



Cressida Technology Ltd
1 Lammas Gate, 84a Meadow
Godalming, Surrey
GU7 3HT, UK

Tel: +44 01483 239300
Fax: +44 01483 239383
Email: info@cressida.info
Website: www.cressida.info



Andy Evans
Senior Security Engineer, Ecora Corp.
andy.evans@ecora.com

Improving Enterprise Security with Ecora's Configuration Auditor

Significant Benefits for the Security Objective Methodologies and Best Practices

Enterprise security is traditionally managed with a plethora of tools. Common among them are firewalls, intrusion detection systems, vulnerability scanning, and penetration testing. Regardless of perimeter protection and the frequency of external scans, systems are continually compromised. What part of the security solution is being overlooked?

Time and time again it has been shown that an oversight in operating system or application configuration is a contributing factor in the great majority of exploits. Ecora's Configuration Auditor software simplifies control through configuration management and assessment. In this document, we describe our methodology and the benefits of this tool for effectively securing the enterprise.

The View from the Inside, Outward

Traditional system security scanning and analysis tools have a singular perspective, to assess only what is apparent from the outside. This leaves the internal vulnerabilities of a complicated infrastructure completely unassessed. The discovery process can only be accomplished with a complete examination of the internals. Ecora's configuration management through documentation offers a new perspective from which to view the problem: an inside-out look at network services, interfaces, software feature sets and revisions, and patches and hot-fixes. The resulting documentation includes an evaluation of well-known best practices with tips, notes, and references to additional information.



painstaking and time-consuming process, often a truly Sisyphean effort. Information can become outdated before the assessment is published; or worse, a critical configuration changes before a manual assessment is complete. Even the best efforts are prone to error and inconsistency. Automation of the process with Ecora's Configuration Auditor software offers a significant breakthrough in IT assessment, control, and management. Accompanying a comprehensive collection of configuration data is an intelligent assessment and analysis presented in easy to read, plain-English text. The most obscure, yet significant parameters are exposed. This workstation-based, agentless technology produces immediately useful documentation in browseable HTML and printable formats. A CSV formatted set of configuration parameters is available for export. Visio diagrams of relationship contexts and topologies are provided for overview and holistic analysis.

Feature-rich and accessible documentation will become an indispensable reference point you can turn to again and again, when you really need to know what's going on inside. Over time, an analyst's knowledge of your infrastructure increases through familiarity of review, itself a significant accomplishment, yet simply a by-product of the overall assessment effort.

The Audit Impact

The audit process is frequently perceived with fear and intimidation. Often, it is the culmination of accountability for a year's worth of effort under a magnifying glass. The process includes significant effort, updating systems, checking consistency, and ensuring that all the facts are presented accurately. In place of fear and intimidation, this effort should be embraced with a much more positive attitude. Regular internal audits should be performed to meet specific objectives and used to assist with enterprise security strategy, assessment, and administration. Ecora's software provides automation in discovery and consistency in reporting. Preparation time is reduced and consistency is realized, which can result in greater acceptance of the audit process. The process should become routine, a component of regular maintenance.

The work of the auditor is intended to benefit the company as a whole, from shareholders to customers. The effort can provide peace of mind – once it's complete. Increasingly, it is becoming a requirement; and may soon be mandated by law. The HIPAA guidelines, the Gramm-Leach-Bliley Act, the FDIC, FDA, FTC, and the Federal CIO Council's efforts are just a few examples... all intending to enforce privacy and accountability requirements that ultimately result in solid IT data integrity. Interestingly, and of significance here, this legislation embraces the audit process.

Policy Assurance

IT audits must correlate with accountability. Enterprise-wide IT policy is an absolute prerequisite. Accountability is an infallible tool in the advancement of security. Without established policy, there is nowhere to begin, nowhere to turn, and no organized flow of ultimate responsibility. A competent IT policy becomes effective only when it is properly promoted throughout the enterprise, with traceable accountability in place at each level. Such policy ultimately defines the influence and effectiveness of audits.

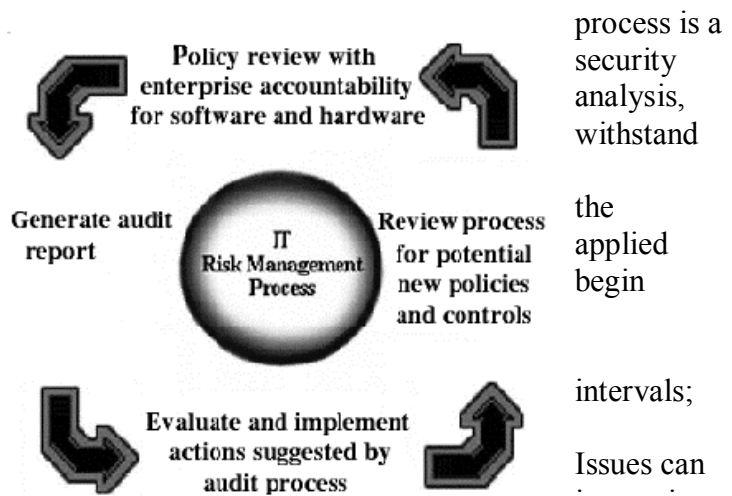
Implement a program to promote IT security awareness and to provide educational material that advocates an understanding of safe computing practices. Educate on what to avoid, define unsafe computing, and demonstrate what users can do should they encounter a potential security breach and how they can avoid unsafe practices. Empower end-users through education, while promoting accountability for their actions.

Once policy becomes established, it does not mean efforts will be consistent and faithful throughout the organization. A process is required to ensure compliance with such policy. This is why it is important to test for policy adherence weekly. A regular, interval-based audit process can only be accomplished with automation.

Auditing for Security

A closed-loop risk-management audit highly efficient method of advancing IT and control. This involves a cyclic audit, and review. Importantly, results must be the scrutiny of established policy. Adjustments in system settings, as well as established policy, should be considered, judiciously, and the process must then begin anew.

Cyclic audits are performed at regular intervals; new systems, software, upgrades, and vulnerabilities will appear unpredictably. Issues can be addressed as they are exposed, security, control, and response immensely. With a policy review process incorporated, enterprise IT policy management gains effectiveness. Risk management becomes an established proactive practice. The audit process should become entrenched within routine maintenance. The power of scheduled assessments promises significant and consistent advancements in enterprise-wide security.



Ecora's Configuration Auditor software provides documentation that greatly simplifies and expedites the audit process. Systems may be organized within HTML format documentation by prioritizing systems through precedence, easing location of prominent and/or sensitive systems. System function classes, by department or other methods within the organization, may then influence the order of resulting documentation trees. Documentation servers are available which allow authenticated access by end-users to relevant documentation, which permits group-based creation and management of documentation with unwavering consistency, centralized control, and supervisory oversight.

Using Configuration Auditor's Change Management and Scheduling Effectively

Ecora's Configuration Auditor software provides options in scheduling and differential comparisons of configurations. Change Management, in its most elemental form, provides a quick analysis of configuration changes between two documentation sets. This exposes modifications and unintended configuration problems or changes instantly. New environments can be developed to precisely duplicate existing implementations and, conversely, proven environments can be replicated more accurately in the field with documentation and the Change Management function.

Baseline documentation sets can be created and implemented as a standardized reference utilizing the Change Management function. Quickly discover which systems do not comply with standardization and which parameters require adjustments. With scheduling options enabled at specific intervals, comprehensive change management can occur. With a quick reference through the Change Management option, systems can be regularly monitored for parameters that deviate from acceptable values.

Summary

A vulnerability can result in disclosure, destruction, or modification of data, and the degradation, mis-delivery, or denial of an intended service, whether inadvertent or purposeful. The likely result from such a compromise includes loss of customer confidence, significant monetary loss, and the loss of productivity. Recovery expenses cannot be readily measured, as consequential damages linger. How do you quantify the value of confidentiality, availability, integrity, or an organization's credibility?

The Computer Security Institute and FBI recently collaborated on a report detailing financial losses due to Internet intrusions, trade secret theft and other cyber crimes, known as the Computer Crime and Security Survey. This survey, while sampling only a small population, clearly demonstrates the soaring costs involved. Accompanying the survey is a projection that the likelihood of security breaches has grown sharply, and that this growth will continue. Their report is available online at: http://www.gocsi.com/prelea_000321.htm

You can quickly and easily implement configuration management controls across the existing network, with baseline comparative documentation a prerequisite "occupancy permit" for the introduction of new systems. Regularly perform enterprise-wide mapping and scanning to ensure compliance with new system introduction and existing controls. Develop a program to reduce the chance that newly deployed applications will introduce unexpected vulnerabilities, and test regularly for unauthorized installations.

Ecora's Configuration Auditor software is certain to compare quite favorably with many of the traditional methods found within the IT assessment process. Personnel-based interval assessments of this nature are prohibitively expensive for nearly any IT budget.

Improving Enterprise Security with Ecora's Configuration Auditor

This is an effective tool for managing risk. If only judged by its inherent audit and assessment value, significant savings can be realized with Ecora's Configuration Auditor. A call to your Ecora sales representative will produce many more factors, including a cost justification analysis (suitable for demonstration and ammunition) that will surely surprise you. Even the most conservative estimates expose real value in an automated audit and documentation tool.

Cressida Technology Ltd. t +44 1483 23 93 00
84A Meadow f +44 1483 23 93 83
Godalming, Surrey e info@cressida.info
GU7 3HT, UK w www.cressida.info



Ecora Configuration Auditor – Cost Savings and Cost Avoidance:

Enhance security:

An interval-based (cyclic) audit process must be considered for any IT risk management strategy. A proactive internal process holds the most promise for future security considerations.

Improve the ability to maintain a system:

Maintenance investments (personnel, experience, and components) are more readily available. Ease of maintenance is relevant to both software and hardware.

Eliminate duplication and unnecessary assets:

Expose multiple, incompatible, or dispensable stand-alone services.

Improve reliability:

Systems will show improved MTBF (less downtime) compared with legacy processes. Reductions in downtime inversely impact productivity and may also reduce labor costs.

Accommodate increases in workload or demand without additional costs:

Avoid hiring additional personnel or survive with reduced staff. Handle an increased workload or the emergence of new regulation driven responsibilities in the future.

Reduce manual operations:

Automation of manual processes frees staff resources to perform other functions. Permit this function to be performed by lower level staff.

Improve efficiency:

Improve access to information while decreasing time required when performing daily functions. It provides faster and more accurate aggregation and analysis of system configuration data.

Facilitate ease of use:

Although accessible, user-friendly methods are generally thought of in terms of increased efficiency or productivity, they can also improve the social and physical environment for employees.

Improve response rates:

Reduce stress by improving administrator's ability to respond to problems more easily.

Recent Regulations and Proposals:

Gramm-Leach-Bliley Financial Services Modernization Act:

- Create written policy approved with the oversight of the board of directors
- Employ generally accepted security practices
- Perform risk assessment and respond to emerging changes
- Perform regular security tests
- Provide written assurance from third-parties of security procedures and policies
- The GLB Act encompasses Financial, Insurance, and SEC-related industries

HIPAA: Health Insurance Portability and Accountability Act

<https://www.ecora.com/ecora/medium/>

Computer Security Act of 1987

Public Law 100-235 (H.R. 145) January 8, 1988

<http://www.cio.gov/docs/csa.htm>

Security of Federal Automated Information Resources

http://www.cio.gov/docs/Appendix_III.htm (April 14, 2001)

Guidance on Implementing the Government Information Security Reform Act

http://www.cio.gov/docs/Security_Act_Memo_and_Guidance.htm (April 16, 2001)

Children's Online Privacy Protection Act of 1998 (COPPA)

Children's Internet Protection Act (CIPA)

The Buckley Amendment:

The Federal Education Records and Privacy Act (FERPA)

The Federal Trade Commission (FTC) is closely monitoring online businesses and transactions. Of primary concern is privacy and accountability. Self-regulation is considered by many to be a failure. Regulation is presently under consideration.

Canada, the European Union, and Japan have all initiated privacy and accountability standards through law. This can present additional liabilities to those involved in export and import as business information regularly traverses these borders.