2:15 p.m. – 2:45 p.m.
Cyberwarfare at the Speed of Light

Mr. Richard Cummings
Nuix

Description:
§ Cyberwar is now being waged on the endpoint
§ The modern defense-in-depth approach of stitching together multiple point solutions is too expensive and ineffective
§ The solution is to build the most effective capabilities from today s point solutions into a single platform focused on the endpoint
§ When capabilities are purpose-built to work together, automation accelerates detection, response, and remediation, giving network defenders the tools to hit back against attackers
Our presentation describes:
§ The problems and gaps in today s approach
§ Eight critical capabilities required for network defense
§ The role of automation in accelerating response
§ Key considerations in designing an endpoint solution
§ Possibilities that open up when big data processing capabilities meet highly structured data

Detail:
Agencies need the ability to counter insider threats by monitoring and detecting anomalous user behavior on an ever-expanding number of endpoint devices on networks around the globe. There must be a means for administrators and security personnel to automatically detect threats and investigate their root causes, by examining all relevant events that occurred prior to, during, and after any alert. It needs to be a proactive capability, in the sense that the solution must be able to identify potentially malicious behavior on its own. Should they choose, operators must also be able to conduct proactive searches across the enterprise, based on their evolving understanding of insider threats to the agency. These monitoring and investigative capabilities must include protections for the privacy of users who are faithfully executing the mission.

An adaptive security framework offers organizations a new approach to protecting themselves from all kinds of cybersecurity threats, including

malicious insiders. This approach helps organizations overcome today s major enterprise security challenges:

1. Perfect prevention is impossible
2. Protecting critical data requires accelerating detection and response
3. Having too many security tools drives up cost and risk
4. Trust is essential
5. Any solution must accommodate mobility

Nuix Insight Adaptive Security can provide the National Geospatial-Intelligence Agency (NGA) with enterprise-wide, near real-time insider threat detection, alerting, and investigation, without negatively impacting endpoint performance or end user experience (even in a bandwidth-constricted expeditionary environment).

Beyond detection and investigation, Nuix Insight Adaptive Security also offers capabilities to protect NGA s enterprise from insider threats. The platform can both interoperate with existing tools, such as the Host Based Security System (HBSS) in its current state and potentially replace HBSS with a single streamlined agent.