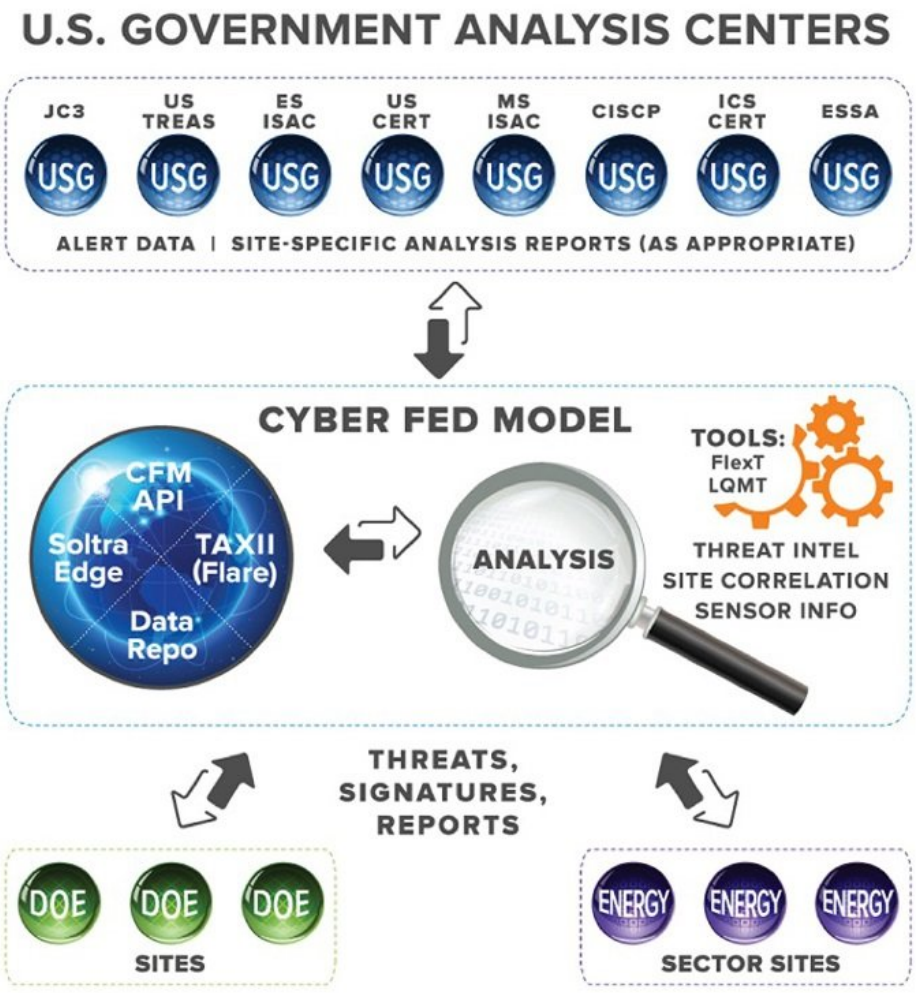
Detect locally, protect globally

January 19 2018, by Steve Koppes



Argonne's Cyber Fed Model routes cyberthreat indicators in near real-time and provides defensive measures and tools to simplify use of this information. Once a participating local system spots an attack, it can be rapidly shared to enable local damage mitigation and prevent its spread. Credit: Argonne National Laboratory

When infectious diseases strike, the World Health Organization acts swiftly, coordinating with the U.S. Centers for Disease Control and Prevention and its foreign counterparts to contain the threat. But there is no equivalent international organization similarly dedicated to identifying and mitigating a cyberattack.

The World Economic Forum (WEF), however, is bringing together infrastructure and technology developers, insurers and government officials from across the globe to develop strategies for responding to interconnected technological risks, including those that can cascade when hackers disrupt cyber-physical systems. Addressing these risks will be among the topics addressed at the WEF's Annual Meeting in Davos, Switzerland, from Jan. 23 to 26, 2018.

The U.S. Department of Energy's (DOE) Argonne National Laboratory is supporting this effort in two primary ways: (1) presentation of a simulated cyberattack, and (2) facilitated discussion of innovative ways to detect and protect against cyberthreats via machine-to-machine information-sharing techniques—the Cyber Fed Model.

Last September, Duane Verner, resilience analysis group leader in Argonne's Global Security Sciences division, presented a simulated cyberattack on the electric grid of "Big City USA." Verner was the keynote speaker of a WEF workshop in Zurich, Switzerland. The workshop met in connection with the WEF's initiative on Mitigating Risks in the Innovation Economy.

The first known cyberattack to effectively cause a power outage occurred on Dec. 23, 2015, when hundreds of thousands of homes in the Ukraine lost electricity after attackers covertly updated infrastructure with malicious software that rendered the power grid inoperable.

"To have a region without power for weeks on end, especially a region that is a major economic hub, would be catastrophic," Verner said. "Losses [would] potentially exceed hundreds of millions of dollars."

Insurance industry representatives at the September WEF workshop stated that the financial losses from the cyberattack could have global impacts. Furthermore, they may be uninsurable.

To address the threat of cyberattacks against physical infrastructure, Scott Pinkerton and his colleagues in Argonne's Global Security Sciences division began developing new ways to detect and protect against cyberthreats via machine-to-machine information-sharing techniques called Automated Indicator Sharing (AIS).

Scott Pinkerton, the Cyber Fed Model program manager at Argonne, made a keynote presentation last November during a workshop at the Siemens' Corporate Technology and Mobility headquarters in Munich, Germany. The Cyber Fed Model that Pinkerton and his colleagues have developed provides near-real-time local detection and global protection capabilities against cyberattacks. Credit: Argonne National Laboratory

By 2009, the Cyber Fed Model (CFM) for "local detection, global protection" had become operational. The model is a community-based system that disseminates cyberthreat indicators in near real-time and provides defensive measures and tools to simplify use of this information. This collective approach to cyberthreat intelligence reduces the cost of defense for members while increasing the cost of attack for hackers.

CFM was also the model the U.S. Department of Energy used in the development of Department-wide information-sharing policies and procedures, as required by the Cybersecurity Information Sharing Act of 2015. The Act was signed into law on Dec. 18, 2015 to improve the nation's cybersecurity through enhanced sharing of information related to cybersecurity threats.

In November, during a WEF workshop hosted by Siemens' Corporate Technology and Mobility at its headquarters in Munich, Pinkerton stressed the importance of rapidly sharing information about cyberthreats automatically. There is a big advantage in collaboration: Relying on humans to share details of a cyberattack can take months, while machines can be enabled to share detected threats in milliseconds. Once a participating local system spots an attack, it can be rapidly shared to enable local damage mitigation and prevent its spread.

The CFM framework can be adapted to fit other information-sharing formats as needed. "One size will not fit all," said Pinkerton, Argonne's CFM program manager. To ensure reliability, the CFM infrastructure was designed from the beginning to employ high-availability with geographically separated services.

"We are looking at how to defend ourselves in the here and now. This system is focused on providing operational benefits immediately," Pinkerton said.

Due in part to Argonne's success with CFM, the DOE leads the U.S. federal government in both intra-agency cyberthreat information-sharing, and in interagency information-sharing across the U.S. government and energy sector. In addition, the Cybersecurity Information Sharing Act went into effect in 2015 to make cyberthreat information-sharing easier among federal agencies and the private sector by implementing AIS capabilities. The DOE was the first agency to implement AIS capabilities using a system based on Argonne's Cyber Fed Model.

If widely adopted, perhaps even at the global level, the Cyber Fed Model might help ensure that the Big City USA scenario remains in the hypothetical realm. The Cyber Fed Model is part of the Cybersecurity Risk Information Sharing Program (CRISP), an innovative real-time, information-sharing capability that DOE's Office of Electricity Delivery and Energy Reliability (OE) developed by working directly with electric utilities. Using sensors on their IT networks, utilities share threat data in real-time with the CRISP program, which conducts state-of-the-art analyses using both unclassified and classified tools to identify threat patterns across the industry.

Provided by Argonne National Laboratory