Dr. Anton Chuvakin @ Security Warrior Consulting

Consulting Services Summary

Updated: February 2010

Introduction

Security Warrior Consulting provides strategic consulting services focused on Security Information and Event Management (SIEM) and log management strategy and implementation, security product positioning and security content development.

Various options such as time and materials (with initial estimates), fixed price (with defined deliverable) or staff augmentation (fixed number of hours per week) are available.

Technology Vendor Services

This section of the services menu applies to security vendors and security services providers. The focus is on security and compliance strategy for product planning, development and marketing as well as on research and content development.

- Product management and strategy
  - Review **security product compliance strategy**, PCI DSS strategy and optimize them for the market
  - Perform market assessment and analysis, competitive analysis, product strategy (build/ buy/ partner); **prepare Market Requirements Documents (MRDs)**
  - Help develop and refine **security product marketing and positioning** messages, focused on compliance and new threats
  - **Augment internal Product Management staff** for strategic security and compliance projects, use case analysis, product definition, Product Requirement Documents (PRD) development
  - Work with product management to help **define and prioritize product features** based on market feedback and compliance requirements.
- Research and content development
  - **Lead content development** for whitepapers, “thought leadership” documents, research papers and other messaging documents, related to security and regulatory compliance
  - **Review security and compliance marketing materials**, site contents and other public- or partner-facing materials
  - **Create correlation rules, reports** as well as policies and procedures and other operational content to make SIEM and log management products more useful to your customers

    - **Map regulatory compliance controls** such as PCI DSS (key focus!), HIPAA, NERC, FISMA, NIST, ISO, ITIL to security product features and document the use of the product in support of the mandates
    - **Develop compliance content** such as reports, correlation rules, queries and other relevant compliance content for security product.
- Events and webinars
    - **Prepare and conduct thought leadership webinars**, seminars and other events on PCI DSS, log management, SIEM and other security topics.
- Training
    - **Prepare and conduct customized training** on log management, log review processes, logging “best practices”, PCI DSS for customers and partners
    - **Develop advanced training on effective operation and tuning of SIEM and log management tools** to complement basic training.

End-user Organization Services

This section of services menu applies to end-user organizations. The main theme is related to planning and implementing logging and log management for security and compliance.

- Log management and Security Information and Event Management (SIEM) product selection – how to pick the right SIEM and logging product?
  - Develop log management or **SIEM product selection criteria**
  - Identify key use cases **aligning log management and SIEM tools with business, compliance and security requirements**
  - **Prepare RFP documents** for SIEM, SEM, SIM or log management
  - **Assist with analyzing RFP responses** from SIEM and log management vendors
  - **Evaluate and test log management and SIEM products** together with internal IT security team
  - **Advise on final product selection**
- Logging and log management policy – how to develop the right logging policy? What to log?
  - **Develop logging policies and processes**, log review procedures, workflows and periodic tasks as well as help architect those to solve organization problems
  - **Interpret regulations and create specific and actionable logging system settings**, processes and log review procedures (*example: what to log for PCI DSS?*)
  - **Plan and implement log management architecture** to support your business cases; develop specific components such as log data collection, filtering, aggregation, retention, log source configuration as well as reporting, review and validation
  - **Customize industry "best practices"** related to logging and log review to fit your environment, help link these practices to business services and regulations
  - **Help integrate logging tools** and processes into IT and business operations
- SIEM and log management product operation optimization – how to get more value out of the tools available?
  - **Clarify security , compliance and operational requirements**
  - **Tune and customize SIEM and log management tools** based on requirements
- Content development – how to create SIEM content useful for you?
  - **Develop of correlation rules, reports** and other content to make your SIEM and log management product more useful to you and more applicable to your risk profile and compliance needs

    - **Create and refine policies, procedures and operational practices** for logging and log management to satisfy requirements of PCI DSS, HIPAA, NERC, GLBA, FISMA, ISO, COBIT, ITIL and other regulations
- Training – how to get your engineers to use the tools best?
    - **Provide the customized training** on the tools and practices of log management for compliance, IT operations, or security needs
    - **Develop training on effective operation and tuning of SIEM and log management tools** to complement basic vendor training.
- Incident response artifact analysis
    - **Analyze logs and other evidence** collected during security incident response

Recently Completed Projects

- Development of PCI DSS-focused application logging strategy, log review policies and procedures and daily operation tasks (excerpt from Statement of Work)
- Security vendor strategy assessment, focused on compliance, competitive strengths and weaknesses and new strategy ideas (excerpt from SoW)
- Comprehensive whitepaper on SIEM and log management architecture (excerpt from SoW)
- Complete definition of a log analysis product, from market assessment to product requirements (excerpt from SoW)
- Development of comprehensive training program on SIEM and log management, use cases, compliance (excerpt from SoW)
- Security market segment assessment, opportunity discovery and strategy tips for security vendor (excerpt from SoW)
- Thought leadership webinars for key security vendors (example)

Why Security Warrior Consulting and Dr. Anton Chuvakin for SIEM and Log Management?

- Many years of experience at leading SIEM and Log Management vendors in strategic and technical roles, developing the products, defining their roadmap and strategy and helping key clients
- SANS Institute called Anton "probably the number one authority on system logging in the world" (SANS Institute, 2008)
- Experience developing training on log management for SANS Institute.
- Working with strategic Fortune 500 clients as IANS Institute faculty.
- Recent consulting client said: "We hired Anton to help us operationalize our infant log management practice and he went beyond the call of duty. Anton is a great professional with foresight and a keen interest in what his client is after. He has a talent in bringing people together and forcing them to go beyond just being compliant and move towards the goal of being security."
- Invited speaker on SIEM and Log Management at leading industry events
- Author of dozens of papers on SIEM, correlation, data analysis and log management
- An author of the upcoming book on practical security log management.

Contact Information

Dr. Anton Chuvakin
Email: anton@chuvakin.org
Phone: 510-771-7106
Skype: *anton.chuvakin*
Twitter: @anton_chuvakin
Site: http://www.chuvakin.org
Blog: http://www.securitywarrior.org
LinkedIn: http://www.linkedin.com/in/chuvakin