Capturing the Expertise of Cybersecurity Incident Responders
Transcript

Part 1: Purpose, Approach, Experts, and Incidents

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute. We are a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a principle researcher at CERT working on operational resilience. I'm very pleased today to welcome one of my colleagues, Sam Perl, who is a member of CERT's Enterprise Threat and Vulnerability Management Team.

I'd also like to welcome Dr. Richard Young, who is a professor with Carnegie Mellon's Tepper School of Business. He and Sam have been doing some really interesting work together on a cognitive study on capturing the expertise of cybersecurity incident responders - those folks who are on the firing line dealing with incidents on a daily basis and have some pretty interesting results and findings from their work that we're going to be talking about.

So with no further ado, welcome to the podcast series, Sam. Glad to have you.

Sam Perl: Thank you, Julia. Glad to be here.

Julia Allen: And Rich, it's really very kind of you to join us today. I look forward to our conversation.

Rich Young: Oh, me too, Julia. Thank you.

Julia Allen: Alright. So Sam, why don't you get us started to lay a little foundation for our listeners? When you talk about a cognitive study of incident handling expertise, what does that mean and why did you decide to tackle this particular topic?

Sam Perl: Sure, Julia. So our basic meaning of the term cognition here is really the study of the human mind -- so the way that people think, the way that they learn, and really in particular for our topic today, the way that they make decisions.

So our study in particular focuses on experts. So that's people that have achieved the label of expert in their field, and we've actually encountered a lot of prior research on what it takes to become an expert. There's research on how to measure experts, how to recognize experts, and we've really borrowed from a lot of those existing methods to determine how to select our experts that we used in this study.

So really, I mean, we're focused specifically on how incident handling experts make their decisions. So we really wanted to observe the experts and identify what information the experts are looking for.

Julia Allen: And as you've formulated this study, Sam, what -- obviously you have some type of hypothesis or some type of desired outcome that you're shooting for. At the beginning of this, why did you decide to go down this particular path? What were you hoping to learn?

Sam Perl: I'll talk maybe a little bit about our purpose. So, like, our purpose was really to determine how the experts make the decisions, and then from that make the knowledge available to a much broader audience that might not be experts. So, one of the missions of my team, which is to develop incident handling teams and skills, was to really formalize the incident handling experts' knowledge into something that we could use to improve the materials that we have to train people.

Or also, frankly, we thought that if we could really get to a successful extraction and description of the expertise, other designers, like technology designers or developers, could also use the results to create new tools that might help both novices and experts; or to improve like existing tools that already are in use today.

Julia Allen: Great, great. So Rich, can you say a little bit about how you went about conducting the study and the time frame?

Rich Young: Sure, Julia. The study started back in 2012, at the suggestion of Rob Floodeen, who was the organizer of the recent FIRST Conference in Berlin, to conduct the study. Sam and I asked four cybersecurity team analysts who were experts, to decide how they would respond to three actual and recent incident reports. So we gave them real stuff to make a real decision about. And the three incident reports had to do with SSH-scan, malware attack, and also phishing -- so three different reports about three different things. And we interviewed them all separately, so they weren't hearing what the other was saying.

We also asked the experts to think out loud as they read these three incident reports -- so to say everything they read, everything, every thought that came to them, any problems they were having, we got it all, and we got it all tape-recorded as they spoke out loud. We transcribed the tapes, we coded the tapes, and also we asked the experts afterwards did they think that this exercise was realistic?

And we were giving them real incident reports and they were real experts and they all agreed, “Yeah, this was what they do on a daily basis.”
And so their spoken thoughts that we got were to give us a window into what information was important to them and also the process that they used to make their decisions. And we were hoping to discover if they shared the same process, the same schema, for making their decisions.

Julia Allen: And how did you pick the people and the incidents? I'm curious about that.

Rich Young: Well, I should let Sam answer that question, because I think he did more of the picking than I did.

Julia Allen: Okay, Sam?

Sam Perl: Yeah. So, I mentioned previously about some of the existing research on identifying experts, and we were very heavily on that. So generally the experts are somebody that's operating at a very high level, recognized by the peers in their group, that they're really outstanding performers in terms of make really high-quality decisions on a very regular basis.

There's been, other research -- varying theories on how many hours it takes in a particular study or practice in the domain in order to become an expert in that domain. But so we approached people that were already in the position of expert in our organization and in some partner organizations to find our experts. So we really could go to people that are already in

expert positions. And for the incident reports, we actually selected real samples of incident reports, which were sanitized. Because again, prior research found that if you use dummy incident reports, or not incident reports, but dummy reports and then put them in front of the experts, the experts are pretty good at sniffing out the problems that you didn't even know that you had in your information.

And that can really throw your study off, because then you're not studying what you thought you were studying any more. But -- so we selected real incident reports which came from a couple of different organizations as well, and we really culled them down to find a few different types of incident reports so that we weren't just testing the same report over and over again.

Part 2: Schemas, Mental Models, and Surprises

Julia Allen: Great, great. So Rich, when you were talking about the study and the time frame, you briefly mentioned the word schema. So when you talk about a schema, because I know that was pivotal in your research, what is that, and what is its specific role on this topic, incident handling?

Rich Young: So a schema is -- well, another name for a schema is a mental model -- so something in the experts' head they used to make their decisions. It's the knowledge that they have in their long-term memories that makes them expert. If they didn't have this schema, this model, this understanding of their job, they would not be experts. So when you give an expert a task, like we gave our experts, they activate this knowledge in their heads and they're able to use that to make their decisions. Now, novices don't have this knowledge, and consequently they can't make an expert decision.

So the function of the schema is to guide their expert search for information through these incident Reports that is key to making the right decision. And so when the experts get an incident report, they already know what type of information they need to look for in it. So it's like they've got a pattern, they've got a process that they go through, they know when information's missing from Reports -- that, "Oh, I need to get this information. It wasn't mentioned." And they also know how to find more specifics and where to go to get information that isn't there that should be there.

And not all the reports are complete. A lot of the reports leave out critical information that the expert needs in order to make a good decision. Expertise has been shown to be dependent on schemas and in just about every field of study, so accounting, physics, medicine, business. That's where I've done a lot of my research in the schemas or the knowledge that business people use to making good business decisions.

But anyway, for our cybersecurity experts, we found that all four of them use similar schemas. They were using -- they were searching for, the same kind of information. They commented on the same types of information in the three incident reports. It wasn't like they did a different process with every different incident report and it wasn't like each different expert did something different. No, they all pretty much shared this common understanding of what was important and what to look for and how to go about making their decision.

We also found that if they had (I might just add this), but they had not just one schema that they were using, but they actually all used two schemas. One, their first schema that got activated and that they were using to search for information, was a schema having to do with the attributes of the attack. Get ready, find out the specifics, certain types of specific information about each of the attacks.

The other schema that they used really drove their incident handling decisions. And that was more of an organizational type decision-making process. So that's in a nutshell what the schema is.

Julia Allen: Boy, that's really fascinating, and I don't want to scoop the next question I'm going to ask Sam, but it seems to me that capturing the schema or this mental model or process or framework -- pick your favorite term -- is really pivotal in helping a novice become an expert, wouldn't you say, Rich?

Rich Young: Oh, absolutely. And it's a great way to teach novices to become experts. I mean, this is improvement in other areas -- that if you can train novices up to the experts' schema, then you can get really quick expertise out of people that at least have a basic understanding -- they don't have the real expertise that you seek from the high-level folks.

Julia Allen: It makes a lot of sense. So Sam, that next mystery question. So what was, I mean, obviously you went in with certain ideas and hypothesis about what you might discover, but from yours, and if you wish to speak for Rich as well, what was or were the most surprising or interesting things you learned during the study? That's the fun of research, right?

Sam Perl: Right. Our particular interest going in was to just describe the schema. We wanted to find it. We thought that they had it. We, right, our hypothesis was that the experts in incident handling would have the schema, much like experts had this in other areas. And we found that they did and we really wanted to itemize it. And we did that too, right?

So great; everything was good, our hypothesis was proven. But some of the surprising things that we found was, when we took an incident report and when that incident report -- the sample actually matched what that expert was looking for in terms of their schema, as well as the order in which they were looking for it, all four of our experts ultimately reached the same incident handling decision. So they -- every single one of them reached the same conclusion.

But then, so when the report did match, so if the incident handling sample was more scattered and did not match what the experts were looking for, and also in the order that they were looking for it, even when that same report was presented to each one of them, probably two things happened. So first thing was they really struggled to find the information -- lot more than I expected that they would struggle to find it, because you just expect, you know, that if you're looking for something and it's there, they're going to be able to find it. But that was not always exactly the case. And then ultimately that resulted in they did not reach a consensus on the final decision.

So, I mean, I guess it turns out that actually is really consistent with experts in other fields, but just intuitively here, I mean, you'd think that if you put the right data in front of an expert, somewhat regardless of how it's presented, they're the expert and they're supposed to make sense out of it, right? I mean, that's what you expect. But it turns out that's not really the case. And really giving it to them in the right way can have a big influence on the consistency of the final decision that you get.

Julia Allen: Right. So what occurs to me is, if the data is sparse or if it has gaps, they're all using their particular maybe more detailed mental model or schema to try and fill those gaps and not necessarily filling them or drawing conclusions that match up, right? Because they really don't have the data on which to make those in a consistent way.

Rich Young: That's right. But they're still making the decisions, right?

Julia Allen: Right, right.

Rich Young: And it's interesting. This is Rich, by the way. And on one ticket they were really, they're really differed on what they decided. A couple of the, two, of the experts said, "Oh, no action needs to be taken." And one of the experts said even, "You've got to take down the attacker site." So it's a night and day difference, at least in terms of the malware ticket.

Julia Allen: Right. So, you can really see from your small sample set why incident handlers across the community or even across an organization have trouble getting consistent data that can be used to improve how they do business, right?

Part 3: Three Recommendations

Julia Allen: So speaking of that, Sam, based on what you learned and any thoughts you've had since, do you have some specific recommendations on how our listeners might be able to use what you and Rich learned to improve their own incident handling capabilities?

Sam Perl: Yes. So we came up with three recommendations and I'll just briefly go through them. But so the first one was provide people that are sending the incident report in with some kind of structured format that reflects the expert schema that we found. So, often in the incident handling world, our teams are worried about putting burden on the reporters because we think it's going to reduce the amount of information that they're going to supply to us. So we often just tell them, "Tell us whatever you saw or found, and then we'll analyze it and get back to you if we need to."

But I mean, based on what we found in our study, I mean, actually, if you do it that way, you're not likely to get something that would match up with the expert schema unless it was an expert that was making the report, which is often really not the case. So we advocate for using a structured format. And just that doesn't mean to use 100 questions for the reporter, "Tell me everything that you ever saw." It's just six total questions. But for those six, you really need to fill them in and not leave anything blank for the expert. So that was our first one.

The second thing is that, if you have -- this goes back to the point that you made earlier, Julia. If you have a junior analyst on your team, or expect that you want some of your analysts to become experts that aren't experts today, you can have them take information or reports that come in and try to put it into the expert schema, right?

So even if you can't impose some kind of reporting structure on your reporters, you can still transfer what they've given you into the expert schema before it gets to the expert. And this has a side benefit too, which gets back to the training aspect that you mentioned, when a novice or a junior trains with an expert schema, then they can become an expert faster than those that don't train with a schema, right?

Julia Allen: Right, that makes sense.

Sam Perl: Yeah. And then the third thing, and this is a little bit more technology focused, is that even for the senior analysts, the experts on the team, using some kind of schema to just assist, right, with the decision- making process has been shown in other fields to be very helpful in terms of establishing consistent decision- making using full information.

This could be very simple. Honestly, some people use a simple printout of the schema that they just have taped to the wall. And they say, "Okay, the information in front of me -- have I hit upon all of the criteria that I should've hit on? And am I comfortable that this is a decision that I'm ready to make?" -- Just formalizes that in their mind. But we actually think you can do a little better than that, and there's some technology Rich could talk about a little bit, where you actually have a little mobile app and you can say," Okay, for this criteria the answer is 'yes,' for this one it's 'no;' for this one it's 'no,' for this one it's 'no,' Therefore, my decision ultimately is, 'no,' we're not going to do anything about this." So you can really track some details.

Julia Allen: Right. So it's almost, I mean, would I be doing it, not doing it, a proper service to say it's almost like a checklist of sorts or something that gives them a sense that they've covered the bases?

Sam Perl: Yeah, it's absolutely a checklist, Julia -- and medical doctors use a checklist -- and all kinds of folks; plant operators use these checklists. And it's just because it's so easy for us, even if we're expert, to get distracted by what's going on and the specifics of the specific case. When we get, you go down deep into the details and we may not come back up again and really think about, "Well, have we looked at everything we need to?"

So it's just how human beings as experts make sure that they're doing the top -- operating at the highest level that they possibly can. It often gives you a record; gives you a record of what you've done and if there's improvement that you need to make on your mental model on your schema, then that becomes more apparent too, because you say, "Hey, I'm doing my checklist but I'm still not getting the kind of results I want. The outcomes I'm looking for -- maybe there's something wrong with my checklist. Maybe I need to improve my mental model, my schema." So you account for a different type of attack that's new or different situation within an organization. So, it can be very helpful, even to experts, to have this app at their disposal.

Julia Allen: Right. It occurs to me that you may even have a senior, senior analyst whose job it is, one of their day jobs, is to take a look at the shortcomings of the current app or the current checklist, and as you said, make improvements based on the experiences of their analysts, right?

Rich Young: I'll chime in here, Julia. So, I mean, what we're really talking about here is some sort of decision-making support system, right? To where —-

Julia Allen: Right.

Rich Young: -- when the expert is going through the details of a report and it making determinations based upon their experience and the schema that they have, you're just making a very small record of that decision. So when we say checklist, I mean, we're not talking about the traditional checklist that you think of when you say, "Do a security audit," right?

Julia Allen: Right, right.

Rich Young: We're talking about a checklist against the schema that the expert already has and already uses to make a decision and you're creating a record of that decision. And so what happens is when you get feedback later on in the process, which tends to happen in this domain, right, where you might handle an incident and then three months later you might get new information, which causes you to revisit the decision that you made three months ago, right? You can now look at the factors and the decision that you made against each of the pieces of criteria in order to make a decision in light of the new information.

Whereas if you weren't tracking any of that stuff in the past, you would have to recreate the decision before you could then incorporate the new information. Right. Does that make sense?

Julia Allen: Fantastic. It does, it does. Fantastic. Well, I hate to bring this to a close, but we're just about at time, and so I am going to wrap this up with us. But I have one last question for you, Sam, and then Rich, if you want to chime in.

Do you have some places where our listeners can learn more? I know when we were preparing for this podcast, you had a presentation that you had put together, but our -- so can you say a little bit about that and any other references?

Sam Perl: Yes, sure, absolutely. So we actually gave a presentation of our study, which also includes slides of all of the schemas that we found. So all of the criteria listed, how it was used by the experts, some comparison of the experts' final decisions against each other. And that's all available in the presentation that was given at the FIRST Conference for Incident Response in Berlin for 2015.

There's another resource which is, for those that are looking for a little bit more, which is -- Rich has written a book and the title is *How Audiences Decide*, and there's a lot of information on schemas and expertise in that book.

Julia Allen: Well, really, gentlemen, thank you both so much for your time and your preparation and for this great discussion. Let me thank you first, Sam, for bringing the work to my attention and for presenting such a compelling research study that we hope will have some legs as we go forward, so thank you.

Sam Perl: Sure thing. Thank you, Julia. It's exciting to be able to talk about it.

Julia Allen: And Rich, great to have you on the podcast series, and I look forward to learning more about your work.

Rich Young: Thank you, Julia. I'll tell you, it's been a real thrill to work on this project and also to work with Sam.