GLOBAL NETWORK TECHNOLOGIES

CybrHawk
Transforming Cybersecurity

Process Injection
Next-Gen Protection

Cybrhawk Process & Memory Injection Detection included in our SIEM platform is a powerfull tool that blocks malware and rasomware before they can launch an attack.

Be aware of the current threats

- 77% of sucess attacks are fileless per 2018 Data, Pokemon Institution
- Each Windows Endpoint is vulnerable to Memory and Kernel Injections attacks
- Process & Memory Injection Attacks are aimed at stealing or locking out data without being detected by AV platforms
- Traditional Antivirus platform don't prevent Memory Injections from ocurring

CybrHawk Adventages

- Blocks 100% Windows Memory Injection advanced attacks
- Exploit, adversary evasion, and file less attack prevention
- Shielding prevents malicious module loads, DLL injection, and shellcode injection
- Authentic no false positives or false negatives
- Blocks attacks in-line before it happens
- Seamless to the end user
- Forensic Evidence: Attribution
- Trusted by Microsoft
- No user interaction – Fully deterministic

ABOUT US

Cybrhawk SIEM is the only SIEM in the market that provides Process & Memory Injection Detection, including all the critical tools: IDS, Intelligence risk, behavior, machine learning & cloud info. The goal is to provide enterprise with full and total control systems.

SIEM ZTR Process & Memory Injection

- Process & Memory Injection on Windows endpoint device
- Pre-Exploit windows Prevention
- Easy integration across the enterprise

Contact Us

www.gntcompany.com

sales@gntcompany.com

1 844 483 2455

Follow Us