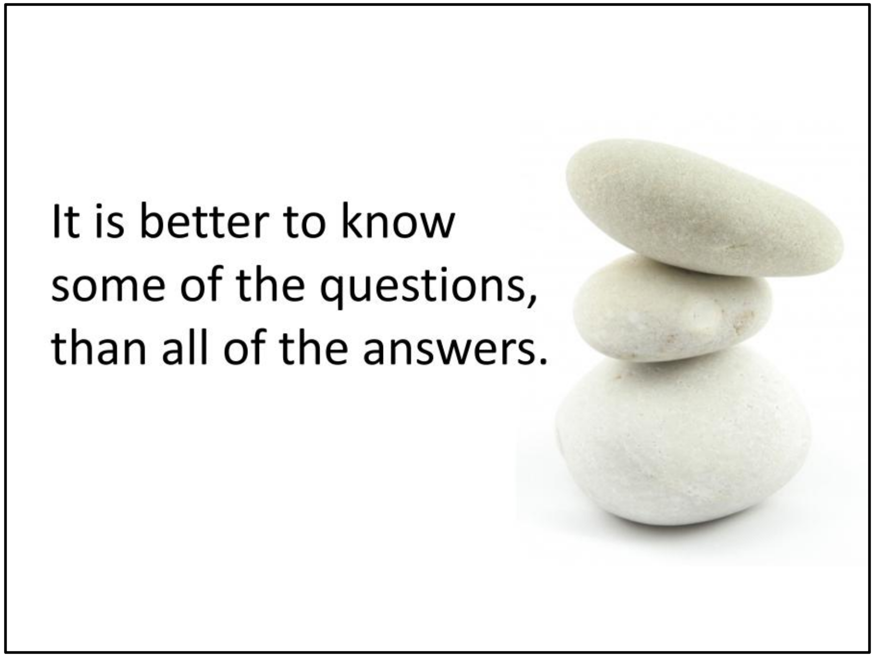
Recognizing that many organizations and individuals find themselves unprepared for dealing with security incidents they may encounter, I prepared several 1-page “cheat sheets” that you might find useful. You can download them in PDF and Word formats from http://zeltser.com/cheat-sheets, and modify them as you see fit.

The first cheat sheet summarizes and expands upon the list of questions I’ve been presenting during this briefing. It’s called *Initial Security Incident Questionnaire for Responders*.

My *Security Incident Survey Cheat Sheet for Server Administrators* captures tips for examining a suspect server to decide whether to escalate for formal incident response.

The *Network DDoS Incident Response Cheat Sheet* captures advice for battling a network DDoS attack on your infrastructure.

Lastly, I co-authored the *Critical Log Review Checklist for Security Incidents* with Dr. Anton Chuvakin to document tips for reviewing critical logs when responding to a security incident.



It is better to know some of the questions, than all of the answers.

One last thought, Zen-style...

It’s better to know some of the questions, than all of the answers.

Really. The answers can quickly become outdated, as the environment, people and processes change. The answers need to be maintained and take a lot of care and feeding to remain accurate across months and years. However, if you know what questions to ask even when the pressure is high, you’ll know where to find the answers that are right for that very moment.

Lenny Zeltser

www.zeltser.com
twitter.com/lennyzeltser
lenny@zeltser.com

If you have any questions for me, please let me know. I’ll do my best to answer them as accurately as I can, given the caveat I mentioned on the previous slide regarding answers.

I’d also love to hear from you if you have any comments regarding this presentation, either what you liked about it, or your suggestions for improving it.

If you’re curious about my professional and extracurricular activities, take a look at my website http://zeltser.com. If you’re on Twitter, you will find me at http://twitter.com/lennyzeltser.