CHIRP Technology - Initial Business Case Analysis Questions:

Please review and answer the questions below if possible. You may find that many of the questions can be thoroughly answered via pre-existing documentation. *Please provide any supplemental documentation upon submission of this questionnaire. (specifications, market information, etc.)

Executive Summary Questions:

- What is CHIRP
    - Forensic and incident response tools have not evolved to combat advancing threats to Cloud security. In response, Sandia developed CHIRP: an innovative, lightweight, agentless Virtual Machine (VM) Introspection tool that transparently interacts with VMs to extract data for indicators of compromise, evidence collection and adversarial tools, techniques and procedures

- What are current technologies meeting similar or preexisting needs?

Public and private enterprises across the globe are turning to Cloud services for their information technology infrastructures due to the benefits it offers, such as lower operating costs, scalability, better collaboration, and flexibility. Gartner predicts that over the next five years, more than $1 trillion in IT spending will be affected by the shift to the Cloud, and that by 2020 most companies are expected to have Cloud-first or Cloud-only policies. The 2018 IDG Cloud Computing Study found that 73% of the organizations they surveyed had at least one application, or a portion of their computing infrastructure already in the Cloud, with an additional 17% planning to do so within the next 12 months. Rightscale's 2018 State of the Cloud report states that 81% of enterprises already have a multi-Cloud strategy in place, including both public and private Clouds spread across a multitude of service providers.

As more information passes through or is stored in the Cloud - e.g., valuable data about customers, transactions, research, product specifications, business intelligence, and other proprietary, sensitive, or classified informationCloud computing receives more attention from both amateur and sophisticated cyber adversaries.

Typically, Cloud Service Providers (CSP) implement baseline protections for their platforms and the data they process, such as authentication, access control, and encryption. But this is not enough, as cybercrime continues to plague public and private industry. The Center for Strategic and International Studies and McAfee estimate that cybercrime costs the world almost $600 billion, or 0.8% of the global gross domestic product. They further report that these costs will continue to increase due to the current low risk and high payoff of cybercrime, leaving law enforcement with the struggle to keep up with the technically complex and legally intricate crimes. As a result, few criminals are caught and prosecuted.

This paradigm shift has left cyber incident response and forensic teams with new challenges:

- Current defense and investigations tools and techniques do not directly translate to Cloud computing environments.
- The transient nature of the Cloud environment makes it much easier for attackers using virtual machines to mask their intrusions, copy or delete information, and erase all trace of their crimes.
- Any hardware associated with Cloud computing would not be owned, managed, accessible to, or located near defenders.

The complexity of Cloud environments and transitory nature of the attackers make Cloud-based cybercrimes difficult to detect and thwart during commission. Due to the lack of tools available to cyber analysts and investigators, these crimes often go uninvestigated and the malicious actors unpunished. So as the number of public, private, and government institutions moving valuable information to Cloud environments expands, the need for more sophisticated, platform-agnostic cyber defense tools increases.

Feature	CHIRP	Azure Security Center	Fortinet FortiAnalyzer-VM	VMware Guest Introspection	Magnet Axiom Cloud	LibVMI-Volatility
Installation Dependencies	Make	Proprietary	Proprietary VM	Proprietary *(vCenter)*	N/A *(third party)*	Cmake, libtool, yacc/bison, lex/ flex, glib, libvirt, libjson-c
Portability	Any system running supported hypervisors	Microsoft Azure Cloud	Service-based *(e.g., AWS Market Place)*	VDI, vSphere	Service-based	Off-line system
Hypervisor Support	KVM, Xen, ESXi	Hyper-V	Xen	ESXi	N/A	Xen, KVM
VM Support	Windows, Linux, OSX	Windows, Linux	N/A	Windows, Linux	N/A	Windows, Linux, OSX
Visibility	User, VM, Network	VM	VM	VM	User	VM
Requires User Credentials for Cloud	No	Yes	Yes	Yes	Yes *(Username, Password)*	VMI Only
Service	Deep introspection *(VM, IaaS)*	Log data *(IaaS, PaaS, SaaS)*	Log data *(IaaS, PaaS, SaaS)*	Agent-based introspection *(VM)*	Log data SaaS *(Apple, Google, FB, Microsoft, Dropbox, Twitter)*	Introspection/ Memory analysis *(VM)*
Guest Agent	No	Yes	Yes	Yes	N/A	No
Cost	No-cost govt. license; flat $995/server	Subscriptionbased per VM, *$0.02/hr*	Subscription: 0.10/hr *(AWS Market Place)*	vSphere/vCenter Subscription: $995-$4,395 per physical processor	$2871 *(add-ons + $1435 each)*	Open Source

Since CHIRP is a first-of-its-kind innovation with regard to leveraging VMI on Cloud-systems, there are no other products in the cyber security market that adequately compare to the CHIRP technology. Thus, similar digital-forensic and/or virtual machine introspection software applications and services have been used for comparison.

National Technology & 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-NA0003525

Each Infrastructure-as-a-Service (IaaS) Cloud platform leverages a VM Monitor, or a hypervisor, to provide memory and processor resources to 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

- What does success look like when this solution is deployed? (for the business, for the user)

Fast, easy-to-use, and undetectable forensic software is essential to combatting those who would steal, copy, modify, or corrupt Cloud-based materials, or use the Cloud for malicious operations. A secure Cloud presence demands the ability to confirm unauthorized access, gauge the nature of the attack and its goals, gather and preserve evidence towards eventual prosecution, and monitor the location for any further intrusion. CHIRP, developed at Sandia National Laboratory, gives cyber defenders these abilities.

CHIRP uses custom Virtual Monitor Introspection (VMI) via a Cloud hypervisor to provide digital-forensic capabilities—a first of its kind. Forensic artifacts are extracted from VMs in real-time without detection, allowing the defender to stealthily eavesdrop and capture adversary intentions, actions, and tools.

CHIRP works with a diverse set of hypervisors and operating systems, and is quickly deployed in on- and off-premises Clouds with simply the click of a mouse. Within seconds, it integrates into a Cloud environment, without prior knowledge of the hypervisor or VM operating system, and begins collecting artifacts for both incident responders and forensic analysts.

- In what scenarios will this solution be used?

By monitoring and collecting data via the hypervisor, CHIRP tackles four areas of previously un-addressed security concerns:

1. Rapid, forensically-sound processing of large data pools. Current forensic tools are simply unable to collect data from sometimes petabyte-large data pools stored in varied formats (e.g. Fiber Channel or Ethernet iSCSI), and Cloud services providers cannot afford to take the storage system offline to gather “forensically sound” evidence from the underlying file systems. CHIRP moves processing to the hypervisor to gather evidence from the file system, where input/output is quickly decoded, saved, and archived before being written to the underlying distributed file system.
2. The ephemerality of Cloud computing. A Cloud service provider’s ability to store all of a particular user’s information indefinitely is not economically feasible. As VMs are cleaned and re-imaged to regain needed resources, all forensic evidence is wiped away. Using the mapping knowledge inherent in IaaS Cloud platforms such as OpenStack and Amazon Web Services (AWS) EC2, CHIRP can use the hypervisor to conduct targeted collection of artifacts from running guests. CHIRP also makes it possible to retrieve information regarding file input and output, memory, processes, and network connections, as well as traceability of the actions on the system.
3. The elasticity of the collection methods and processing of the data. CHIRP addresses this concern by collecting data from multiple Cloud servers (hosts), capable of spanning various datacenter and geographic locations – fusing multiple sources with a common information model and custom naming convention. Every

host serving VMs with valuable information may be seamlessly added to a holistic view to contribute to the collection and processing of forensic artifacts.

4. Artifact provenance. Forensic collection and time correlation of the guest artifacts makes it hard to establish the provenance of artifacts. By collecting artifacts from the hypervisor, CHIRP allows all logs, accesses, and interactions created by the intruder

   to be verified and provides a forensic timeline of events that is grounded with a trusted time source can be created.

- How far do you want to forward this technology? i.e. establish working prototype, make product available to end user.
    - Make a product available to the end user

Product Specification Questions:

- Do you have documentation that will help to answer the following?
    - Fit? How does this technology integrate or mate with another part or assembly? Or business process?
        - N/A
    - Form? What is the size, weight and dimensions?
        - N/A
    - Function? What is the purpose of the part by how it should perform and operate?
        - N/A

Assumptions/Constraint Questions:

- What potential entities need to be established to advance? (admin, manufacturing, maintenance, support?)
    - Admin
    - Security operations
    - SEIM to collect data
- What potential restrictions, limitations to solution design, construction, testing, validation and deployment potentially exist? i.e. (regulation, license, IP, market conditions, etc.)
    - The organization must currently adoption of off prem and on-prem cloud

Requirement Questions:

- What are the 'must have' user requirements (i.e. features, functionality)
    - categories to consider (Reliability, Performance Efficiency, Operability, Security, Compatibility, Maintainability, Transferability)

- What are nice to have requirements that may not necessary be within the solution scope? (i.e. should have, could have, won't have)

- In what scenario(s) will this solution be deployed? (example: operator handheld scanners, distant monitors at entrances?)

Cost Summary Questions:

- What is the target market and size?
    - Medium to large companies that have moved to cloud.

- Who is the target end user(s)? (example: fire fighters)
    - Incident responders who have to defend cloud-based environments.

- What is the current direct material, labor, and manufacturing costs? This question may be difficult to answer but any cost documentation or a SME would be helpful. (i.e. bill of materials)
    - None, this is software.

- What are the estimated costs to consumer? Price points?
    - ~ $995/Server.

- What entities need to be established to achieve outcome (admin, legal, manufacturing, software vendor, etc.)
    - Software vendor
    - Support infrastructure
    - Company

- What is the expected shelf life of this solution?
    - Given the heterogeneity and cloud adoption ~9-12 year.

- What is the life of the project?
    - The project has been going on for ~ 8 years.

- Is there an expected salvage value? (if applicable)
    - N/A

- Is there a required rate of return or discount rate? (if applicable)
    - N/A

- What is the ideal payback period? (if applicable)
    - N/A

Benefit Questions:

- What are the basic benefit objectives? (increase revenue, reduce cost, increase market share,

- Decreased operational cost for doing IR/DF in the cloud.

- What are the non-financial objectives? (improve morale, increase flexibility to respond to change, improve customer satisfaction, reduce exposure to risk)
  - Increased visibility
  - Decreased risk to moving to the cloud

- What cost savings or efficiencies can be gained through the implementation of this solution?
  - Depending on the deployment 100x decreased in cost.

- What are indicators that can be tracked to measure effectiveness of solution? (help to define non-financial impact)
  - Incident trackability

Risk Questions: What risks are present for adoption of technology?

- Likelihood of adoption?
  - High

- What are the boundaries of the customer purchasing solution?
  - Current adoption and risk tolerance

TRL/MRL Questions:

- What is the TRL and MRL level?
  - 5-6

- Is there a technical data package? Bill of materials?
  - Yes

- Has there been a bench-top prototype made?
  - Yes

- If COTS products make up the bulk of the product, what is the IP that allows this to work?
  - NA

- What are the known competing technologies?
  - See figure above

- What is the current footprint? Can it be miniaturized?
  - It's a driver
  - No, it can't be miniaturized

- What is your (sponsor) vision of the form factor? Has any hardware been designed?
  - N/A

- How much will you involve yourself with technical commercialization?
    - As much as they will allow the team to

Stakeholder Questions: (we will likely need a few more meetings to ask a few clarifying questions with your SME's)

- What is the availability SME's?
    - Sponsor – N/A
    - Inventor – Has availability
    - Cost related – N/A
    - Regulatory related – N/A
    - COTS product supplier – N/A

- What is the process for contacting SME's for this technology?
    - Can we contact them directly?
        - Yes, Vince Urias veuria@sandia.gov (505) 284-5584