CYBRARY | FOR TEAMS

Maximizing Security Operations:

How to enhance your SOC's capability and maturity

PART 2:

SOC Architecture and Management

Q&A with SOC Expert, Chris Crowley

Q Is it more difficult/costly to manage a decentralized CSOC?

Decentralization is definitely more difficult. Distributing between multiple teams adds complexity that needs to be handled, usually through a combination of technology, process, and staff effort. It is likely also more costly. But, I don't have certain data on the cost comparison of centralized vs. decentralized.

Q Most companies are short staffed in their SOC operations because they are afraid to hire new people and train them. That's why there is some oversight in identifying any anomalies. Why do companies find it hard to hire new people and train them?

First, I think that the reason for "some oversight in identifying any anomalies" isn't primarily due to a shortage of staff. I'll come back to that.

To answer your question about it being hard "to hire new people and train them?" I'll say that most companies have an expectation for SOC staff that doesn't match the existing candidate pool. The expectations for background knowledge, experience, and capabilities don't match the career trajectories of available candidates. So, less experienced staff are hired into a SOC analyst position with an expectation that there was already knowledge to do that role. In reality, there's about 2-3 months of ramp up for any new staff into a SOC analyst role. The role is often perceived as challenging, unfair, and tedious. So, people are prone to leave it as soon as possible, creating a vacuum and desperate demand by organizations. That's the worst case. I know many SOCs that don't have that situation. As a generalization, they tend to either invest in their people, or retain people because the organization is the only business in the area that employs people with that skill set and there's some reason for the employees to stay in that geographic area.

Back on the topic of "some oversight in identifying any anomalies." I think this is a result of a combination of bad SOC architecture under-resourcing the SOC, or having excessive expectations which is effectively the same thing. The bad architecture is failing to engineer detections for use cases for business relevant detections as well as not implementing a hunting regime to drive adaptation and address adversary developments quickly. Under- resourcing is the expectation that a few people can completely monitor millions of events in a given period of time.

Why do "Entry Level" positions require 1-3 years of experience? Do you think there is an optimal amount of experience someone should have before applying for basic SOC positions?

This depends entirely on what the organization is willing to invest in the staff. The years of experience is in place to assure that the person will provide value immediately to the SOC team. People lacking experience often get in the way, or cause damage when making mistakes. “More trouble than he’s worth,” is the cliche. For every person hired, there’s a cost to the team of coordination, oversight, training, and team dynamics.

What are your thoughts on a cloud-based SOC for a small to medium size company? How would you enable this successfully?

I think this is an appropriate technology architecture for organizations of all sizes if the data sensitivity allows for it. I’d design, build, implement and operate a cloud based SOC in the same way I’d design, build, implement and operate a purely internal SOC. With the right technology and procedures around various technology selections. I’ve developed a Gantt chart to capture what that looks like. A summary is in the webpage here: https://montance.com/timeline/ and there’s a link to purchase the full Gantt chart. It’s sold on a sliding scale. I speak about this extensively in my https://soc-class.com look at the “upcoming classes” if you are interested in attending. It’s my three day answer to how to enable a SOC.

I’m wondering about the quality and capability of the tools … are those ever a challenge to effectiveness and efficiency in SOCs? Also, maybe even integration between different tools — is that ever a factor in the ‘Effective tool use’ category and/or ‘Skilled staff’?

Yes, tools vary greatly in effectiveness. Sometimes it’s the shortcoming of the tool, sometimes it is the shortcoming of the operator of the tool.

If you’re coming from a traditional SIEM-powered SOC and transition to an automated SOC by SOAR solutions, how does that impact SOC headcount (can people be replaced by effective SOAR) and what should we be doing about the freed up hours, if any?

If you have SOC staff who are sitting around trying to figure out what to do with all their free time after you implement a SOAR tool, I really do want to hear about it!

You can email me (chris hat montance dawt com). What's more likely to occur is the staff can take on more sophisticated use case engineering and hunting. (Being self-referential again, but look at my WWHF "Hunting by numbers" talk on developing a hunting program). I don't think the SOAR tool's intention is "making people redundant." If you have that as an objective, I think it can be partially accomplished. But the organization looking to do that probably doesn't have a training and development program or particularly skilled cybersecurity staff to begin with.

Companies are talking about SIEM killer XDR - Do we need SIEM systems in the future if we have a good XDR solution in place?

My approach to technology is that we need tools to do certain things. One part of the SOC is the synthesis of data from multiple sources to identify potentially unauthorized and unwanted events. If a tool does that, then it can be implemented for that purpose. SIEM Killer XDR sounds like a movie title and marketing intended to keep SOCs on the upgrade treadmill without addressing the real problem of cybersecurity operations. The real problem is in developing operational excellence, and selecting tools that are good fits for the process. The marketing trap is getting you to buy new products then you're stuck trying to figure out how to use the product.

Apart from monitoring IT infrastructure 24/7, how vigilant should SOC analysts be when considering monitoring Operational Technology (OT) environments?

In my opinion, OT environments are almost always more "mission critical" than IT environments. Do I want to keep the lights on, keep the manufacturing facility operational, keep the water filtration system providing safe water to drink? Yes. Yes, I do.

How can we detect ransomware in EDR if the ransomware is zero day?

This is not really a question related to SOCs and more about per-system defensive architecture. Zero days are exploits. Ransomware is the adversarial application of seizure of control through a monetization strategy to try to force payment of ransoms. Presumably, your question is: "after a host has been compromised but prior to complete encryption of all files, how do we intervene in the control of the system to stop the complete encryption of files?" In attempting automatic response to a compromised system, you would stop processes which are modifying many data files.

You would need to have something at the kernel, processor, or hard drive level which can't be affected by other kernel level drivers. When too many files are affected, the hard drive stops deploying those changes permanently.

When was the SOC Survey conducted (month/quarter) in 2020?

Wow. I had to go back in my archives and that was only a year ago! Originally, the plan was to begin in April, and end in October with a report release in November. I started working on it in February. The survey itself was open online from August 3rd through November 7th. The report was released in December.

MEET THE EXPERT:

Christopher Crowley

SOC Expert and Consultant, at Montance®, LLC

Chris's experience includes security operations, incident handling, mobile application and device assessment, network operations, software development, and security policy to name a few. He has instructed courses and spoken widely on key topics in cybersecurity over the last 15 years, and continues to share his expertise and thought leadership with audiences around the world.

Find Chris on LinkedIn

Resources to advance your skills:

On-demand recording: Part 1: The Role of a SOC

Free E-Book by MITRE: Ten Strategies of a World-Class Cybersecurity Operations Center

Video Series: Chris Crowley's SOC Survey Key Findings and Results

Cybrary SOC Analyst Career Path options for continued development:

SOC Analyst - Level 1 | SOC Analyst - Level 2 | SOC Analyst - Level 3