Coronado Group, Ltd.

# SCIT-Based Self Regenerative Survivable Cyber Security
# A Self-Regenerative Incorruptible Enterprise That Dynamically Recovers With Immunity

Coronado Group, Ltd. a leading provider of systems based on new and emerging technology and SCIT Labs, an innovative research and development firm delivering technologies that address the need call for new approaches to information security and survivability based have partnered to deliver transformational cyber security products and services that deliver proactive approaches using self-regenerative and recover with immunity technology.

SCIT Labs' patented [1]Self-Cleaning Intrusion Tolerance (SCIT) platform provides a valuable new tool to deliver cyber security and information assurance. SCIT allows information systems to dynamically recover with immunity in mission time without human intervention in response to unforeseen error and/or previously unknown cyber attacks. SCIT uses its patented technology in conjunction with virtualization technologies to defeat cyber attacks while protecting operating systems, device drivers, and applications. SCIT technology delivers proactive cyber defense capabilities using a combination of ultra-low intruder persistence and system regeneration at intervals as low as one minute.

SCIT robs adversaries of surveillance and intelligence gathering by limiting their presence to very short intervals while continuously replacing the operating system, device drivers, and application software with a pristine environment. To intruders the network appears static while operationally the environment is continuously rotated through a series of "clean" servers without requiring rebooting or making modifications to existing security protocols and practices. This approach provides enhanced adversary denial and deception. When equipped with SCIT forensics, this approach also enables added intelligence on intruder methods and attempts. SCIT is transparent to authorized users. It does not require changes to the services and capabilities. SCIT requires no modification of current cyber security protocols minimizing implementation risk and providing inside the network perimeter defense. In cloud computing environments equipped SCIT based regenerative systems capabilities reverse the asymmetric nature of current static system architectures and the inherent security risks without sacrificing the value of cloud based solutions.

---

[1] See US Patents 7725531, 7680955, 7549167 and US Patent Applications 1269686 and 11419832

## How It Works

SCIT provides proactive cyber defense and deterrence through delivery of ultra-low, configurable intruder persistence time. The SCIT moving defense paradigm allows systems to deter an attack by consistently changing the attack surface making it difficult to plan an attack. The systems are able to continue working through an attack, with automatic and rapid recover to a clean state. SCIT continuously replaces the operating system, device drivers, and applications with a new pristine server. This approach removes the residue from errors and cyber attacks automatically without human intervention.

Our approach supports wide ranging attack space coverage of cyber platform resources making it harder for an attacker to hit their target and successfully launch an attack. The regenerative aspects of SCIT support in-battle software upgrade and maintenance with no downtime supporting machine generated reconstitution with high levels of corruption immunity and digital asset protection; and battle field software repair and enhancement.

The SCIT approach does not rely on rapid forensics or intrusion detection to deliver defense capabilities detecting and defeating threats before they can be discovered using current cyber security techniques. SCIT's proactive approach differs from current cyber defense strategy based on defense in depth which works best when all layers are independent - firewalls and IDS/IPS systems for network defense. These approaches are reactive requiring a priori knowledge (signature) of the attacker and/or a complete description of normal behavior; approaches that are ineffective against the customized malware of determined adversaries. SCIT assumes that intrusions are inevitable focusing on proactive denial of persistence and automated cleanup and recovery of server assets. SCIT does not rely on packet inspection or intrusion detection. SCIT does not require this advanced system awareness to operate successfully.

The key component of SCIT's efforts will be to transform the current static ("sitting duck") servers into dynamic servers. Servers are constantly changing. This dynamism offers the following special advantages in the area of computer security and operational resilience:

- Servers are cleaned and restored to a pristine state every minute:
- SCIT parameters can be tailored to increase the security posture of high value assets;
- Malware is deleted without the need to detect it;
- Attacker visibility is increased by forcing the attacker to apply multiple attacks in an attempt to gain access to digital assets;

- Increased security of cloud environment;
- Elimination or reduction in server failures due to errors like memory leaks through self-regeneration;
- Near-real time management of digital assets supporting reconfiguration and application of patches and upgrades without rebooting servers;
- Better planning of software deployment and patch management; and,
- Because SCIT continuously deploys a pristine operating system, applications are harder to corrupt, disable or remove.

When a server is booted up, SCIT software launches a pristine, malware-free copy of the server's operating system (OS) and application into a Virtual Machine. After a certain, potentially random, exposure time to the Internet (usually less than a minute) the virtual server is taken offline and a new, pristine virtual server replaces the prior one. The decommissioned virtual server is wiped clean, loaded with a pristine copy of the OS and placed in a queue for re-activation. SCIT has focused on servers most exposed to malicious intruders. Such servers are located in a network's Demilitarized Zone (DMZ). SCIT focuses on containing any losses resulting from an intrusion without knowing that an intrusion has occurred, i.e. unlike other intrusion tolerant architectures SCIT does not require the intrusion detection step — it just assumes attacks to be continually in progress.

Using virtualization technology, SCIT rotates pristine virtual servers and applications every minute, or less. The nearby figure shows three different time periods. At any given time, there are five servers online and three servers being wiped clean. In each case a different set of servers is being cleaned. Eventually every server will be taken offline, cleaned and restored to its pristine state. SCIT technology can be used to build a variety of servers that meet enhanced security requirements. It is best suited to servers that are designed to handle short transactions – the lower the exposure time the shorter the transaction. The following four type of SCIT servers have been built and tested: SCIT - web-server with session persistence; SCIT - web-server supporting ecommerce; SCIT - single-sign on server; and SCIT - DNS Authoritative server.

SCIT Labs successfully addressed these issues using information only web servers, DNS servers, ecommerce webservers and single sign on servers. SCIT seeks to extend that research to the challenge presented by complex mission critical and war fighter systems. Complex systems support thousands of servers, millions of users and extensive information and operational assets. The transition from a static environment to a dynamic environment has the potential to delivery improved attack deterrence and intrusion protection.

Coronado Group and SCIT Labs personnel are an interdisciplinary team of computer scientists and information engineers all of whom have direct experience on developing and deploying cyber deterrence infrastructure.