



Q: What is Meerkat™?

A: Meerkat™ is a data-driven, line-of-sight-based security analysis tool that can help substation owners and operators choose the most cost-effective and comprehensive solutions for their physical security system upgrade projects. It uses accurate data of the facility and surrounding terrain to produce a realistic 3D model that can be manipulated in real time to test assumptions about how effectively certain mitigation tactics will protect critical assets from ballistic threats. Supported by a team of industry experts, this tool can help you feel confident in choosing the security upgrades that are the best for your budget.

Q: Is Meerkat™ meant for planned, new or existing substations?

A: Meerkat™ can benefit any substation site, no matter the shape or size. For planned and new locations, the proposed substation layout can be synthesized into the tool and mitigations can be tested before the site has been constructed. For existing locations, high-quality data is collected to map out an accurate 3D model of the existing infrastructure and mitigations. That accurate model can then be manipulated in real time to show you whether your existing solutions can be used in more effective ways and help you determine where additional mitigations are most needed.

Q: Is Meerkat™ more expensive than traditional security analysis methods?

A: While the upfront investment of Meerkat™ is marginally higher than other traditional methods, our tool has the potential to provide significant cost-savings in other parts of your project. When involved early in the design and engineering phases of your project, Meerkat™ can minimize construction costs while maximizing security benefits. In addition to that, Meerkat™ can be categorized as capital expenditure, opening your operations and maintenance budgets for other applications. Another benefit of Meerkat™ is the amount of time it saves, allowing your teams to make informed and tested decisions in a matter of weeks rather than months.

Q: Is Meerkat™ more accurate than traditional security analysis methods?

A: POWER's patent-pending methodology uses high-quality, location-based data for every site. When publicly available data or pre-existing 3D models of the area are outdated or insufficient for our purposes, we collect our own high-fidelity data of the site. This ensures accurate analyses of your location, even in scenarios where there have been significant changes to the area. Because of this, our site-specific data is often more accurate than the publicly available data used in other methods of security analysis. The fact-based and data-driven results provided by Meerkat™ allow us to remove subjective opinions from security analysis and provide you with confidence in your chosen security solutions.

Q: Will I be able to run the Meerkat™ application on my own?

A: While this feature is on POWER's radar for the future development of this tool, for now our experts will need to remain connected to the project throughout the duration of the surveying, testing and analysis phases. In the meantime, you will have direct access to our industry-leading team of physical substation security experts, innovation leaders, visualization specialists and experienced engineers. They will be available to discuss operational concerns around mitigation designs before the final selections are chosen.

Q: Is the need for this solution compliance driven?

A: Meerkat™ was originally developed in response to NERC's Critical Infrastructure Protection standards. The goal was to help substation owners and operators find more accurate and efficient ways to protect their critical assets from malicious physical attackers. However, our clients are finding value beyond compliance requirements, gaining improved resiliency and significant overall cost savings on their security upgrade projects.

Q: Is Meerkat™ a standalone tool or can it be used alongside other industry-accepted security analysis methods?

A: It can do both! The NERC CIP-014 standard accepts many ways to conduct threat and vulnerability studies, and we kept them all in mind when designing Meerkat™. The collaborative nature of our tool allows a wide variety of inputs to weigh in throughout the lifecycle of the project, including those derived from other analysis methods! Meerkat™ can help you test solutions and explore alternatives.

Q: What are the deliverables for this effort?

A: POWER builds an accurate 3D model of the study area, captures relevant data that may be referenced during analyses and generates a comprehensive threat mitigation report. Once our involvement in the project ends, we relinquish ownership of all delivered materials, including the 3D model, to the client company and remove the data from our systems.

Q: What measures are in place to ensure the security and confidentiality of my data?

A: POWER exercises extreme caution when handling sensitive data. The last thing we want to do is provide a roadmap for bad actors to circumvent your mitigations. Once our involvement in the project ends, we relinquish ownership of all delivered materials to the client company and remove the data from our systems. Any information we share about security upgrade projects we've worked on is done with explicit permission from the client and is sanitized of any information that could compromise the security of their substations.

Q: What can I do to learn more about whether Meerkat™ is a viable option for my next project?

A: It's easy! Any entity that is interested in learning whether Meerkat™ is the right tool for their projects can request a free demonstration from our experts at meerkat.powereng.com. We are happy to answer any questions and provide our expert perspectives to help you take the next steps toward achieving your goals.