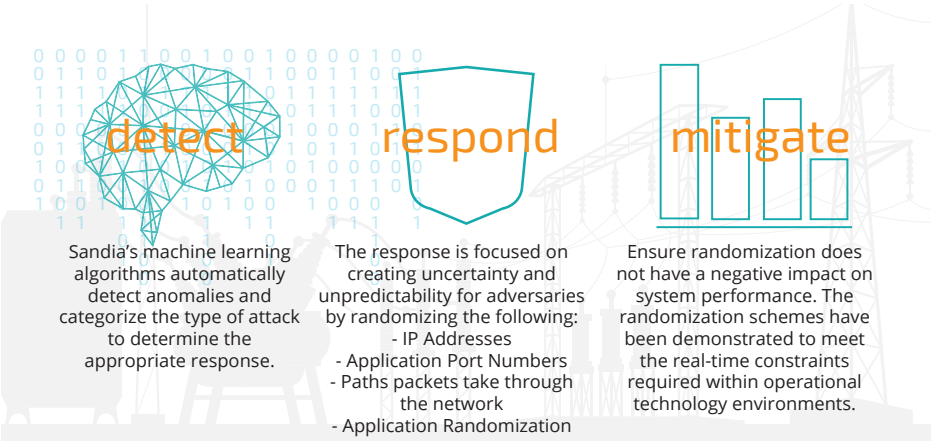
ADDSEC: ARTIFICIAL DIVERSITY & DEFENSE SECURITY

US Pat. No. 9,985,984
Technology Readiness Level: 6/7
Technology demonstrated in relevant environment

System that automatically detects and responds to threats within critical infrastructure environments in real-time

Networks and systems that monitor our grid or other critical infrastructure environments use predictable communications and static configurations, making them vulnerable to attack. Sandia researchers have developed a technology that automatically detects and responds to potential threats in under 1 millisecond—preventing an attack that can have a devastating impact on the nation's economy and public health and safety.



Sandia's detection approach is a set of machine learning algorithms that recognizes anomalous behavior and then subsequently classifies those anomalies into categories of attacks. Depending on the attack categorization, an appropriate response is activated to mitigate the detected threat. Our responses include several moving target defense strategies that modify the underlying environment so that the attack must be re-targeted by the adversary. The moving target defense strategies include randomizing Internet Protocol (IP) addresses, application port numbers, communication paths, and application library function locations. Our technology is being applied towards Industrial Control Systems (ICS), which requires real-time detection and response to maintain high levels of availability. For wide-scale industry adoption, our detection and response algorithms have been demonstrated to successfully inter-operate with several commercial and open source solutions currently available.

TECHNICAL BENEFITS

- Real-time detection and response to threats (under 1 millisecond)
- Automates network monitoring and surveillance
- Utilizes a "moving target defense" approach to improve security
- Proven on a representative industrial control system

INDUSTRIES & APPLICATIONS

- Any critical infrastructure environment such as utilities and power grid, finance, and telecommunications

ip.sandia.gov
ip@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2019-3525 M