Grid's Physical Security

Conversation with POWER Engineers' Chris Ott

Physical security is crucial for energy and utilities companies to create a safe environment and prevent unauthorized access to people, property, and information. It is an ongoing concern for utilities, which must protect infrastructure from menacing physical attacks on power stations and other nefarious events.

Being watchful is essential but it is also important to keep costs down while being protective, as affordability is a key part of the regulatory environment. A new security tool takes aim at that.

Entering the energy lexicon is Meerkat™. Like the ever-vigilant mammal it is named after, Meerkat™ promises to objectively identify all avenues that could be used by a threat actor. In this conversation with POWER Engineer's Senior Security Engineer Chris Ott, you will learn all about it and more.

PUF's Steve Mitnick: Talk about your job and role in the industry.

Chris Ott: I am doing the absolute best I can to try to protect our power and critical infrastructure. Everybody needs power, and just about everyone is a ratepayer.

Nobody likes seeing their power rates go up, so if we're able to protect the grid without driving up costs, then it makes everybody happy that we are solving the security problem more efficiently.

PUF: You also have an interesting background. What should we know about that?

Chris Ott: I got started in the industry back in the late '90s. Before 9/11, I served in the United States Marine Corps as a power generation and distribution expert. Pre-war era, we were just out training and drilling.

I got good at my job. Then, after 9/11, we saw a massive influx of funding into the DOD. Because of my role at the time, I got voluntold, which was how things happened in the Marine Corps, to try and help on the backside with the war efforts.

What we were doing at that time was identifying critical infrastructure for foreign nation states, in this case Iraq and Afghanistan. At that time, early in the war, whatever we did, we had to ensure we were going to be able to help rebuild the community and the infrastructure.

If we had to send troops into a town or a city and knew there were a lot of bad actors, in some cases, we had to figure out how to neutralize their power grid. Whether that was temporary or permanent depended on whatever assets the military had available; boots on the ground or airborne assets.

I left the Marines in 2006. Toward the end of my career, I went back to college and got my electronic engineering degree.

I spent the next fourteen to fifteen years designing security systems, security mitigations, and protections for clients ranging from big tech to healthcare. It was a lot of different types of projects. Then, around 2011 or 2012, I jumped into designs for utility companies.

In 2013, I was hired onto a corporate security team for a utility in the Pacific Northwest. I worked on threat vulnerability assessments, subsequent mitigations, designs, and protections. In 2023, I joined POWER Engineers.

At an enterprise level, what every utility should do is create a risk profile for these facilities. Not every substation is built the same, and they all face different challenges.

PUF: What type of security are you talking about?

Chris Ott: I'm a physical security expert, so I've worked with things like card access systems, intrusion detection, and sensors used to monitor abnormal activities. I know enough about cybersecurity to talk at a high level about it, but I am not a cybersecurity expert. Those two areas overlap but are different skill sets.

PUF: There have been incidents involving physical security, but are threats increasing to substations and other critical parts of the grid?

Chris Ott: They are increasing. Prior to the 2013 incident in California where substations were shot at, most of the substation security events were break-ins or thefts, whether for copper or tools.

At that time, the chain-link fence was the standard. In some cases, it still is today, but it shocked the industry when the Metcalf substation incident occurred, resulting in changes to industry standards in 2014.

PUF: Isn't the real challenge that the grid is everywhere? What can be done?

Chris Ott: At an enterprise level, what every utility should do is create a risk profile for these facilities. Not every substation is built the same, and they all face different challenges.

For instance, when transmission or distribution substations go offline, the effects differ. In a distribution substation, a neighborhood or a couple of businesses might be lost. A transmission facility might lose an entire region.

These risk profiles must be built to then identify what the most expensive worst-case scenario is going to be and what can be done to prevent that. Is extra equipment on standby for quick replacement? What's the outage duration going to be?

Lost revenue must be considered. It's a bit of a challenge. A matrix must be created to identify the risks and the best financial

The worst-case scenario – I like calling it the Mission Impossible scenario – is where bad actors want to go in, do the absolute most damage possible, and don't care if they get caught.

ways of mitigating those risks, or to identify whether there is an acceptable level of risk that can go unmitigated.

PUF: Who are the threat actors?

Chris Ott: It's a wide array of bad actors. There are general thugs, like the ones in the Pacific Northwest, who wanted to take down the grid to rob a convenience store.

There are also anti-tech folks. There's a fairly good-sized community of them. A lot of those people were Ted Kaczynski sympathizers and followers.

Then there are foreign nation state actors; terrorists, whether domestic or foreign. Those are typically groups with external intents, who want to create damage and get away with whatever else they had planned.

The worst-case scenario – I like calling it the Mission Impossible scenario – is where bad actors want to go in, do the absolute most damage possible, and don't care if they get caught.

PUF: What are the latest innovations for the work you do with utilities and grid operators?

Chris Ott: One of the issues I found when I was working in my corporate security role was that the security experts would be brought into a build process late, sometimes at the sixty percent design mark or even later. That ends up being a more costly way of working. If the facility can be engineered with security in mind from the get-go, then it saves money through the entire process.

We recently launched a tool called Meerkat™ to help with that. Back in my time at corporate security, we would do threat and vulnerability assessments, but they were subjective. It would be my perspective or my colleague's perspective on what we thought would be the critical asset, or how I would attack it if I was a bad guy, or how my colleagues would attack it.

The regulatory bodies and auditors don't like that subjective approach. They want to know what all the avenues or threat vectors are and how they could be used to create damage.

We want to know what they are too, and how to help our clients go about mitigating those risks. We created this tool to objectively identify all the avenues that a bad actor could use.

PUF: You're calling it Meerkat™, why did you name it after that animal?

Chris Ott: They're very alert animals. They're very aware of their surroundings and they live in a community, so they're always looking out for each other. That's why we call it Meerkat™, because that's what we're trying to do is create awareness of the danger and protect the assets that serve our communities.

PUF: What does Meerkat™ look like and how does it work?

Chris Ott: It's another way of using a digital twin, but for security purposes. We gather a bunch of data and create a very accurate and realistic 3D model.

Once that model is created, in real time, we can go through and identify everywhere in the area of concern a bad actor might use for various activities, such as gathering intel, shooting, whatever. Then we start working through scenarios.

It allows us to simulate some different ideas and mitigations. We can track the cost in the tool, too, so once we have a baseline number, we can start working backward. We test ways to reduce this cost and still keep a high level of security.

Once we're all done, we give that model to the client along with a detailed report and the client takes it from there.

PUF: Was this hard to put together?

Chris Ott: We reached out to a handful of trusted clients that we've done business with for many years and had a good relationship with and said, "Hey, what keeps you awake at night from a security perspective?"

Then, we worked with our engineering team and our software writers and tried to create something that could help alleviate those concerns. It took a couple of different iterations. We did a handful of pilot projects with these clients, got some feedback so we could tweak it, tailor it, make it the best possible, and then we added to it from there.

PUF: Where does Meerkat™ go next?

Chris Ott: We just launched in February with version 2.0, the one we call Meerkat™. Before that, we called it the BLOS system, or the Ballistics Line of Sight survey system. Version two is where we're at right now, and on our roadmap, we have some clients who've indicated they would like to try and perform this in-house.

We're not there yet. We're trying to get to that point because security information is a big part of security. If you can control who has access to that information, then that provides a level of security in and of itself.

If the facility can be engineered with security in mind from the get-go, then it saves money through the entire process. We recently launched a tool called Meerkat™ to help with that.

PUF: What was the most rewarding part of this project?

Chris Ott: We did one project, and I can't use names and locations, but we saved one utility anywhere between ten million and twelve million dollars in mitigating risk by using this product-enabled service.

PUF: As an expert in physical security, what would you say to the readers?

Chris Ott: Look for more innovative things coming from us. We do free demonstrations of the tool and will be giving presentations and hosting displays at some upcoming conferences. If you're interested in what we're doing with this particular product or anything else, reach out. PUF