CRUCIBLE EMBEDDED HYPERVISOR

Crucible enables system engineers to leverage virtualization to enhance the integrity and upgradability of defense systems that operate in the most hostile computing environments. Tactical virtualization of combat systems is a reality due to the availability of COTS hardware designed specifically to support virtualization. This emerging hardware allows Crucible to be highly performant.

GUARANTEES SECURITY + RESILIENCY

Crucible enables combat systems to survive and operate through cyber attacks with advanced isolation, attack surface minimization and cyber resiliency capabilities.

- Separates and isolates system components (services and functions) via strong, hardware-enforced boundaries, so interfaces between components are explicitly controlled
- Enables system engineers to deploy security service domains such as VPN domains, cryptographic service domains, security monitoring domains and encrypted storage domains
- Removes unneeded features and components from the hypervisor and common service domains to greatly reduce attack surface
- Leverages existing fault-tolerant protocols and recovery techniques to ensure functional and security service domains overcome, respond to and recover from suspected compromise
- Unlocks potential to deploy aggressive and entirely new attack response actions while minimizing risk to operations
- Addresses 39% of NIST 800-53 technical controls applicable to weapons systems

ENSURES PERFORMANCE + UPGRADABILITY

Crucible facilitates the allocation of system resources to ensure performance. This includes optimally performing runtime integrity monitoring of core service and application VMs (virtual machines), and enabling efficient and secure upgrades to the hypervisor, service domains and cryptographic support functions.

- Guarantees pre-defined allocation and non-oversubscription of hardware resources thereby ensuring critical applications can complete operations without interruption or interference by the hypervisor or other VM's.
- Supports real-time operations and thru-data paths while stopping compromised service domains from executing denial-of-service attacks by monopolizing processing resources
- Includes an interface to efficiently and securely upgrade the hypervisor, service domains and cryptographic support functions without worry about hardware and driver compatibility

ADDITIONAL SOFTWARE STACK SECURITY

Crucible primarily aids in decomposing software and hardware components into separate and isolated processing domains. Star Lab's other products provide additional security and anti-tamper protections throughout a combat system's software stack and can be protected by Star Lab's Titanium Security Suite.

Headquarters
1221 Connecticut Ave NW
Washington, DC 20036

STAR LAB SOFTWARE

202.706.7027
info@starlab.io
https://starlab.io