Secureworks®

WHITE PAPER

Incident Response: Lessons Learned Template

Introduction

The lessons learned process may be one of the most important phases of the incident response lifecycle (Figure 1) as it allows the organization an opportunity to identify and understand the causes that contributed to a cybersecurity incident. By identifying the causes, the organization is afforded the ability to act on any areas for improvement, both technical and non-technical, which reduces the risk of a repeat occurrence.

This document is intended to shed some light on the process that the Secureworks® Incident Response Team utilizes when working with our clients to plan and facilitate a lessons learned events, and imperatives that can be gleaned from that to ensure a successful outcome.

While the process goes by many different names (e.g., post-mortem, lessons learned, incident debrief), there is no one perfect recipe to conduct post-incident activities as each incident and organization is unique; what works for one organization with a specific incident type may not be ideal for another situation. Because lessons learned events are not one-size-fits-all, ample planning from an experienced incident response consulting team helps to drive success from these events and ensure that the recommendations that stem from such an event are relevant, comprehensive, unbiased, and properly explore the entirety of the incident.

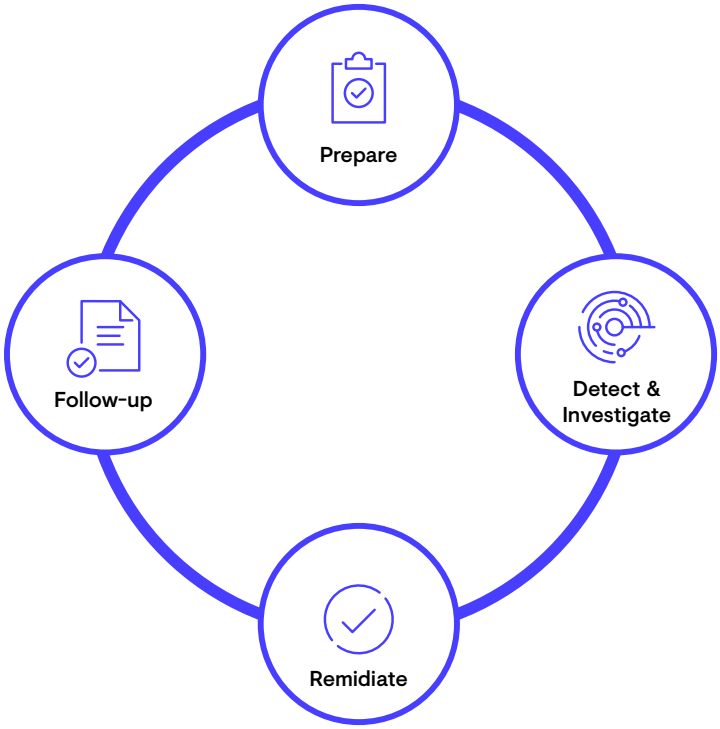

Figure 1. Secureworks Incident Response Life Cycle

Pre-Engagement Planning

While each lessons learned event has some variation, several steps are commonly leveraged in order to ensure a successful outcome.

1. Executive Sponsorship

As with most critical initiatives, an executive sponsor must be secured at the onset of the engagement. The sponsorship will ensure that the initiative is prioritized against competing tasks and gives credence to the activities. Perhaps most importantly, the executive sponsor will communicate to any stakeholders that the lessons learned process is of importance to the organization and is not an attempt to assign blame. The goal of the lessons learned process is not to assign individual blame. It is a natural human emotion to be defensive when actions are examined after a cybersecurity incident. To mitigate this emotion, the executive sponsor must have the authority to create a culture of psychological safety to enable the rewards from failing to be explored, identified, and realized. Assurance from an executive sponsor will help facilitate an atmosphere of openness to examine the factors surrounding the incident collectively and holistically.

2. Timing

Depending on the cybersecurity incident faced by the organization, staff is likely to be fatigued and will want to "move on" from being preoccupied with the incident. If the cybersecurity incident dragged on for days, or even weeks or months, staff may be both physically and emotionally taxed. Because of the potential lack of desire to revisit a stressful epoch, there may be a desire to push a lessons learned event out several weeks.

While there is never a perfect time to conduct such an exercise, the organization should aim, at a minimum, to conduct the lessons learned exercise as soon as possible after the conclusion of the cybersecurity incident.

3. Data Collection

In an effort to determine the scope of the lessons learned engagement, the lessons learned coordinator may request a variety of documentation from the organization, including incident response plans, incident reports, and other artifacts. Some of this information may be within the customer's organization, while other artifacts may reside with outside partners (e.g., Secureworks).

Assurance from an executive sponsor will help facilitate an atmosphere of openness to examine the factors surrounding the incident.

4. Stakeholder Identification

Because engagements may involve dozens of personnel, some of which may be external to the organization, Secureworks will identify stakeholders that participated in the response. This may consist of technical and cross-functional personnel that had both major and minor roles in the response. Identifying these stakeholders from the onset enables Secureworks to identify those with key information relating to the planning and overall response. It may be necessary to conduct interviews with said stakeholders.

The goal of the lessons learned process is not to assign individual blame.

5. Unique Engagement Considerations

Lessons learned events are unique consulting engagements that come with its own set of potential sensitivities. This may include ensuring that efforts are compartmentalized with specific stakeholders or defining the involvement of counsel to ensure privilege is maintained. Secureworks will work with the project points of contact to determine specific processes for document labeling and work product dissemination.

Lessons Learned Formats

Based on the Pre-Engagement Planning steps, Secureworks may conduct individual or small-party interviews of key stakeholders. Group discussions may also be considered.

Interviews

The purpose of the interview is to gather qualitative feedback on the incident response process and ensure stakeholders have a forum to elaborate on their observations above and beyond what may be contained within existing documentation. Often, these interviews are an hour long and, based on findings, may occasionally require a follow-up session. Questions will be focused on the incident itself as well as historical factors that may have enabled the event to occur.

While some customer points of contact will desire to join each interview, Secureworks suggests to have only the interviewees participate in the session. Having additional parties may discourage interviewees from providing candid responses to questions, thus limiting the feedback, providing an incomplete picture of the environment or incident.

Group Discussions

Depending on the customer environment, a group discussion may take place with select stakeholders. This may enable feedback to be gathered in a more expeditious fashion with Secureworks functioning as the facilitator of the discussion.

Interview Questions

Due to the fluid nature of stakeholder interviews, no interview will contain the same set of questions. However, common questions that may be asked during interviews include:

- Exactly what happened, and at what times?
- How well did staff and management respond and participate in the handling of the incident?
- Were the documented procedures followed? Were the procedures adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations be improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- Which stakeholders should have been engaged in the process that weren't or or which stakeholders should be engaged sooner?

Output and Outcomes

As with the lessons learned process, the final deliverable is not static. Depending on the status of the engagement and organizational sensitivities, we are able to provide a report and/or a verbal debrief. Optionally, Secureworks may present an onsite executive briefing. The report will examine the incident and segregate recommendations into three groups: People, Process, and Technology. If necessary, organizational sensitivities will be considered during the engagement planning phase to ensure that written materials are appropriately limited.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp