SECURWEAVE

Weaving the fabric of next generation security

CHESS-P
Data Sheet

Overtime, hacking has shifted its intentions as well as its sophistication. Originally created for thrills to test one's capability to gain access to protected areas, the focus inevitably moved to money and in recent times, the attacks have become even more brutal with state sponsored teams and organized crime rings, targeting defense establishments, critical infrastructures and large corporations. A standout feature of many of these attacks is the complexity and sophistication of the malware making conventional security solutions woefully inadequate to detect or prevent them.

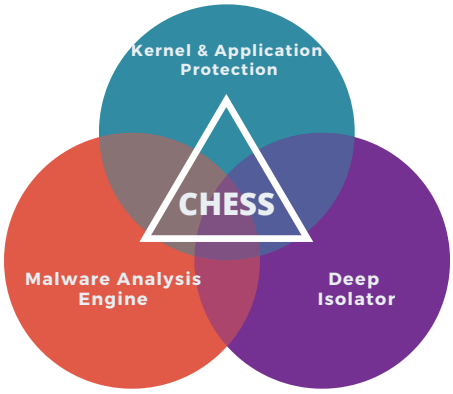
Threats that avoid detection and harvest valuable information over a long time are known as Advanced Persistent Threats (APTs). Traditional security measures such as antivirus, firewalls etc. cannot provide protection against APTs thereby leaving systems vulnerable to data breaches. The consequence of an APT attack is devastating as the attack may continue for a long time uninterrupted due to the limitations of most of the current security solutions.

SecurWeave's Hardware Enforced Security solution, CHESS is designed to fill the gap in cyber defense against APTs there by solving the long standing security gaps across endpoints, mobile phones, data centers and embedded systems.

Today's Challenges

- Exponential rise in complexity and sophistication of cyber attacks
- Existing security solutions cannot defend against kernel mode rootkits
- Breach discovery takes an average 197 days
- Attacks continue for years evading detection

Our Solution

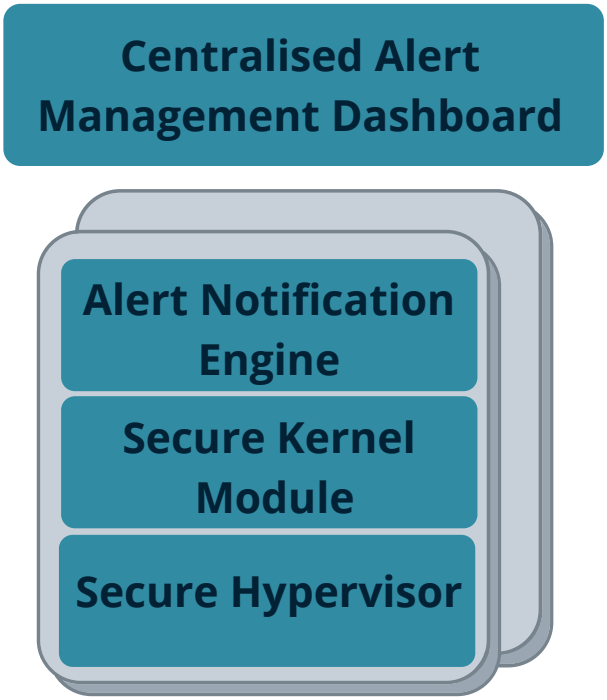


CONFIGURABLE HARDWARE ENFORCED SAFETY & SECURITY

CHESS-P

Configurable Hardware Enforced Security Solution - Kernel Protector

SecruWeave's CHESS-P is designed to protect Linux powered systems from kernel mode attacks. With the patented secure hypervisor technology, CHESS-P has a unique vantage point into the running system and can detect, stop and alert kernel mode attacks of any complexity. CHESS-P comes with a policy driven architecture and a configurable UI that can be interfaced with SoC for centralized alert management.



Features

Key protections offered

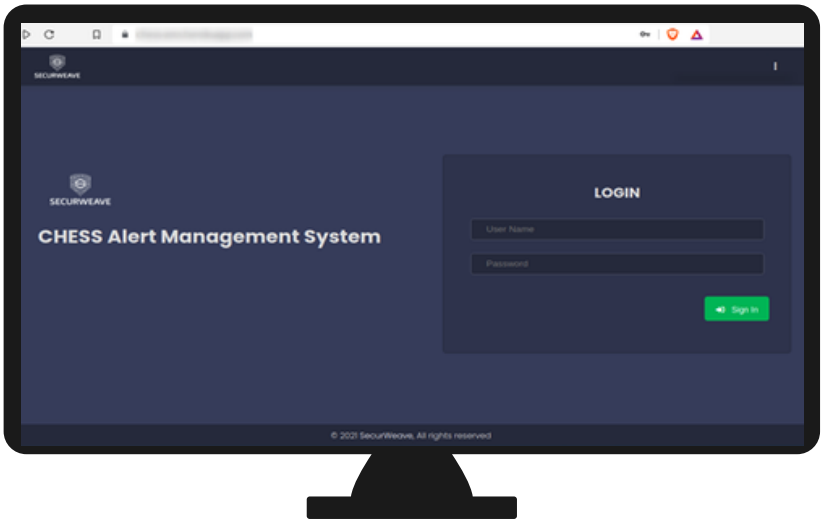
- Detects and Prevents malicious kernel code injection
- Detects and Prevents tampering of critical kernel data structures and security critical CPU registers.
- Detects privilege escalations through kernel vulnerabilities
- Protects against DMA attacks by preventing unauthorized changes to IOMMU

Non By-passable as Secure Hypervisor runs at higher privilege level than kernel mode malware

Multi level alert log mechanishm

CHESS Alert Management System :

OpenAPI based Alert Mangement system for consolidated view of all the CHESS installed machine status and alert log



- Supports both cloud based installation as well as in premise installation
- Includes License manager
- Easy to integrate with third party alert management solutions through OpenAPI
- Status of CHESS on each system can be monitored with configurable heartbeat

CHESS-P Requirements:

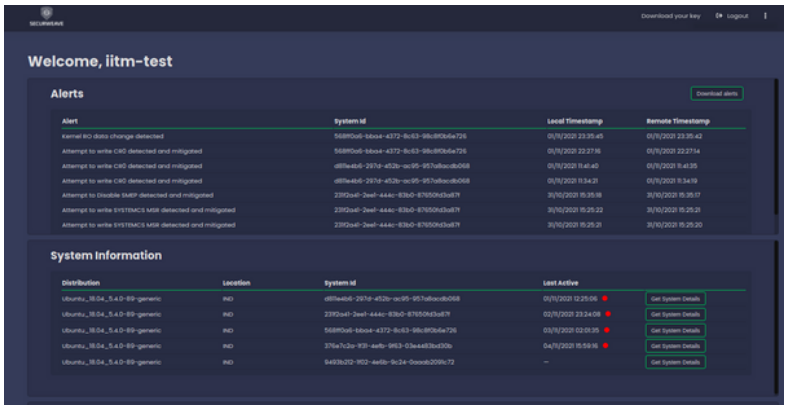
- Intel 64 bit processor with Virtualization support i.e. VT-x and VT-d enabled
- Linux based Operating System with Grub as the bootloader

CHESS-P Test Summary:

Intel Processor Variants	Linux Distributions
Intel Core i7-9700, Core i7-7700, Core i7-2600	Ubuntu 20.04, Ubuntu 18.04
Intel Core i5-7200U, Core i5-4200U, ore i5-3570	BOSS (Debian) 8
Intel Core i3-8145, Core i3-4010	RHEL 8.2

Able to detect and prevent major kernel mode rootkits like

- Diamorphine
- Reptile
- Sutekh
- LilyOfTheValley



<0.1 % performance impact observed during tests

"Though there are a few commercially available separation kernel / embedded hypervisors in the market, we zeroed in on CHESS-P due to the advanced threat prevention features it provides. The kernel mode protection features of CHESS-P are a need of the hour especially considering the proliferation of Advanced Persistent Threats in recent times"
- Prof. Kama Koti, Director IIT Madras

SECURWEAVE

securweave.com
info@securweave.com
+91-8790532463

Plot No 13/A, Laxmi Nagar Colony, Manikonda,
Rangareddy Telangana,
India 500089