The WithSecure™ guide to rainbow teaming

Gold team

Building resilience through crisis management rehearsal

A WithSecure™ Consulting whitepaper

WITH secure

WithSecure™ consulting

WithSecure™ Consulting is a research-led cyber security consultancy, partnering with enterprises and early adopters worldwide. We exist to build resilience in an ever-changing digital world by providing evidence-based security advice. Our research drives service innovation, pushing the industry forward.

We're a multi-disciplinary team, equally intellectually curious and passionate about security. It's this that compels us to solve the world's most complex security challenges.

www.withsecure.com/consulting

Contents

Introduction to rainbow teaming 4
Gold teaming background 6
Walkthrough 7
Phase 0: Project initiation 7
Phase 1: Technical simulation 10
Phase 2: Executive simulation 12
Phase 4: Debrief and report 13
Summary of outcomes and conclusion 15

This paper:

Driven by industry advancement in recent years, there is now a broader range of initiatives available to support the development of an organization's cyber security posture across the Predict, Prevent, Detect, and Respond (PPDR) model. Combined, these are colloquially referred to as a "Rainbow Team", delivering purple (collaborative), blue (defensive), red (offensive), and gold (crisis management) activities. When delivered sequentially and continuously, organizations gain the ability to utilize outputs from each development area and measure incremental improvement.

Each paper in this four-part series explores one such testing approach through the eyes of the teams – external and internal – leading and participating in the engagement. The aim: to demonstrate how the practical and technical delivery processes lead to real-world impact. For readers who have taken part in similar testing activities already, the series will help explain how to boost the benefits of that pre-existing investment.

The sequencing of rainbow teaming activities depends on the security testing and implementation your organization has carried out, and the experience of your security staff and senior security stakeholders.

Practice and develop the business-wide response to a cyber incident through impact mitigation

Background

Nothing quite sharpens the executive mind like an ongoing cyber security breach, and a threat so severe to the organization its survival might be in jeopardy. Situations like this often require an organization to suspend normal rules of operation to handle the elevated threat developing in real time. Many of the skills required for its security staff involve rapid processing of unusual and unfamiliar information, before disseminating this to a non-technical executive, along with potential implications and actions for them to decide from.

Organizations' decision making and communication channels are often poorly prepared for day-to-day operations whilst under sustained attack.

Thus, designing and rehearsing Crisis Management Team (CMT) strategies makes all the difference in effectively dealing with a live incident and supporting other teams combatting the threat directly.

There should be company-wide knowledge of the key critical assets to safeguard in the case of a live attack, to ensure everyone understands their role in protecting them. In addition, recovery plans need to be in place should critical assets, which are essential to business continuity, need to be restaged.

A poorly-managed incident can have a devastating impact on an organization, way beyond its Security Operations Center (SOC) and IT team. Being able to communicate externally upon request, preemptively managing internal and external communication, and knowing when to inform regulators are key areas requiring practice in order to mitigate reputational damage, during and after a crisis.

The rehearsal of this situation is known as a Crisis Management Exercise (CME) or gold team exercise, and is delivered by a team of external practitioners, with knowledge across incident response, management, and risk. Though still technical at its core, gold teaming aims to present an executive – rather than purely technical – team with the issues, considerations, and decisions serious enough to justify escalation of a cyber security incident to their level. It helps those two, often disparate teams, practice communications and collaboration, so managing the fallout of said incident becomes the duty of all affected, and is dealt with effectively. As such, gold team exercises play a vital role in the rainbow teaming activities of large, global enterprises with complex infrastructures of people.

Walkthrough

The following walkthrough depicts a crisis management exercise. For the purposes of this paper, we'll use a fictional client, Acme Bank. And to provide a true-to-life demonstration, we will base the walkthrough on the recent real-world engagements of our own consultants.

Phase 0: Project initiation

Acme Bank is a large financial enterprise, with a global presence and over 30,000 employees. This includes a dedicated security team and a 24/7 security operations center. It has invested in standard security hygiene, as well as improving detection and response capabilities against well-known attack techniques via purple teaming activity executed 12 months prior.

The organization has been observing recent attacks on competitors and the consequent fallout. It now wishes to run a Crisis Management Exercise to gauge and improve its own ability to withstand a persistent, intelligent threat. This will enable staff to practice:

- Making challenging decisions to reduce long-term risk during active incidents
- Executing their individual roles and responsibilities under stress
- Containing crisis from internal and public relations perspectives
- Using CMT communication channels currently in place
- Delivering recovery activities in the incident aftermath

CMEs can be targeted at different organizational areas, from board level to the technical team, and at different processes. At the project initiation stage, these, plus the validation of Acme Bank's fitness for various severity levels of engagement are defined collaboratively with WithSecure™'s CME facilitators. This takes place by designing a scenario around the following factors:

Recent incidents experienced by competitors

One of Acme Bank's closest competitors was attacked by the threat actor group FIN7 around 18 months ago. The breach resulted in 1.5m being stolen, and the data of thousands of customers made public. The bank's ability to recover from the incident has been slow, and many customers have switched to competitors such as Acme Bank.

Whether to involve the media

WithSecure™ consultants will assume several roles during the engagement to make it more realistic. Media requests to comment and conversations on social media can rapidly amplify rumors, so WithSecure™ advises Acme Bank to include the external comms component in the exercise.

Whether to run an executive simulation, technical simulation, or both

As with blue team engagements, a mixed, technical and non-technical CME is possible. One downside of this approach, especially if the teams are unused to working together, is that an overload of information can leave one side feeling more engaged than the other. An exercise targeted at the leadership team, for example, will have a broad scope that touches all areas of an organization's operation. Conversely, the activities of technical stakeholders during the same crisis are likely to be hands on, narrower in focus, with information being communicated upwards in the management chain. As those separate teams develop greater confidence in their own individual area, so too does the ease with which they can co-participate in engagements

Whether an outcome of success or failure will be most worthwhile for learning

The objective of the exercise is to test the participants and processes in scope through rigorous stress. Simulations can be run across a scale of complexity, making them easier or harder to dynamically respond to as the narrative unfolds. If the participants feel the odds against them are impossible to overcome, however, they are unlikely to react in a realistic manner. Instead, an exercise that opens at a comfortable level before increasing in difficulty allows them to recognize some success, before identifying the points at which their crisis organization breaks down – a vital indicator of where to improve. Depending on the sophistication of those participants, a successful conclusion to the exercise is necessary to demonstrate recent improvements are effective and to raise morale.

After planning that includes interviews with the leadership team to find out more about the organization's past responses in crisis, the following engagement is agreed upon:

Setup

A half-day technical simulation, followed by a half-day cross-team simulation. The technical simulation will focus again on Acme Bank's CSIRT, the team responsible for responding to cyber security incidents, giving them an opportunity to develop their skills in the context of the wider organization. The second simulation will require the participation of Acme Bank's leadership team to guide the organization through the unfolding crisis. These participants will include members of the existing CMT. Numbers are limited to those who would receive information coming up the chain, such as the COO, head of communications, and so on.

Scenario

An area of concern highlighted by Acme Bank during the preparation of the exercise is communication generally between the technical security team and the bank's executive stakeholders. The exercise will be considered a success if information provided to the leadership team helps them accurately understand the immediate threats and risks involved, allowing them to make fully-informed decisions.

The scenario will reveal the initial breach vector relied in part on a legacy external payments interface, the decommissioning of which has been delayed multiple times over the last two years.

Phase 2: Technical simulation

10:00 - Simulation

The simulation kicks off with an introduction from the WithSecure™ consultants facilitating the exercise. Present are all Acme Bank participants. The introduction includes:

A reminder of the exercise objectives

To test the people and processes that deal with CMT, the availability of processes to the participants, and the participants' knowledge of them.

A run-through of the agenda

Two parts – technical first, non-technical second – with a short break.

Roles and responsibilities of Acme Bank participants and WithSecure™ facilitators

Each participant plays their own role. The WithSecure™ facilitators will guide them through the scenario, answer any questions, and clarify any misunderstandings where appropriate. They will also roleplay absent stakeholders and external third parties to provide missing pieces of information.

Rules of engagement

In order to mimic a real incident, a set of instant messaging services is made available for the participants to use as they wish: from organization and tracking tasks, to sending updates to the different teams involved in the simulation.

Exercise instructions

The facilitators stress that as an exercise, the simulation will not be used to expose and penalize individual participants; the entire engagement is designed to be objective and non-judgmental. Participants are instructed to listen to one another, and, with the simulation starting shortly, to immerse themselves in their role and the scenario.

10:30 - Simulation phase 1

The technical participants are the first to be taken into the simulation room. This is a large meeting room at Acme Bank's office, used when managing operational incidents. This is where they would meet during a real crisis. Participants are seated, each with their own access to information channels, including Slack, the instant messaging service. A whiteboard is also available for the participants to use as they please.

The simulation begins with an overview of the scenario:

A member of the Security Operation Center (SOC) is contacted by an external authority. The authority signals that traffic originating from Acme Bank is beaconing to a known malicious command and control (C2) channel.

An initial investigation confirms the existence of the traffic but cannot identify a legitimate reason for it.

The authority informs Acme Bank that, after extending their investigation, it is believed they have identified the threat actor group involved: FIN7, which is known for the destructive actions performed against target financial organizations.

Acme Bank's own internal investigation reveals several malicious indicators they suspect are related to the group:

- Several workstations are communicating with each other via SMB traffic (Port 445)
- Event Logs are showing several Base64 encoded PowerShell events
- Network logs have shown a significant spike in data traversing the firewall

Phase 1 simulation activity begins with the participants being asked to demonstrate their investigative abilities by answering the following:

- How did the breach occur?
- When did the breach occur?
- How do we recover and remediate the breach?

WithSecure™'s facilitators guide participants through the exercise. Timing is controlled throughout, and the sequence of events unfolds at strategic points to progress through the scenario. At times, facilitators assume the roles of Acme Bank employees aware of, and impacted by, the incident. Prompts, also known as "injects", are sent to participants via the simulation Slack channel to demonstrate appropriate actions. The actions the participants take will affect the subsequent prompts from the facilitators.

At 12:30 the participants and facilitators leave for a 30-minute break.

13:00 - Simulation phase 1 resumes

Before the simulation restarts, participants are reminded of the exercise objectives, as well as best practice for investigating and recording a compromise.

They are informed immediately after that a disagreement has arisen between the security and firewall teams regarding an instruction to block certain traffic. Since the details of the decision should have been noted down at the time it was taken, they are asked to settle the dispute using incident records. It emerges that the details of the decision were not documented at the time, leaving the dispute unresolved.

The next instructions request an overview of current investigation and containment workstreams, outstanding actions, and the outcomes of concluded tasks. This should be readily available from the team's incident management workflow, including:

- The active workstreams and the people holding responsibility for each
- The person responsible for keeping a clear view on the status of the overall incident
- The person prioritizing resource allocation for the various investigation and containment streams

The participants are further instructed to prepare a full situation report for Acme Bank's executive crisis management team, as the incident has been escalated to a critical level. First, the following questions are put forth for consideration:

- Is enough information recorded and available to proceed with drafting such a report, or does this need to be collected first?
- Who will be responsible for drafting the report, extracting the key points for leadership consideration, and presenting it to the executive team?

As they proceed with preparing the CMT situation report, an inject comes in the form of a new investigation finding, raised by the facilitators:

Investigators following the attackers' trail have discovered an intrusion into the bank's merchant payment services environment. Their activities seem to be focused on a legacy third party payments system still used by some merchants for bulk payment processing.

Participants are asked to consider the following:

- How does this impact the incident's severity and risk rating?
- What containment strategies might be effective? Do any of these require special authorization?
- How does this affect the team's prioritization of resources and efforts?
- Should any additional stakeholders be involved?

The decisions are logged, and the participants and facilitators take a short break

13:00 - Simulation phase 2

In the second phase of the exercise, participants from the executive team join from another meeting room. The exercise is now split, with technical stakeholders on one side, and the business and operational aspects of the incident on the other. The executive participants join this emerging situation at a higher level and will need to:

- Protect the future of the business and minimize the impact of this incident
- Continue the normal business functioning as best as possible
- Process the digested information emerging from their technical teams and other sources in order to drive appropriate decisions
- Driving and managing rapid, responsive external communication and external interactions during the crisis

The dedicated Slack messaging channel is now also used for the two teams to communicate decisions and actions as they occur. A slideware program is also set up to share injects with the executive participants.

As an introduction, the technical team is asked to brief the executives on the state of the investigation, based on the notes taken. Open and closed actions are discussed, and a high-level summary of the incident is given (enumerating the risk identified). Ten minutes are allowed for this exchange before the first inject focusing on the executive team is announced by the facilitator:

An increased number of employees are worried for their safety, and a rumor is spreading amongst them. One employee has reached out to their line manager, telling them they do not feel safe in the present working environment, and are worried about their personal data, as well as that of their clients.

Focus now shifts to internal and external communications, as well as their compliance to regulation. Based on the information shared by the technical team and with the investigation still ongoing, the heads of HR and comms are asked to put together their respective internal and external comms plans.

Inject: As the rumor of a compromise spreads, several journalists are reaching out for comment.

Participants are asked whether to ignore or respond to the request for comment. They work together to provide a statement by requesting key information from the CSIRT. This is then “sent” to the facilitators roleplaying the media.

The technical team advises that their current containment plan calls for disconnecting two key systems from the network for approximately two to four hours. Though this will cause some disruption to one client-facing service, it is considered the best course of action given the information available. The final request for a decision is escalated to the executive team, since client services will be impacted:

- Does the disruption request contain enough information on reasoning and impacts to enable your decision? Were alternatives considered and proposed?
- What impact will this have on the bank’s public image and reputation, given the rumors of compromise already circulating?

At 15:30, the participants take a 30-minute break before regrouping for a debrief.

Phase 4: debrief and report

At 16:00, all participants are present at the debrief led by the same WithSecure™ facilitators. Exercise fatigue is a common eventuality in CMEs, so the session is kept high-level, focusing on immediate feedback to encourage participants' self-identification of issues that arose during the exercise. A survey is then run to collect more detailed, though still immediate, insight. The exercise is formally concluded, and the facilitators and participants leave the simulation room.

A week later, a separate more thorough debriefing takes place, face-to-face as per Acme Bank's request. This will form part of the final report, and consists of the following topics:

- How the situation unfolded
- The skill and outcome of decisions made
- Insufficient processes and procedures
- Further necessary preparation

The full simulation report focuses on key areas observed during the simulation:

Roles

A team that is organized and works systematically together is a key success factor during a cyber security incident. Unclear responsibilities and management can make it difficult to work effectively in high-stress situations. Ultimately, unclear roles and responsibilities can cause critical delays in analysis and actions to contain the damage during an incident.

Escalation and delegation

During an incident, the different teams and units of the organization and relevant vendors should concentrate on the core task of minimizing damage to the business and facilitating quick recovery. The team should ensure they avoid generating unnecessary bottlenecks with their own decisions and should work actively to remove other obstacles.

Communications

The importance of good and consistent communication is emphasized during an incident. Communication actions are needed to keep their own staff, suppliers and subcontractors, business partners, other stakeholders and the public informed. Good and timely communication reduces speculation and incoming information requests, releasing time and resources for other actions.

Situational view

Collecting and maintaining an accurate situational view is crucial during an incident. It consists of collecting all information that is relevant to know about the situation, what actions and decisions have been taken, and what the status of each action is.

Decision making

The team needs to be able to make decisions based upon partial information that may later be determined to be inaccurate. However, the decisions made should be based on the best available situational view of the emerging events.

Operational security

Operational security can be defined as the need to protect the work of the team and communications from further information leaks and disturbances. Good security practices consider the possibility that during an incident, the normal, internal communication channels (email, IM, etc.) may not be available or may not be trusted if an attacker has gained access to those systems too. Therefore, during an incident, many organizations use alternative tools for communication.

Recommendations are given for each section, with missing materials, such as processes or unclear paths of escalation, highlighted.

Summary of outcomes and conclusion

In the case of Acme Bank, a CME provided the organization with a rare insight into their resilience in a rapidly-changing, high-stakes crisis. Individuals and teams were challenged as they exercised a combination of pre-learnt and improvised ways of working to process information and respond to the situation.

The engagement exposed how interactions between technical and executive teams would likely occur in such situations, as well as the technical team's ability to rapidly summarize complex technical situations to non-technical stakeholders. Many participants were able to demonstrate their ability to interpret and process information, clearly escalating information up the management chain to the benefit of the executive team – and therefore, the business. Except for key information going unlogged, many actions were strategic and well planned.

A successful CME simulates the crisis of a cyber incident in a broader context, and facilitates an organization's journey through it, out of its comfort zone and into unknown challenges. This allows stakeholders to identify shortcomings for themselves, about themselves and the wider business.

Where an executive team is likely to include highperformance, failure-averse individuals, a CME helps them reconsider their readiness in a meaningful way. They can then improve their personal approach to response, build stronger legal protections to manage liability, and develop a proper understanding of how security investment (especially for prevention) would be spent.

A team equipped for crises can refer to experience from situations whilst also improvising. Where gold teams help build this, is by asking insightful questions that play into existing knowledge (from crisis management rehearsals around natural disaster, fire, terrorism, etc.), but also – most importantly – by highlighting unknowns. Preparation is key here. Instead of a rigid, catastrophefocused scenario that sets participants up for failure from the beginning, a good CME is open and flexible enough to steer them in a direction that uncovers and highlights strengths and weaknesses yet uncharted.

www.withsecure.com/consulting

WITH secure