TechConnect Innovation Challenge and Defense TechConnect Chal

SAND2019-2058C

Submission Form

	Contact Information
First name:	**Vincent**
Last name:	**Urias**
Organization:	**Sandia National Laboratories**
Job title:	
Address:	**1515 Eubank Blvd SE**
City:	**Albuquerque**
State:	**NM**
ZIP:	**87123**
Country:	**USA**
Phone:	**(505) 284-5584**
Cell phone:	
E-mail:	**veuria@sandia.gov**
	Note: In addition to the contact information, the following information may be made available to conference attendees if organization is invited to participate in program. **Please do not include any confidential or proprietary information in your submissions details.**
	Organization Information
Company or Organization:	**Sandia National Laboratories**
Website URL:	**www.sandia.gov**
Organization size:	[ ] 1 - 19 [ ] 20 - 99 [ ] 100 - 499 [ ] 500 - 2499 [x] 2500 or more
	Technology Details
	List as you want printed in the program.
Technology/Solution Name:	**Cloud Hypervisor Forensics and Incident Response Platform (CHIRP)**
Brief Description of Technology in layman's terms:	**Cloud-based entities – cloud service providers (CSPs) and cloud customers – have not established foundational forensic capabilities that can help reduce cloud security risks. Our Cloud Forensics Platform provides analysts the ability to collect forensics artifacts in real-time about potential threats.**
	50 words max.
Technology Development Status:	[ ] Concept [x] Prototype [ ] Proven Manufacturability [ ] Ready to Market [ ] Commercial Product
Organization Type:	[x] Academic/Gov Lab [ ] Early-stage Startup (Seed) [ ] Mid-stage Startup (A or B) [ ] Commercial Startup (C+) [ ] Small to Medium Enterprise [ ] Corporation
Primary Application Area:	[ ] Materials, Chemical [ ] Electronics, Sensors, Communications [x] Cyber, AI, Data, Software [ ] Space, Defense, Mobility [ ] Energy, Efficiency, Resilience [ ] Water, Waste, Environmental [ ] Medical Devices [ ] Biotech, Pharma [ ] Manufacturing, Instrumentation

Secondary Application Areas: (select all that apply)	[ ] Materials, Chemical [ ] Electronics, Sensors, Communications [ ] Cyber, AI, Data, Software [x] Space, Defense, Mobility [ ] Energy, Efficiency, Resilience [ ] Water, Waste, Environmental [ ] Medical Devices [ ] Biotech, Pharma [ ] Manufacturing, Instrumentation [ ] Other
Other:	
	(if you selected Other above)
Technology Keywords:	**Cloud Forensics, Cloud Incidence Response; Digital Forensics**
	Enter up to 3 technology keywords separated by commas.
Market Keywords:	**Cybercrime Defense; Cloud Security**
	Enter up to 3 market keywords separated by commas.
Detailed Technology Summary:	**More than $1 trillion in IT spending will be affected by the shift to the Cloud during the next five years. This shift to Infrastructure-as-a-Service (IaaS) platforms has brought challenges to cyber Incident Response (IR) and forensic teams investigating not only breaches and leaks, but also cyber-crime, due to the ephemerality, location and ownership of the data, disks, and technology provided by Cloud Service Providers (CSP). Our Cloud Forensics Platform introduces a novel approach using Virtual Machine Introspection (VMI) to provide intelligence and forensic artifacts from active VMs in cloud systems. Each IaaS leverages a VM Monitor, or hypervisor, to service VMs in the Cloud. Most hypervisors do not expose a useful Application Programming Interface (API) to support customizable, contextual introspection, which is what an analyst needs to conduct an investigation. We have developed scalable VM instrumentation and introspection at an in-depth level that allows fast handling of events, as well as direct access to VM state (or memory), in a safe, stable fashion.**
	What is transformational about this technology? How is it different from existing technologies? What is the potential impact on industry, markets and society? 200 words max.
Value Proposition:	All IaaS clouds rely on hypervisors; we have developed a lightweight, deployable, hypervisor-agnostic (supporting KVM, VMware and Xen), Operating System (OS) agnostic (supporting Windows, Linux and Mac) tool that can be loaded to both on-premises and off-premises cloud environments – with simply the click of a mouse. It is a first of its kind advancement. It detects and can load itself into these environments without prior knowledge of the hypervisor or VM OS and begin collecting artifacts to support both IR and forensic analysis within seconds. Textual information, binary data (such as malware, files, images), network data (exfiltration), are pulled instantly from the system and stored in the platform to aid the analyst. Our technology provides new opportunities to meet these challenges in the Cloud through innovative VMI, including correlation with network data and active state collection. We provide defenders the ability to extract various forensic articles from a cloud system in real-time without affecting the guest and without guest detection, thereby allowing the defender to gain the advantage to capture an adversary's intentions, actions, tools and evidence.
	Why should a prospector or funder be interested in this technology? faster/lighter/stronger/cheaper/efficient, etc. 200 words max.
List any Vetted Programs/Awards your tech has been acknowledged	n/a
	i.e, ,Prize, Challenge, Accelerator, Award Programs. 50 words max.
Any Government Awards/Contracts (list agency, amount, award-date)**:**	**n/a**
	i.e, SBIR, OTA, Grants, etc. 50 words max.
Any External Funding to Date (non-Gov.)**:**	**n/a**
	VC, corporate, angel, grants, etc. 50 words max.

Market Strategy, Customers & Partners:	
	200 words max.
Please document top 3 executive team members and experience:	**Vincent Urias is a Principal Member of Technical Staff at Sandia National Laboratories, where he has spent the last twelve years conducting cyber security research and development. His research areas include cyber test-bedding, cyber modeling and simulation, as well as cyber analytics, cloud computing, and networking.** **William Stout is a Senior Member of Technical Staff at Sandia. His research interests include emulation platforms, network virtualization, software-defined networking, and cyber-security systems design and assessment. He holds a Master's in degree in Computer Engineering from the Air Force Institute of Technology.** **Caleb Loverro is a Principal Member of the Technical Staff at Sandia where he has worked as a reverse engineer in Cybersecurity since 2009. He holds a master's in Computer Science from the Naval Postgraduate School.**
	200 words max.
Would you like your tech to be considered for XXXXXX	[ ] Yes [ ] No