Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE®) Platform Security Overview

1. IDENTIFICATION

This white paper, Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE®) Platform Security Overview, has been prepared by Norwich University Applied Research Institutes (NUARI). No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from NUARI.

2. INTRODUCTION

2.1 Purpose

The purpose of this white paper is to provide an overview of the cyber security posture and considerations of the DECIDE® platform. **This document does not contain the sensitive and detailed security policy, procedures, and practices implemented by NUARI.** It is intended to convey the scope and commitment of NUARI efforts to offer a cybersecurity exercise platform that can be trusted to protect client /user data in a secure cloud computing environment.

2.2 Background

DECIDE® is an interactive, human-in-the-loop, decision-making-focused, fully distributed cyber-security exercise and assessment capability that engages all levels of an organization in decision-making within a cybersecurity risk framework. DECIDE® is an interactive simulation exercise platform for decision makers to test and improve coordinated response to cyber-attacks, kinetic events, and other technological disasters of natural or human origin within critical infrastructure sectors. DECIDE® uses interactive simulations to facilitate business model improvement in today's high-threat cyber space. This provides organizations and government agencies with a simulated environment for all functional staff (e.g., operations, legal, compliance, information technology, communications, et al.) to practice decision-making when dealing with cyber threats, and the analytical tools for senior leaders to see the potential impacts of those decisions.

As part of the DECIDE® development effort, an extensible architecture was designed and prototyped that supports the integration of systems, dependencies, and business model process flows from any number of interdependent critical infrastructure domains. This significant architectural enhancement has expanded the capability from an exclusive focus in the financial sector domain to all critical infrastructures, such as transportation, electric power utilities, oil & gas, and healthcare. This extensible architecture has been implemented into the current DECIDE® platform that supports the integration of

multiple critical infrastructures and is designed to provide a common set of services centered on an interactive, human-in-the-loop, business-model decision-making focused, and distributed cyber security exercise and assessment capability.

3. DECIDE® SECURITY OVERVIEW

3.1 DECIDE® Platform & Cloud Infrastructure Security

DECIDE® servers currently reside in Amazon Web Services (AWS). AWS provides secure infrastructure and services, while the customer is responsible for secure operating systems, platforms, and data. To ensure a secure infrastructure, AWS configures infrastructure components and provides services and features that can be used to enhance security, such as the Identity and Access Management (IAM) service, which can be used to manage users and user permissions in a subset of AWS services. The shared responsibility model for Amazon EC2 (DECIDE® servers for example), specifies that AWS manages the security of the following assets:

- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure

Consider AWS the owner of these assets for the purposes of Information Security Management System (ISMS) asset definition.

The AWS services used with DECIDE® are what AWS refers to as “Infrastructure Services”. This category includes compute services, such as Amazon EC2, and related services, such as Amazon Elastic Block Store (Amazon EBS) and Amazon Virtual Private Cloud (Amazon VPC). With these services, DECIDE® servers are designed and built in a cloud infrastructure using technologies comparable to on-premises solutions. The operating system and the identity management system, that provides access to the user layer of the virtualization stack, can be strictly controlled by the customer.

Throughout this document, NUARI is the customer of AWS and provides services and infrastructure for our clients. This can be during a sector-wide exercise, such as Quantum Dawn 3, or as a service for individual clients. Clients can also set up their own infrastructure and run DECIDE® and would then be responsible for the security of that infrastructure.

3.2 DECIDE® Access Security

DECIDE®’s AWS cloud infrastructure employs industry-standard 256bit SSL (Secure Sockets Layer) to provide secure communications over the Internet. Normal DECIDE® operations, including accessing the

DECIDE® web application, are encrypted using Hypertext Transport Protocol over Transport Layer Security (HTTPS) or Secure Shell (SSH).

- Authentication and authorization to access DECIDE® is controlled at all points of user contact.
- Web Authentication – DECIDE® users can log in to the DECIDE® web application using their login name and password. Authentication data is transmitted over an encrypted SSL channel via HTTPS.
- DECIDE® provides role-based access control (RBAC) for user account privileges (e.g. administrator accounts, standard user accounts). Customers assign roles to control the level of access provided to the users within their account. There are two available roles a Customer user may have: Author and Participant. Authors can grant fellow Customer Users the Author role. Authors have access to their Customer Exercise Management tools and Participants can only join exercises. (Note: For NUARI use only: The Administrator role is reserved only for NUARI employees, only an administrator can grant the administrator role. An Administrator can edit license numbers and expiration dates of Customer users and Customer accounts.
- DECIDE® administrators can also customize password management policies (e.g., set minimum password length, set password expiry interval) to meet the overall security policy.
- AWS DECIDE® administrative access uses Multi-Factor Authentication (MFA) which provides an extra level of security for administrative sign-in credentials. Administrative users will be prompted for their user name and password (the first factor–what they know), as well as for an authentication code from their MFA device (the second factor–what they have).

3.2.1 Internet Protocol (IP) Based Access Controls

Access to the DECIDE® servers can be further secured by setting policies that restrict access to predefined source IP addresses. With IP access policies defined, users must both authenticate successfully and originate from an authorized IP address. For example, IP login access can be limited to a range of addresses allocated to a customer's corporate network.

3.3 Authenticated Email

All DECIDE® users are required to have a valid email address for notification purposes. The system ensures that users have a valid email address from the point of account creation through any changes that are made to the user's profile.

3.4 Virtual Data Center Security

DECIDE® uses the virtualized data centers of AWS's cloud infrastructure, which are made of multiple virtual machines, networks, and network services including Virtual Private Networks (VPNs) and shared drives. DECIDE® secure cloud architecture isolates the underlying platform and data channels from other customers' resources.

DECIDE® servers have limited accessibility from the Internet. SSH servers require authorization through a public key authentication process and does not allow password based authentication. Administrators must explicitly enable inbound Internet traffic other than port 22 (SSH). Normal use will also require HTTP (port 80) and HTTPS (port 443). Access to these ports may be restricted to a specific VPN, or from a specific IP address or IP range, as noted earlier.

3.5 Virtual Machine Security

All DECIDE® customer applications are executed in virtual machines hosted on AWS. AWS actively monitors and maintains the hypervisor fleet to ensure each has the latest security patches and is operating within defined parameters. The hypervisor provides strong isolation of the processor, memory, network, and disk state between virtual machines. This prevents one virtual machine from inspecting the state, or even detecting the existence of, other virtual machines on the same hypervisor. The only communication channel between virtual machines is through managed private links between internal virtual machines. NUARI administrators are not permitted access to the hypervisor or physical machines within AWS; they can only manage virtual machines through SSH or HTTPS access.

NUARI (or individual customers) have full control of the Operating System (OS) and application software running in their virtual machines (VMs). NUARI (or individual customers) are responsible for configuring and maintaining OS and all application software to ensure security of their virtual machine environments. This includes password management, patch management, anti-virus (AV) software and malware detection/prevention, and running firewalls to secure their virtual machines. As mentioned, virtual machine networks are, by default, not exposed to the Internet. This is an important security feature of DECIDE®. Within DECIDE®, NUARI (or individual customers) controls if or when VMs are exposed via public IP addresses, or have mapped ports open to the public Internet. DECIDE® customers can also block outbound network traffic from VMs to the Internet. This is discussed in the next section.

3.6 Network Security

DECIDE® servers are registered in Domain Name System (DNS) to allow for management via Uniform Resource Locator (URL). Users can leverage several mechanisms to manage access to their VMs and networks from within segregated networks and the Internet.

3.6.1 Internal Network Access Control

Each virtual network can be isolated from all other virtual networks within DECIDE®. Routing between networks can be constructed if needed, but is not done by default. Networks within different accounts will not be connected.

3.6.2 Outbound Network Access Control

Virtual machines access the Internet through a default gateway provided on each network. Internal private addresses are mapped to a public DECIDE® address using IP masquerading, Network Address Translation (NAT). DECIDE® users can disable outbound access at any time.

3.6.3 Inbound Internet Access Controls: Port Forwarding

Networks within DECIDE® are generally not visible or accessible from the Internet, but customers can selectively allow inbound Internet access for specific network services (e.g., HTTP). Network rules in DECIDE® permit incoming packets from the Internet on specific ports to reach the virtual machine; all other ports remain blocked.

3.6.4 Inbound Internet Access Control: Public IP Addressing

Individual clients managing their own infrastructure can also acquire a Public IP address from AWS and attach the address to individual VMs. This allows customers to open all ports for both inbound and outbound Internet access without port mapping. This is not recommended, but is possible. The current NUARI configuration uses a customer-facing load balancer to provide access to an internal subnet, which has private IP addresses.

3.6.5 Internal Firewall with Port Forwarding or Public IP Addressing

Individual clients managing their own infrastructure can customize their network security posture by deploying and configuring their own virtual network appliances with port forwarding or attached Public IP addresses. For example, a customer can provision a virtual firewall appliance with complex port forwarding and Access Control List (ACL) rules on traffic destined to and from other VMs within the network. As noted above, the current NUARI configuration uses a customer-facing load balancer.

3.6.6 IP Security (IPsec) Virtual Private Network (VPN)

Customers can connect their DECIDE® networks to external networks through IPsec based VPN tunnels. For example, DECIDE® networks can be securely connected to a corporate network through a tunnel. With such a tunnel, all traffic to and from the customer's virtual network in DECIDE® will flow through the secure tunnel to the customer's in-house network where the traffic can be subject to internal IT network policies. Customers have full self-service control over the IPSec VPN parameters in DECIDE®, including the protocols, shared key, and network policies. DECIDE® provisions an independent IPSec VPN gateway for each customer.

Network traffic to and from VMs are restricted to only the virtual network(s) they are attached to through Virtual Local Access Network (VLAN) isolation at the physical and virtual hypervisor switch layers. Each environment may contain one or more virtual networks. Internet traffic to virtual machines is controlled by a firewall at the DECIDE® data center network perimeter. In addition, customers can deploy their own virtual network appliances within their virtual networks or configure firewall policies within their virtual machines. A dedicated VPN gateway is provisioned and connected to the

development environment's virtual networks in order to provide an additional level of security to that virtual environment. NUARI administration of this configuration is via a VPN gateway. Customer access to the DECIDE® servers, is via a load balancer, which provides the TLS endpoint connection. That is the only 'public-facing' address for customers when using NUARI provided and configured services. If a client chooses to set up their own infrastructure, they would determine the configuration and management of that infrastructure.

3.7 Data Security

3.7.1 Data Architecture

The DECIDE® data architecture design has implemented a multi-tenant style design. This design allows data to be compartmentalized by customer organization. Facilitator question responses are associated to a participant through the role(s) they were given during the exercise. Yet there is an association of the data to the customer organization level. Therefore, we are able to silo responses from customer A vs. customer Z. The customizable DECIDE® meta-data for scenario creation, for example valid values for exercise roles, are shielded from one customer organization to another.

There is one application access point to the DECIDE® database. There are no user-defined direct connections to the DECIDE® database. A user/participant can only access scenario data from within the DECIDE® application. The responses from the facilitator questions are available for analysis through database views in a separate schema from the application schema. This separation allows for providing read-only access to Cybersecurity Analysts for providing after action reports (AARs) and business intelligence graphs.

With the stated concepts in place, data provided by the participants are not encrypted in order to not hinder performance. Falling under the personal identifying information, each password for participant application access is encrypted within the database.

3.7.2 Securing Data at Rest and In Transit

AWS DECIDE® maintains its data—including disk images, asset files, and shared drive contents—in virtualized network-attached data stores and exposes it via independent network file-system mounts. This provides isolation between file data for different customers, and between all disk images: when a virtual machine is run, only the disk images for that machine are exposed through the mounted file system, and only during the time the VM is running.

Further, movement of data between the storage layer and the physical servers are on an isolated management network that is not accessible to customer environments. In addition, NUARI may use encryption on the attached data volumes to provide additional security. **Customer data may be purged post-exercise, upon request.**

3.7.3 Continuous Monitoring and Remediation

All DECIDE® servers are scanned for new vulnerabilities on a regular schedule. Any required remediation, including patching, configuration changes or updates, are instituted as required. In addition to using built-in AWS tools for monitoring (such as AWS Trusted Adviser, Systems Manager, CloudTrail, CloudWatch, Security Hub and Config), NUARI uses a tool called CloudCheckr that maintains awareness of AWS services and compares the configuration to four separate security frameworks. The four that are being used currently are:

1. Cloud Security Alliance Cloud Controls Matrix v3 (CSA CCM v3)
2. NIST Cybersecurity Framework
3. NIST 800-171 (Protecting Unclassified Information in Nonfederal Information Systems and Organizations)
4. NIST 800-53 rev 4 (Security and Privacy Controls for Federal Information Systems and Organizations)

The goal of this monitoring in multiple frameworks is to maintain 100% compliance to all four frameworks. Any lapses are investigated and remediated as quickly as possible.

-- NOTHING FOLLOWS --