Chapter 12

Strategy 10: Stop. Think. Respond . . . Calmly

In a given year, SOCs will track hundreds or even thousands of cases, vulnerabilities, and threats. In each instance, the SOC must render a response that is appropriate, given the criticality of the situation. As a result, the majority of our incident handling should be routine and not cause for an emergency. In our tenth and last strategy, we examine techniques for addressing incidents in a professional, trustworthy, and effective manner. Accordingly, we discuss how to track incidents from cradle to grave.

12.1 Professional Incident Response

When there is a major incident, all eyes are on the SOC. If it has followed the guidance laid out in the previous sections of this book, most aspects of incident handling should come naturally. The SOC should have the following in place:

- A workforce with strong technical, analytic, and communication skills
- CONOPS, SOPs, and escalation procedures that guide the SOC's actions
- Means to coordinate analysis and response activity among members of the SOC
- Established POCs with whom to coordinate response actions
- Established and ad hoc log, PCAP, and live system image data collection and analysis tools sufficient to help establish the facts about incidents

- The authorities to enact swift and decisive response actions when called for and passive observation or incident de-escalation when they are not.

We must ensure our incident response is efficient, effective, relevant, and complete. Failure to do so could undermine the SOC mission, which is to limit damage, assess impact, and render a durable response. Let's consider some dos and don'ts when we think the SOC has found something bad:

- **Follow your SOPs.**
  No two incidents are exactly the same, and some are more complex than others. That said, most incident handling should be routine—easily handled by one or two analysts—and no great cause for concern. They should fall under well-structured SOPs that can be picked up by members of the SOC and easily understood. This saves the SOC's energy for cases that fall outside the daily routine, such as root compromises, whose response is not entirely formulaic and cannot be completely scripted.
- **Don't panic.**
  When police, firefighters, or paramedics arrive on the scene of a 911 call, they are cool, calm, and collected. They are able to assess and stabilize the situation and direct response accordingly. Doing so engenders trust on the part of the complainant or the victim. The SOC should follow the same practice. For those not familiar with CND operations, an incident is cause for great excitement and emotion. This can lead to reactions that amplify damage. The SOC will gain the trust of those involved if it provides measured response, no matter what circumstances it encounters.
- **Don't jump to conclusions.**
  "Oh my god, we're being attacked!" has been uttered in response to many an incident. Are we really? What is causing us to draw this conclusion? Are we just looking at IDS alerts, or do we have a system image that clearly indicates a root compromise? It takes a skilled analyst to correctly interpret what a set of security logs or media artifacts do or do not say. Recognizing the limits of our understanding of a situation is critical, especially when an unambiguous "smoking gun" is hard to find.
- **Be careful about attribution.**
  A NetFlow record may indicate that an entity from Kazblockistan is scanning our enterprise or is receiving DNS beaconing from a compromised host. Is it really someone in that country or is that just the next hop out in the network connection? Furthermore, just because an audit log is stamped with user Alice, was it really Alice sitting at the keyboard, was it Trudy who compromised Alice's account, or, perhaps was it automated activity using Alice's identity? Most times, an incident responder can only propose theories and suggest a degree of confidence about who is behind a given

set of malicious or anomalous activities. Unless we can actually prove who is sitting at the keyboard, user attribution is theory and not fact.

- **Assess the full extent of the intrusion.**
  We have a malware hit against a box—Was it the only one compromised? We see a privilege escalation attack on a given system—Is this box linked through a trust relationship to other systems or enclaves? We found some malware on a box involved in a compromise—What other indicators can we find that point to what activity, by whom, and at what stage in the attack life cycle? Shallow analysis can be very dangerous, and the operator must endeavor to understand the full scope of what has occurred. *Gather as much relevant evidence as possible and exploit it to the maximum extent practicable.* This goal must, of course, be balanced with the need to act in a timely manner, even though you don't have *all* of the facts nailed down.
- **Understand the "so what?"**
  When the SOC explains an incident to stakeholders and upper management, the bottom line is not about bits and bytes, it's about mission, dollars, and, sometimes, lives. The SOC must translate technical jargon into business language. There are four questions that should be answered: (1) what (and/or who) was targeted, (2) was the adversary successful, (3) who is the adversary and what is its motivation, and (4) how do we continue the mission?
- **Follow rules of evidence collection and documentation, when appropriate.**
  The more critical the incident, the greater pressure the SOC will likely face. All too often, the SOC must draw both a timeline of the adversary's actions and a timeline of how the SOC responded. By carefully documenting its incidents and incident handling, the SOC can demonstrate the rigor behind its actions, when scrutinized. Documenting everything also means clearly having incident evidence in careful order. Finally, in the case of collecting artifacts and documenting actions taken, the SOC must carefully follow any applicable digital forensics or evidence collection laws for their jurisdiction. In fact, it often is best to err on the side of having forensically sound evidence, even when the SOC doesn't initially think the case has any legal significance.
- **Provide measured updates at measured times.**
  When a hospital patient goes in for surgery, family members sit for hours in a waiting room, anxiously awaiting news of their loved one's fate. While it would be great to hear frequent updates on their loved one's procedure, doing so would impede the surgeon's ability to complete the operation correctly and in a timely manner. When firefighters show up at the scene of a fire, the onsite incident commander calls the

shots. The district fire chief and the city mayor generally don't show up because there is no need. For most SOCs, these clear boundaries of trust and communication are not as well established as for doctors or emergency responders.

In cyber incident response, the SOC must play a careful balancing act between keeping management and constituents up-to-date and executing analysis and response efforts. If not careful, key analysts will constantly be pulled away from actually analyzing and responding in order to brief stakeholders. It is wise for SOC leadership to manage expectations of constituency seniors and run interference so the SOC can continue with the mission.

During a serious incident, the SOC may consider two separate regular meetings every day or two. The first is for direct players in the incident who can talk bits and bytes, and usually occurs informally on the SOC ops floor or over the phone. The second is a more formal SA update to upper management. This keeps seniors out of the weeds, ensures everyone is on the same page, and allows SOC personnel to focus on operations.

The SOC should also be careful about which parties are given status updates. Many parties want to know about every incident that leaves the SOC, yet, in many cases, their need to know is tenuous at best. The SOC can cut down on second-guessing and time spent reporting status to external parties by carefully negotiating a reporting structure for major incident types.

In addition, it's important to let junior members of the SOC team know that they are not to release details on the incident without authorization. A SOC's credibility can be easily destroyed by just one or two cases where a Tier 1 analyst picked up the phone and gave "half-baked" incident details to the wrong constituent. Furthermore, the SOC must be careful not to let details of incidents leak out in emails or other communications that could be seen by an adversary.

- **Carefully assess the impact of countermeasures and response actions.**
  The SOC must work with system owners and sysadmins in order to get to the bottom of an incident through careful artifact collection, analysis, and damage assessment. The SOC should not perform "knee-jerk" response actions that may take down key mission systems or networks. Blindly reimaging and reinstating systems involved in an incident without performing artifact and malware analysis is almost always counterproductive, because (1) we don't know whether the adversary has lost its foothold, and (2) we will never be able to fully assess what actually happened.

  Rather, the SOC must understand how proposed countermeasures will impact their ability to assess the extent of the intrusion and how the adversary's actions might

change as a result. SOCs that have strong adversary engagement skills may actually enact a series of response measures designed to guide the adversary toward a desired goal, revealing additional details of the adversary's TTPs and motives.

- **Ensure the entire SOC is working toward the same goal.**
  In the heat of the moment, it is easy for members of the SOC to step beyond what they are authorized to do, considering their limited perspective on what needs to happen next. Telling a system owner to disconnect a system or shut off access could be disastrous, even if it seems like the right thing to do at the time. Coordination isn't just between the SOC and external parties—it starts internally, through both peer-to-peer collaboration and a clear command structure.
- **Don't be afraid to ask for help.**
  Not every SOC has all the skills and knowledge in-house to handle every intrusion. Incidents must be evaluated within the context of the mission and systems they impact—meaning the SOC must frequently reach out to system owners. Is an attack targeted at a specific business or geographic region? By talking to other partners, the SOC can find out more. Do we have the necessary skills to analyze a piece of malware? If not, another SOC or third party might provide reverse engineering expertise.

12.2 Incident Tracking

Every mature SOC needs a robust incident tracking capability. However, there is no one size fits all, meaning every SOC does it a little differently. In this section, we talk about key requirements and architectural options for incident tracking. We also discuss areas in which an incident tracking system (by itself) falls short, indicating the SOC should seek out additional forms of knowledge management.

The SOC's needs for incident tracking are not terribly different from general case ticketing and tracking used in general IT help desk and system administration. That said, the SOC has several key requirements, many of which are unique to CND:

- Allows consistent and complete information capture across incidents for each state of the incident life cycle—Tier 1 triage, Tier 2 analysis, response, closure, and reporting
- Is able to record both structured information from analysts (incident category, time reported), semi-structured data (impacted users, impacted systems) and non structured information (analyst narrative), along with time-stamped notes
- Is available to SOC personnel while protecting sensitive details from constituents, thereby avoiding compromise of any insider threat cases or word getting out about an incident prematurely or to the wrong parties
- Protects details about cases even if the general constituency is compromised

- Supports escalation and role-based access control for different sections within the SOC
- Supports long-term trending and metrics
- Can incorporate artifacts or pointers to artifacts, such as events or malware samples.

It's also important to note that as an alternative to calling the SOC or sending it an email, constituents could input information about suspected cyber incidents on a form on the SOC website. Although this information might automatically populate a case, submitters outside of a SOC should not have access to that information after it is submitted (unlike an IT trouble ticketing system). Many SOCs will choose to keep this form submission system separate from their internal case system for security purposes.

Unfortunately, there is no standard IT case management system used for CND. Usually, SOCs will adopt one approach from those listed in the Table 24. Let's look at the pros and cons of each potential approach to cybersecurity incident tracking.

Table 24. Case Tracking Approaches

Approach	Pros	Cons
Manually (on paper). Each case is tracked through a collection of hard-copy notes and artifacts.	Free Easy to set up and use Escalation is straightforward. Compromise of SOC systems does not compromise case data.	Can be slow. Paper copies can be lost. Large amounts of paper accumulate over time. Lack of structured forms can lead to inconsistent tracking, especially over time. Very "19th century" Trending or metrics are manual.
Manually (in soft copy). The same as hardcopy, but artifacts are left on a network share.	Startup is relatively straightforward, assuming SOC already has a file share.	Nearly as haphazard as hardcopy Lack of structured forms can lead to inconsistencies over time. Trending or metrics are manual. Short of changing directory and file permissions to each case, loss or compromise of data is possible.
Existing IT case management system	Acquisition and O&M free to the SOC. Reporting and metrics possible. Seamless escalation of cases from/to IT help desk	Unlikely to be flexible to SOC needs. Sensitive data is comingled with general IT help tickets. Ticketing sysadmins, power users can see SOC's cases; very high likelihood of compromise of internal threat cases. If general constituency systems are compromised, it is fair to assume the adversary can see SOC cases. Incorporating case artifacts may be a challenge.

Table 24. Case Tracking Approaches

Approach	Pros	Cons
SOC instance of COTS IT case management system	System comes with polished feature set, documented setup, and central administration. Robust reporting and metrics possible Case details available only to parties designated by SOC	Usually very expensive Customization to SOC needs might be a challenge. Incorporating case artifacts may be a challenge.
SOC instance of FOSS IT case management system	Depending on tool chosen, system comes with polished feature set, documented setup, and central administration. Very flexible Free to acquire Reporting and metrics possible Case details available only to parties designated by SOC	General IT case tracking system will require nontrivial customization to fit CND use cases; not "turnkey." O&M customization will likely require staff with some experience in scripting, programming, or databases.
Custom-built ticketing system	Extremely flexible Reporting and metrics possible Case details available only to parties designated by SOC	Expensive to acquire and O&M SOC must build system from scratch, requiring staff with extensive experience with programming and databases. Development of system may take a while, since SOC must start from scratch.
SIEM case tracking system	Free if SOC owns a SIEM System is specifically built for tracking security incidents. System leverages user groups and permissions setup for other SIEM tasks. Users can attach events and some artifacts to tickets. Escalation paths are useful if SOC leverages an event-driven workflow and correlation rules. Reporting and metrics possible	Extremely expensive if SOC does not own a SIEM Limited to no flexibility, depending on SIEM product If SIEM goes down, nearly all aspects of SOC operations (triage, analysis, case tracking) are kaput.

There are a number of issues to consider here. Some SOCs will get started with a manual hardcopy or softcopy case management system, but as we can imagine, this will not last for very long. Leveraging an existing IT help desk ticketing system may also seem appealing, but the SOC has a specific set of needs and sensitivities. As such, that option isn't very appealing either. A few SOCs have been known to build their own custom

ticketing system from scratch, but only when requirements and customized use cases support the resulting expense, as is sometimes the case in large, tiered, and coordinating SOCs. There may be good examples where case-by-case access controls are needed, such as with a SOC that has as strong law enforcement or insider threat mission need.

On the basis of the pros and cons, many mature SOCs choose to leverage their own customized instance of a FOSS ticketing system. Request Tracker (RT) has been openly customized for use by SOCs [284], making it an appealing option. If the SOC chooses to implement or customize its own ticketing system, there are a number of existing examples of incident tracking forms found in Section 3.7.5 of [3].

That said, best-of-breed SIEMs have complex correlation capabilities. With these they can automatically generate cases prepopulated with key information. This is commonly used for cut-and-dried incidents like AV hits. Implementing automatic case generation for these use cases can save Tier 1 and Tier 2 a lot of time, but may be contingent on using the SIEM's ticketing system. One alternative is to have the SIEM automatically send event details in a scripted action to a customized FOSS ticketing system. The critical decision here is where the SOC chooses to bring the analysts' workflow out of the SIEM and into a third-party ticketing system.

As mentioned in Section 11, it's also important to recognize that not everything a SOC needs to track over time may be contained in case notes. For instance, the SOC will likely want to build a knowledge base that is system-, adversary-, or TTP-focused, rather than case-focused. Some SIEMs have internal knowledge base features, but such functionality tends to be limited in its customizability. For more information on cyber threat knowledge management, see Section 11.