**Compatible with:**

Windows NT 10/8.1/8/7/XP
Windows NT Server 2012-R2/08-R2/03
Linux Kernel Build Work Station & Server
Macintosh OS & Macintosh OS Server
IBM PC/Intel x86 & Successor Mainframe
HP-UX, SCO UnixWare, Others/Misc.

**Note:** *Can be integrated to Splunk, Cisco Umbrella and Stealthwatch, or similar security tools.*

# *Product Quick Guide:* Hippogriff LLC Anti-Tampering Log File Detection Suite

***Global, Innovative, Computer Technology Protection Services***

*"In February, 2016 hackers managed to steal around $81 million from a Bangladeshi bank in one of the largest digital heists in history. Security researchers from BAE Systems published details of what they claim to be a piece of sophisticated, custom-made* ***malware used to cover the hackers' tracks by manipulating logs*** *and forcing printers to produce phony transaction confirmation messages."* - Motherboard.com, Vice Media LLC

**Proper chain of custody is an important aspect of information security. Hippogriff's approach allows for the flexibility of keeping logs private while eliminating the need to store the complete contents with a verified third-party.**

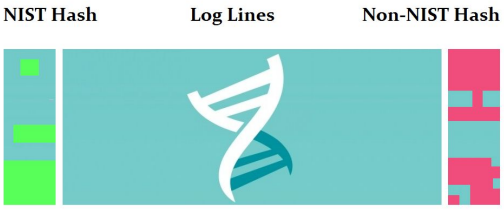
**Systems generate an incredible amount of logs and while development continues and complexity expands, the demand for logging solutions is rapidly increasing. Secure off-site storage of these logs has created an expense insufficiency and is not guaranteed to be incontestable.**

**This secure methodology from Hippogriff could be applied to systems – with little overhead necessary – including but not limited to:**

- *TRANSPORTATION*
- *INFRASTRUCTURE*
- *COMMUNICATIONS*
- *BANKING/FINANCE*
- *IOT ENABLED TECH*
- *ELECTIONS/VOTING*
- *SPACE ORBITALS*
- *PUBLIC SAFETY*

**This product solution is the only approach which provides a seasoned proof that a compromised system has not had its log files modified or replaced.**

## Visual Concept of Single Origin Cryptographic Chain of Custody (SOCCC)




| NIST Hash | Actual Log Files | Non-NIST Hash |
|---|---|---|
| foAHF8e72 | Log Line # 1 | Jkmfes751 |
| f8ijsjg93jss | Log Line # 2 | Wkf5i73gf |
| 9sjwFjsbge | Log Line # 3 | Zcndj7enl |
| KsjfjsdKfjns | Log Line # 4 | Kmfd63spl |
| 8J6sedw3t | Log Line # 5 | Whnvhdw4 |
| J8kp3fu5kd | Log Line # 6 | Jmnrpo45g |
| kjvcrjg6Djk | Log Line # 7 | F6wjnlhr7 |
| KfuefurGn5 | Log Line # 8 | M6fjswjmf |
| xw32kjH8 | Log Line # 9 | bgw427k |
| Ag45wjKfh | Log Line # 10 | 335ximg9 |
| Jw4Knfn77 | Log Line # 11 | 8Pmfahjd4 |

- This method of fusing encryption and mathematical hashing increases its strength against tampering or code breaking; even in resistance to quantum computation attacks.
- Every line's hashed values are mathematically computed from the results of the previous log lines.
- Both one-way algorithms are intertwined to protect the integrity of the payload (log lines) from tampering.
- The green and red shaded areas are results of two different mathematical hash algorithms based on the data residing in the blue area.
- The range of the blue area can be configured to suit the end user's needs in regards to performance vs. strength.

**This** proprietary software product from Hippogriff utilizes a unique method of fusing the results of two parallel cryptographic functions in order to mathematically prove that an audit log has not been tampered with, modified, or replaced. This product allows for a Single Origin Cryptographic Chain of Custody (SOCCC/SO-3C) which alleviates unnecessary overhead via expensive third-party log storage – with limited guarantees of integrity or prompt access by system administrators.

**A** SOCCC allows for confidentiality, control, and confirmed custody of system log files. The purpose of this approach is to avoid information disclosure with third-parties on sensitive systems while effectively maintaining a secure logging solution.

**A** small signature is written before and after each log line which yields a mathematical sum of the previous logs contents using two algorithms. Each line written to the log compounds the security and integrity, further strengthening the system against exploits.

**The** mathematical methods of hashing are modular and can support National Institute of Standards and Technology (NIST) and non-NIST algorithms or even a combination of both. This non-deterministic redundancy helps alleviate concerns about vulnerabilities in mathematical functions as a potential backdoor or weakness in one of the hash algorithms; hence it cannot be exploited due to the other hash function not being symmetrically vulnerable in the same manner.

U.S. Toll Free Phone: **1-866.273.4831**, E-mail: **inquiry@hippogriff.tech**, Web: **http://www.Hippogriff.TECH**