

Achieving “World Peace” with Groovy Security Tools



– Spyro Malaspinas, CISSP, CISM, CISA, GCIH
Principal – 3Factor

Making of a Security Nerd - Bio



- Principal - spyrom@3factor.com



- PCI Global Practice Leader



- Managed Security Services: Security Architect
- Global Consulting Services: Sr. Security Consultant



- Global Services Security Engineer/Firewall Architect



Alphabet Soup:

CISSP, CISM, CISA, GIAC-GCIH, CCNA, CSPFA
CCSE + , CCSE, CCSA, NSA, Six Sigma

Agenda

- What is “World Peace” in the Enterprise
- Colliding Agendas: Metrics, Goals, and Politics
- How are we to achieve “World Peace”?
- Three Groovy Security Tools that everyone will love
 - IdM - Identity Management
 - SIM/SIEM - Security Information Manager
 - File Integrity Monitor
- Making the case for your organization
- Considerations (Pros/Cons)
- Questions?



What is “Peace” in the Enterprise?

- "Harmonious and synergistic habitat where operations, compliance, and security coexist... peacefully, efficiently, and productively" - me



Where does this fantasy land exist?

- Put simply, It doesn't!
- We must consistently compromise while still striving to achieve our goals
- This means working with teams with differing goals, agendas, metrics, and political aspirations



Problems Inherent in Today's Enterprise

- Today security and compliance are often seen as draconian principles, single - sided, and oblivious to REAL business needs
- Operations, security, and compliance leaders are often motivated by different goals, many of which are mutually exclusive
 - Too many agendas
 - Too many disparate goals
 - Too much politics



Colliding Agendas, Metrics, and Goals

- Operations: Typically measured by uptime, associated costs, adherence to SLAs, and customer satisfaction
- Security: Measured by residual risk, costs, ability to protect assets from confidentiality, integrity, and availability disturbances
- Compliance: Typically measured by adherence to regulatory and best practice standards, ability to avoid fines, breaches, pass audits, and communicate with partners and industry watch dog groups



With Differing Metrics and Goals?

- Operations: Aims to ensure uptime and SLA's are met at ALL costs
- Security: May disrupt operations in an effort to meet their goals, desiring best of breed security methodologies in favor of security practices that work well for the operations environment
- Compliance: Can be disruptive to security and operations teams; desiring reporting and heavy logging that can thwart real effectiveness of a security program, operating environment, and security tools

FIGHTS BREAK OUT, EGOS "MINGLE", AND THE SUCCESS OF THE LARGER ENTERPRISE SUFFERS AS A RESULT!



Harmonious Existence...

- What are some of the ways that we can coexist with operations in a way that benefits both operations, security, and compliance objectives and principles?
- Deployment of productive tools, processes, and practices that enable each of the groups success.
- Specifically we will look at a use of the following tools within one of the largest hotel chains on the planet. All repeatable success stories in medium to large enterprises.
 - IdM - Identity Management Tool
 - SIM - Security Information Manager
 - File Integrity/Configuration management



Identity Management: IdM

- An Identity Management System (IDMS) identifies individuals in a system and controls their access to resources within that system by associating user rights and restrictions with each identified individual.

From a security perspective, weak, stale, and shared passwords are oftentimes considered to be the biggest threat to an enterprise by experts.

Why: "passwords are the weakest link in the enterprise," says Robert Lonadier, president of RCL & Associates, a security consultancy in Boston.

Passwords are still the most pervasive tool used to secure today's organizations!

IdM: How does it work?

- IdMs centralize user administration for many devices, appliances, and applications
- OSs, applications, and devices will not authenticate to local user repositories, rather a query will be made to the IdMs for authentication and authorization levels



username: _____

password: _____

IdM: Passwords; a security slant

- According to CERT, 80% of the security attacks they investigate are password related
- Vulnerabilities of password-based solutions stem from the following
 1. Humans aren't perfect and cannot be relied upon to maintain a process that is rules-based
 2. Other, more job-related processes compete for attention
 3. Certain insiders and outsiders are intentionally seeking ways to compromise the solution

hacker

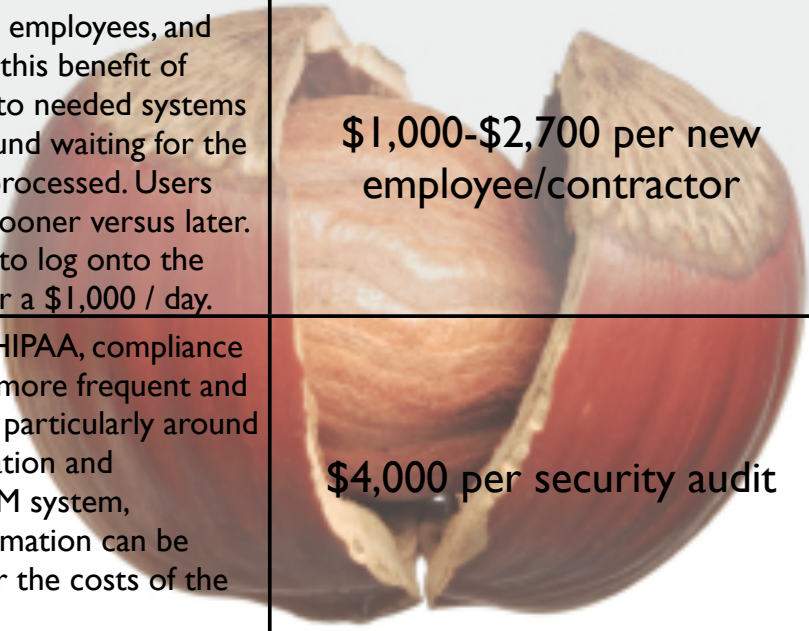
What are the costs of poor password management?

- 40% of all help desk calls are for forgotten passwords*
- Each year companies spend up to \$200-\$300 per user attempting to maintain secure passwords*
- ★ ? How many calls per quarter does your help desk receive?
- ★ ? What does it cost to run your help desk per quarter?

*Gartner

IdM: Real ROI... in a Nutshell

Benefit	Summary	Avg \$ Savings
Improved Application Development	With a centralized user admin stack, developers don't have to spend the usual 20% of a project writing user login and admin. code. Utilize identity stack as a service.	\$15,000 per application
Improved IT Efficiency	Captures the value of having a centralized, fast responding, IT infrastructure. Fewer licenses are required because they can be tracked better. Companies can absorb M&A	\$75,000 per 1000 users/yr
Faster user account activation	For contractors, new employees, and users changing roles, this benefit of getting faster access to needed systems instead of sitting around waiting for the change order to be processed. Users become productive sooner versus later. A contractor unable to log onto the network can run over a \$1,000 / day.	\$1,000-\$2,700 per new employee/contractor
Reduced Compliance Costs	With SOX, PCI and HIPAA, compliance audits are becoming more frequent and require more details, particularly around user account information and privileges. With an IdM system, requested audit information can be provided faster, lower the costs of the security audits.	\$4,000 per security audit

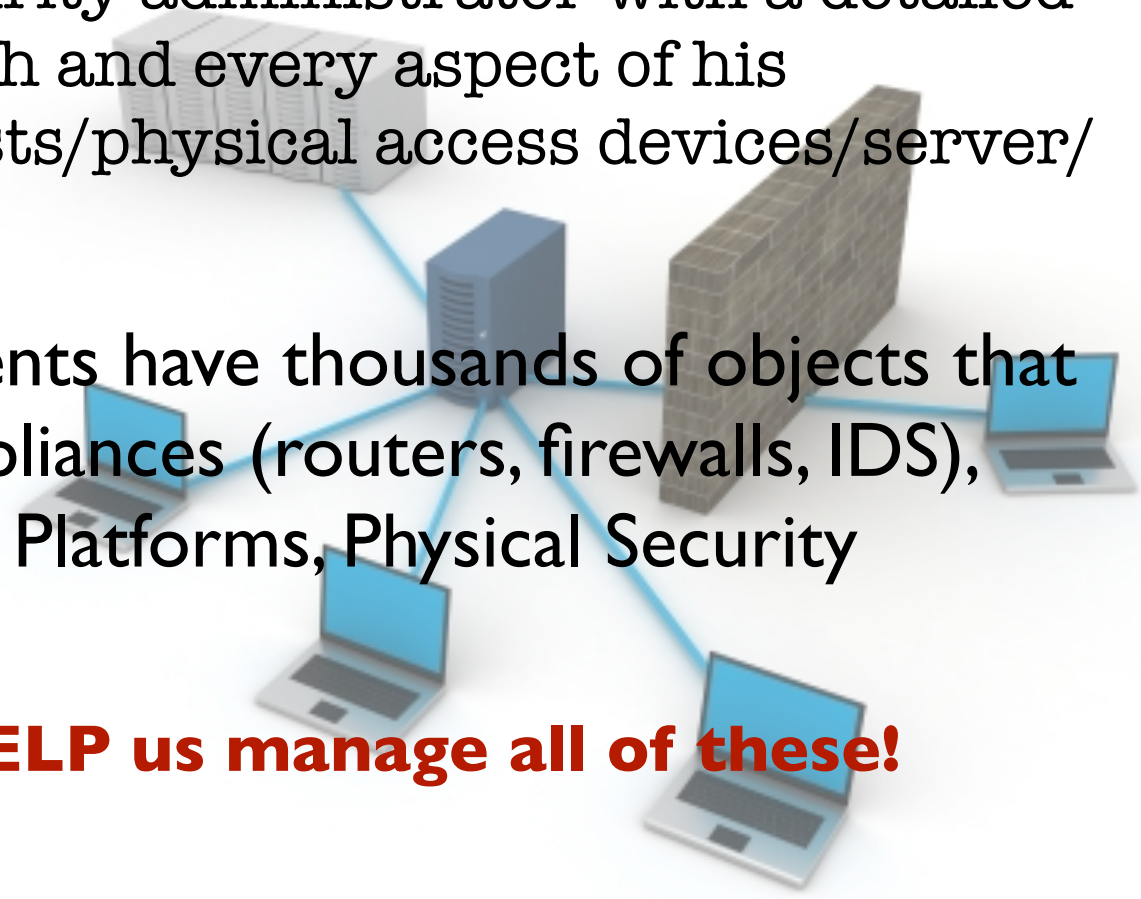


SIM/SIEM: Security Information Management

- What it is: Comprehensive compilation of tools which, when working together, grant a network/security administrator with a detailed view over each and every aspect of his networks/hosts/physical access devices/server/etc...

Many of our clients have thousands of objects that log; network appliances (routers, firewalls, IDS), applications, OS Platforms, Physical Security

SIMs HELP us manage all of these!



SIM/SIEM: How does it work?

- Popular SIM tools have the ability to collect logs from disparate devices, appliances, OSs, applications, and even physical security doors, card swipes, etc.
- SIMs typically receive logs via syslog, or through “collectors” that normalize logs from proprietary and or non-standard logging formats
- SIMs deployed in large environments may have log aggregators, or filtering log appliances that filter and aggregate logs from remote sites for submission over a WAN/MAN connection to save bandwidth, and processing cycles

SIM/SIEM: Solving Problems

A hand is shown with the index finger pointing at a circular button labeled 'LOGIN'. The background is a blurred image of a person's face.

Security:

Problem: no way to receive, monitor, manage, or react to security threats in a proactive manner without centralized logs that includes some intelligence.

Benefits:

- PROACTIVE:** Real-time event monitoring
- INTELLIGENCE:** Multiple event correlation methods to detect both known and unknown threats while reducing the number of false positives
- VISUAL:** Dynamic visualization for fast and intuitive threat identification, tracking, and analysis
- Integrated risk assessment to understand the overall vulnerability of any particular logging asset within the enterprise
- FORENSICALLY SOUND:** Comprehensive reporting and forensics for all levels of security operations
- WORK FLOW:** Robust incident-management system that organizes security event data and enforces security response workflow
- HOLISTIC:** Complete event monitoring for all multivendor security environments

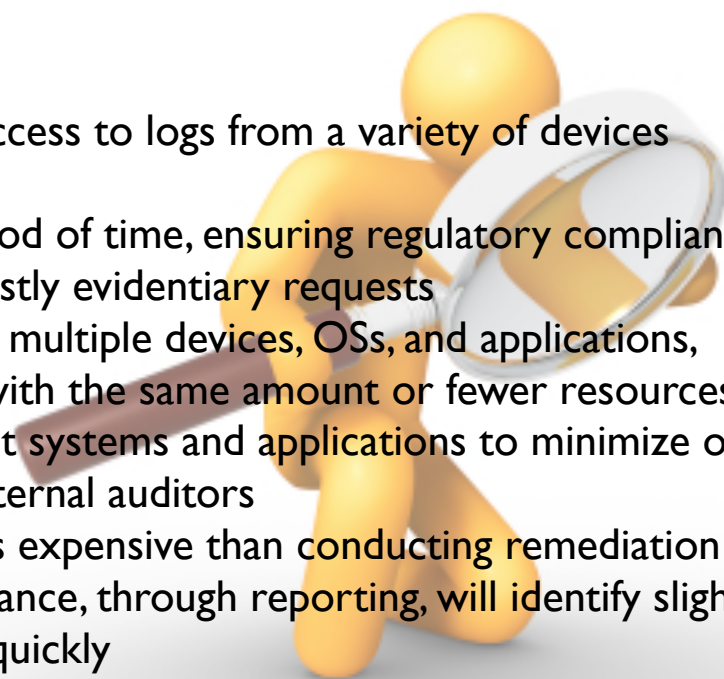
SIM/SIEM: Solving Problems

Compliance:

Problem: no centralized repository for logging. Troublesome, costly, and time consuming to pull logs from disparate systems on a regular basis to ensure internal policies and external regulatory controls are being met.

Benefits:

- **TIMELY:** Compliance staff can be given read only access to logs from a variety of devices based upon need to know
- **RETENTION:** Logs are kept for a pre-defined period of time, ensuring regulatory compliance is met. Stale logs can be purged to protect against costly evidentiary requests
- **COMPREHENSIVE:** With logs being received from multiple devices, OSs, and applications, compliance can be more thorough in their sampling with the same amount or fewer resources
- **PREPARED:** Empowering internal audit to pre-audit systems and applications to minimize or eliminate the deficiencies that will be identified by external auditors
- **SAVE MONEY:** Maintaining compliance is much less expensive than conducting remediation overhauls annually. Consistent monitoring by Compliance, through reporting, will identify slight variances in controls which can be fixed much more quickly



SIM/SIEM: Solving Problems

Operations:

Problem: Operations typically responds to problems reactively; via open help desk tickets, calls from employees, customers, or partners.

Benefits:

- **TIMELY:** Logs received from applications can often alert staff to a small problem which can lead to outages
- **UPTIME:** More timely alerts, leads to a quicker, prioritized response, leading to better uptime
- **HAPPIER CUSTOMERS:** With better metrics and SLAs, customers are happier
- **COMPETITIVE:** Real time alerting can be a competitive advantage to service providers who manage customer assets, their uptime, and availability
- **EFFICIENT:** Automated alerting often leads to staff reduction opportunities, and reappportionment of this staff to more strategic, revenue generating projects

File Integrity Software



- What it is: Software that alerts on changes to critical system and application files (logs, configuration files, password files, event tracking, owner, group, hash values, etc.)

Most of large enterprises have system build procedures for systems and applications. Once installed into production, very little monitoring occurs relative to deviations from the original build.

File Integrity Software help us monitor changes in our environment!

File Integrity Software: How does it work?

- File Integrity software is configurable (think packages) relative to the application, OS, or appliance that you are managing
- Integrity software can manage changes to system files by running hashes or comparisons between current state, and original file state
- Even the slightest change in configuration will yield a hash change, and can trigger an alert to a support center

System connections, open sockets, CPU, and countless other attributes can be monitored

File Integrity Software: Solving Problems

Security:

- Problem: Once platforms and applications are deployed there are few checks to ensure that systems continue to adhere to build standards (gold disks).
- Compromises by more advanced intruders are often unnoticed without extensive monitoring

Benefits:

- **PROACTIVE:** Real-time event monitoring
- **INTELLIGENCE:** Can be used in concert with SIM to detect a multitude of different attacks, and system misconfigurations which can lead to vulnerabilities and subsequent compromise
- **HOLISTIC:** Modern day solutions provide significantly more knowledge around the production environment, critical assets, and all important configuration files, and how they adhere to enterprise security policies

File Integrity Software: Solving Problems

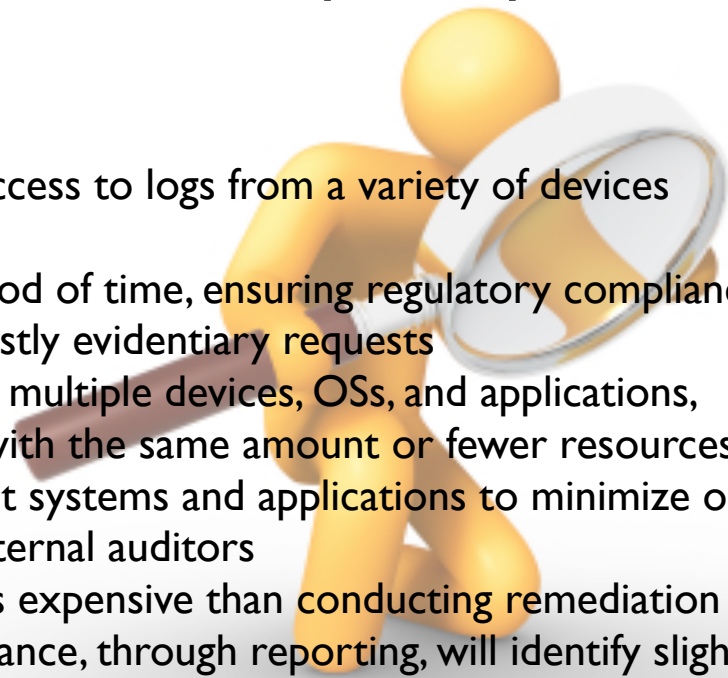
Compliance:

Problem:

- Sampling systems to ensure that control frameworks, and security policies are being met is time consuming and flawed.
- Reporting is laborious, and oftentimes requires engaging with operations, taking time away from critical day to day responsibilities.

Benefits:

- **TIMELY:** Compliance staff can be given read only access to logs from a variety of devices based upon need to know
- **RETENTION:** Logs are kept for a pre-defined period of time, ensuring regulatory compliance is met. Stale logs can be purged to protect against costly evidentiary requests
- **COMPREHENSIVE:** With logs being received from multiple devices, OSs, and applications, compliance can be more thorough in their sampling with the same amount or fewer resources
- **PREPARED:** Empowering internal audit to pre-audit systems and applications to minimize or eliminate the deficiencies that will be identified by external auditors
- **SAVE MONEY:** Maintaining compliance is much less expensive than conducting remediation overhauls annually. Consistent monitoring by Compliance, through reporting, will identify slight variances in controls which can be fixed much more quickly



File Integrity Software: Solving Problems

Operations:

Problem: Operations typically responds to problems reactively; via open help desk tickets, calls from disgruntled employees, customers, or partners.

Benefits:

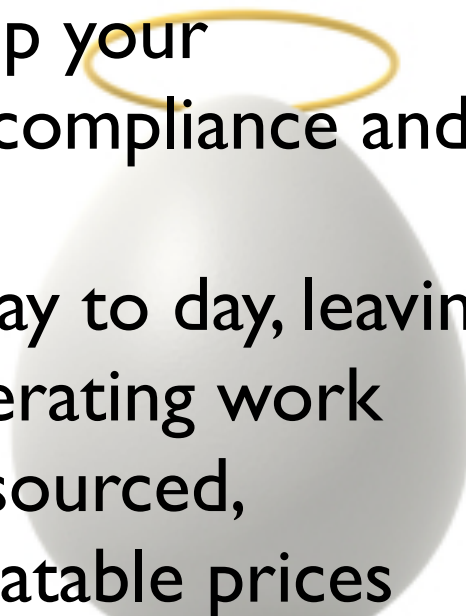
- **TIMELY:** Alerts received from file integrity monitoring software can often alert staff to a small problem which can lead to outages
- **UPTIME:** More timely alerts, leads to a quicker, prioritized response, leading to better uptime
- **HAPPIER CUSTOMERS:** With better metrics, SLAs, customers are happier
- **COMPETITIVE:** Real time alerting can be a competitive advantage to service providers who manage customer assets, their uptime, and availability
- **EFFICIENT:** Automated alerting often leads to staff reduction opportunities, and reappportionment of this staff to more strategic, revenue generating projects

Harmonious Existence...making the case

	IdM	SIM	Integrity Monitoring
Security	Password policy, authorization, entitlements, termination processes all benefit	Real time alerting to security events from a multitude of security devices, correlation to help prioritize incidents, false positive reporting to reduce wasted cycles	Ensures adherence to system builds and baseline standards. Slight deviations can be alerted on in real/near real time
Compliance	Auditing is less timely, sampling size is more significant, management of compliance is now possible for entitlements	Audit log retention is crisp, purging of stale data is now possible comprehensively, monitoring of compliance levels can occur more easily and throughout the year, rather than point in time compliance	Adherence with internal security and compliance requirements, ongoing compliance checks are less intrusive upon ops/security teams
Operations	Quicker access for new employees/contractors, user administration is lighter, less help desk calls	Misconfigurations of applications are often reported more quickly, reducing downtime, and failed SLA measures. Prioritized and correlated alerts for down links, disk usage, high CPU utilization, etc.	Misconfigurations of applications are often reported more quickly, reducing downtime, and failed SLA measures. Prioritized and correlated alerts for down links, disk usage, high CPU utilization, etc.

SIM, Integrity Monitoring, and IdM: Things to Think about

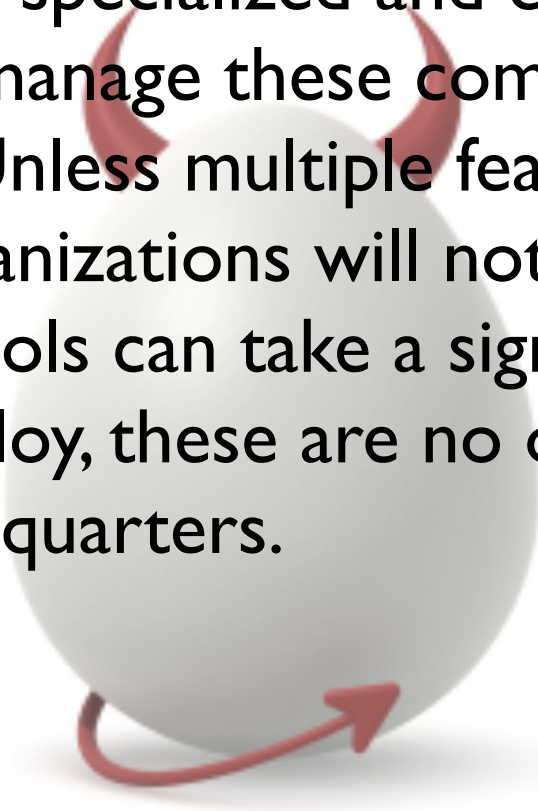
Pro's:

- In the right environment, these tools can save businesses hundreds of thousands of dollars a year
 - These tools in combination will help your organization mature from a security, compliance and operational perspective
 - Less time will be spent managing day to day, leaving more time for strategic, revenue generating work
 - Many of these services can be outsourced, providing similar benefits at more palatable prices
- 

SIM, Integrity Monitoring, and IdM: Things to Think about

Cons:

- These tools can be very expensive to deploy
- A specialized and costly workforce may be required to manage these complex tools
- Unless multiple features are utilized some organizations will not get their monies worth
- Tools can take a significant amount of time to deploy, these are no over night projects. Many take 2-3 quarters.



QUESTIONS?

