AN EIS BUILDS A COMMON OPERATING PICTURE & SITUATIONAL AWARENESS

Graham Tech White Paper:
Executive Information System

GRAHAM
TECHNOLOGIES

TABLE OF CONTENTS

ABSTRACT

An Enterprise EIS system can be used to create situational awareness (SA) and a common operating picture (COP) in nearly any complex environment. In this case, we applied EIS to IT system management so that a number of stakeholders could effectively work to combat cybersecurity threats.

Government agencies are working to improve cybersecurity in the face of a torrent of new threats. Agency IT systems can be complex and consist of multiple subsystems that may or may not be integrated. Visualizing the status and security posture of these systems is a critical first step toward helping stakeholders assess, prioritize and address cybersecurity vulnerabilities.

Graham Tech's EIS is an effective framework for aiding decision-makers in this and other complex, rapidly evolving situations. Here we describe the approach and impact when applied to the challenge of cybersecurity in a complex IT environment.

The Graham Tech EIS helped stakeholders:

1. Integrate disparate information from across multiple sources.
2. Understand the geospatial components and implications.
3. Visualize data patterns and trends.
4. Create a Common Operating Picture for stakeholders to focus on.
5. Aid in situational analysis and decision-making.

Graham EIS integrated data from multiple disparate systems to provide intuitive data visualization and situational awareness for stakeholders working to address cybersecurity concerns.

Customizable dashboards increased collaboration, and pattern & trend analysis. This helped decision-makers quickly understand the situation and to use their expertise, collaboration, and intuition to develop faster, higher-confidence decisions to mitigate cybersecurity threats.

The Graham Tech EIS system continues to provide key performance indicators and metrics regarding security threats, enabling leaders to make informed decisions in real-time.

A similar approach can be taken to track assets in the field, evolving battle conditions, epidemiological information and more. This implementation created significant value for the client, while serving as a powerful proof of concept for other problem spaces.

The U.S Director of National Intelligence ranks cybercrime as the number one national security threat, ahead of terrorism, espionage, and weapons of mass destruction. There have been over 445 security breaches of state, local and federal government agencies since 2014, with the number of breaches climbing in 2018 and 2019.

INTRODUCTION

We are inundated with data to help make decisions. However, acquiring this data is only part of the battle for more informed quantitative decision making. Data must be processed, analyzed, and visualized to provide maximum value, while the data is still relevant and useful.

Raw (unprocessed) data reports may provide some important insight for making strategic decisions, but data relationships, patterns, and trends analysis, along with threshold alerting, quarantining, automated recommendations, and pertinent data visualization is what provides the greatest benefit to informed decision making.

Consider these consistently mentioned customer pain points:

- Over 61,000 security breaches in 2015
- Cyber products do not integrate with existing systems
- High-level executives can't make key decisions to mitigate cyber threats

Given these customer pain points and the need to enhance informed decision making, Graham's EIS application provides a solution to manage and inform on organizational IT systems. EIS supports the administration of system security policies, controls, risks, assessments, and weaknesses, offering an assessment of system security postures for enterprise governance, risk, and compliance management & collaboration.

PROBLEM DEFINITION

There is an industry need to gain advanced oversight into enterprise governance, risk, and compliance to enhance decision making for upper management. In addition to drawing from experience and intuition, leadership needs tools and technologies that assist with making informed decisions for proactive business management.

Graham has identified its top customer challenges and resolution in Appendix A. This whitepaper focuses on this subset of challenges and resolutions:

1. High volume data processing,
2. Data analytics for automated insight,
3. Meaningful data visualization and
4. Poorly engineered IT solutions can't easily be maintained and adjusted to meet future business requirements

Technology can be a great accelerator for accessing and utilizing information to inform and collaborate. It can also be costly, non-extensible, non-interoperable, slow-paced through the software development life cycle, and difficult to use and understand.

Graham solves these challenges using streamlined solution processes, enhanced product workflows, state-of-the-art open-source technologies, and innovative custom development.

SOLUTION

An automated EIS eGRC (electronic Governance, Risk, Compliance) tool allows system owners, information system security officers (ISSOs), privacy officers, and security analysts to easily identify system weaknesses and potential issue resolutions for improved efficiencies and cost savings.

Graham used the following methods to advance security posture insight and solve the challenges of high-volume data processing, data analytics for automated insight, meaningful data visualization, and the development of less-ridged IT solutions:

1. **High volume data processing:** To process high volumes of data efficiently, Graham used frameworks including Hadoop and MapReduce. These frameworks make it possible to run applications on systems with thousands of nodes involving thousands of terabytes of data. Its distributed file system facilitates rapid data transfer rates among nodes and allows the system to continue operating uninterrupted in case of a node failure. When processing the data, an application is broken down into numerous small parts. Any of these parts can be run on any node in the cluster.

2. **Data analytics for automated insight:** EIS's Geospatial Information Systems (GIS) Google Maps feature provides system assists by telling a visual story of continuity of operations for such things as recently affected natural disaster areas. EIS correlates all devices within a given system and monitors device and map thresholds to alert of undesired status and risk.

3. **Meaningful data visualization:** EIS provides an innovative modern dashboard application with an integrated repository to facilitate real-time approval, monitoring, and reporting for multiple enterprise systems. Our application is user-friendly and high performing, including:

   a. Consistent site layouts, visually appealing look-&-feel, search and tag data, dynamic, asynchronous page-region refreshes, GIS Google Maps displays, and dashboards for fewer keystrokes to gain access to data

   b. Compliance with Section 508 (accessibility) and ISO 16982:2002 (human-centered usability).

   c. Interoperability with web servers and web browsers

   d. REST JSON-based web services for server exchange, adhering to function signature name and type controls to maintain the ability to adjust underlying code without negatively affecting the users of that function

   e. A discoverable API via URI exchanges for machine-readable API descriptions and operations, and HTML5 front-end code for desktop and mobile browser rendering

   f. User-generated content with social media hooks such as wikis, forums, blogs, and feedback

4. **Graham uses Agile (SCRUM):** for easily adjustable and quick feature turnarounds within the software development life cycle (SDLC). This project management methodology promotes:

   a. Cyclical user engagements that analyze, decide, and provide early feedback for the overall solution and project goals and requirements (epics, user stories) to steer solution success.

   b. Cyclical project team evaluations manage requirement & task level of effort, decomposition, story points, risk, and clarification requests on a smaller scale; and then use previous iterations to help plan and guide the current iteration.

   c. Agile team planning and evaluations for cyclical requirements prioritization, assessment, demonstrations, progress tracking, promotion decision, and introspections.

SOLUTION (CONTINUED)

Factors for Successful Execution

Our project team solutions manage traceability from goals down to implementation tasks; and between design, test, code, integrate deployment decisions, and bugs. Our Capabilities Maturity Model Integration (CMMI) III project processes and procedures ensure processes are repeatable, effective, and efficient.

We follow proven industry standards such as World Wide Web Consortium's (W3C) web standards, Institute of Electrical and Electronics Engineers (IEEE) sharing standards, Representation State Transfer (REST) web service integration, and JavaScript Object Notation (JSON) data transfer standards, UI section 508 and ISO 16982:2002 compliance, NIST SP 800-60 data types, defining a Federal Information Processing Standard (FIPS) 200 security controls baseline (access control, incident response, business continuity, and disaster recoverability), NIST SP 800-53 security controls and assessment procedures, Department of Defense Architecture Framework v2.0 (DoDAF), Software Engineering Institute's (SEI) Capability Maturity Model Integration (CMMI) Maturity Level (ML) 3 processes, ITIL project management.

BUSINESS BENEFITS

Graham designed and implemented this and other dashboards from requirements to design, execution and solution satisfaction. We used industry standards and proven processes and practices to enhance consistency, interoperability, extensibility, and rapid solutions maturity to meet cost, schedule, and quality goals.

Graham's EIS tool accomplishes the following high-level business goals:

- **Dashboard Views:** A modern dashboard application with an integrated repository to facilitate real-time approval, monitoring, and reporting for multiple enterprise systems. The dashboard views roll-up and consolidate incident and risk-based information to allow leadership to make informed data-driven decisions.
- **Maintain Engineering Principles:** These include availability (there-when-needed), accessibility (can easily access it), adaptability (easily modifiable w/ minimal refactoring; easily extendable with future code/technologies), portability (not confined to one host/platform/environment) and compatibility (integrates well with other components/solutions).
- **Advanced Security & Risk Management:** Supports the risk management framework (RMF) tasks and activities to measure compliance and manage risk. Maintain system information related to the security controls listed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." Supports current and future NIST requirements for security authorization, including, but not limited to, the Federal Risk and Authorization Management Program (FedRAMP) and NIST SPs, as applicable.
- **Integration:** Maintains a central repository for organizational and partner agency digital assets.
- **Data Analytics:** Collects & analyzes patterns and trends within data regarding enterprise information systems, including vulnerabilities, configuration standards, audit logs, hardware, and software inventories.
- **Monitoring & Reporting:** Enables the integration of security-authorization and system-stability related continuous monitoring.
- **Documentation:** Generates the documentation required throughout the process to enable reapplication or adjustment to future processes and methods of a similar nature. Documentation should happen as unobtrusively to the administrators and end-user as possible yet suffices for all roles to interact with the products effectively.

BUSINESS BENEFITS (CONTINUED)

Rapid Prototyping

Graham employs rapid prototyping and system development utilizing a more efficient Agile development & management approach, coupled with cost-effective and ease of integration for cutting edge technologies.

Requirements traceability is maintained throughout the entire SDLC to ensure the delivery of customer valued solutions. Program plans, including development, build, release, and verification schedules, are traced to the specific requirements that are addressed. Our continuous integration approach results in better capabilities, shorter delivery cycles, and lower cost.

In addition, this Agile development methodology also reduces the risk of late-stage adverse issues and requirements misunderstandings, which greatly enhances and contributes to our solution's verification & validate success.

Effective system integration services with well-defined service level agreements (SLAs) and common application programming interfaces (APIs) using standards such as XML, enable our systems to integrate and share data for enhanced interoperability.

Our processes leverage service-oriented architecture (SOA) which eliminates redundant investments while enabling better justifications for new IT systems integration and technology adoption. Our approach to enterprise architectures promotes increased levels of mission effectiveness and interoperability by standardizing the development and use of architectures within and between organizations, including principles for eliminating waste and duplication, increase shared services, close performance gaps and promote engagements among partners. Our SOA approach enables EIS solutions to assemble from a collection of interacting services and exchange information.

CONCLUSION

Leadership teams need an executive information system to manage and collaborate on system security policies, controls, risks, assessments, and weaknesses. The ability to review and assess system security postures and to make informed decisions on enterprise governance, risk, and compliance within a single collaborative online tool is critical.

Graham's Executive Information System (EIS) - Enterprise Governance, Risk, and Compliance (eGRC) application provides leadership teams with the insight and analysis needed to make informed security posture decisions. In addition, EIS demonstrates Graham's ability and capabilities for developing innovative IT solutions.

Graham's IT solutions approach uses proven open-source products, industry-standard exchange formats. Our Agile development model enables our partners to integrate with our system, promote reusability and increase the sharing of data using interoperable systems.

WHY PARTNER WITH GRAHAM?

Graham has over ten years of industry experience, providing enterprise solutions to IT challenges. Graham's proven processes, technical staff, and advanced technology solutions are the perfect combination to assist with the challenges inherent in improving enterprise governance, risk, and compliance.

We welcome the opportunity that comes with assisting our customers solve tough IT challenges and enjoy the personal satisfaction that results.

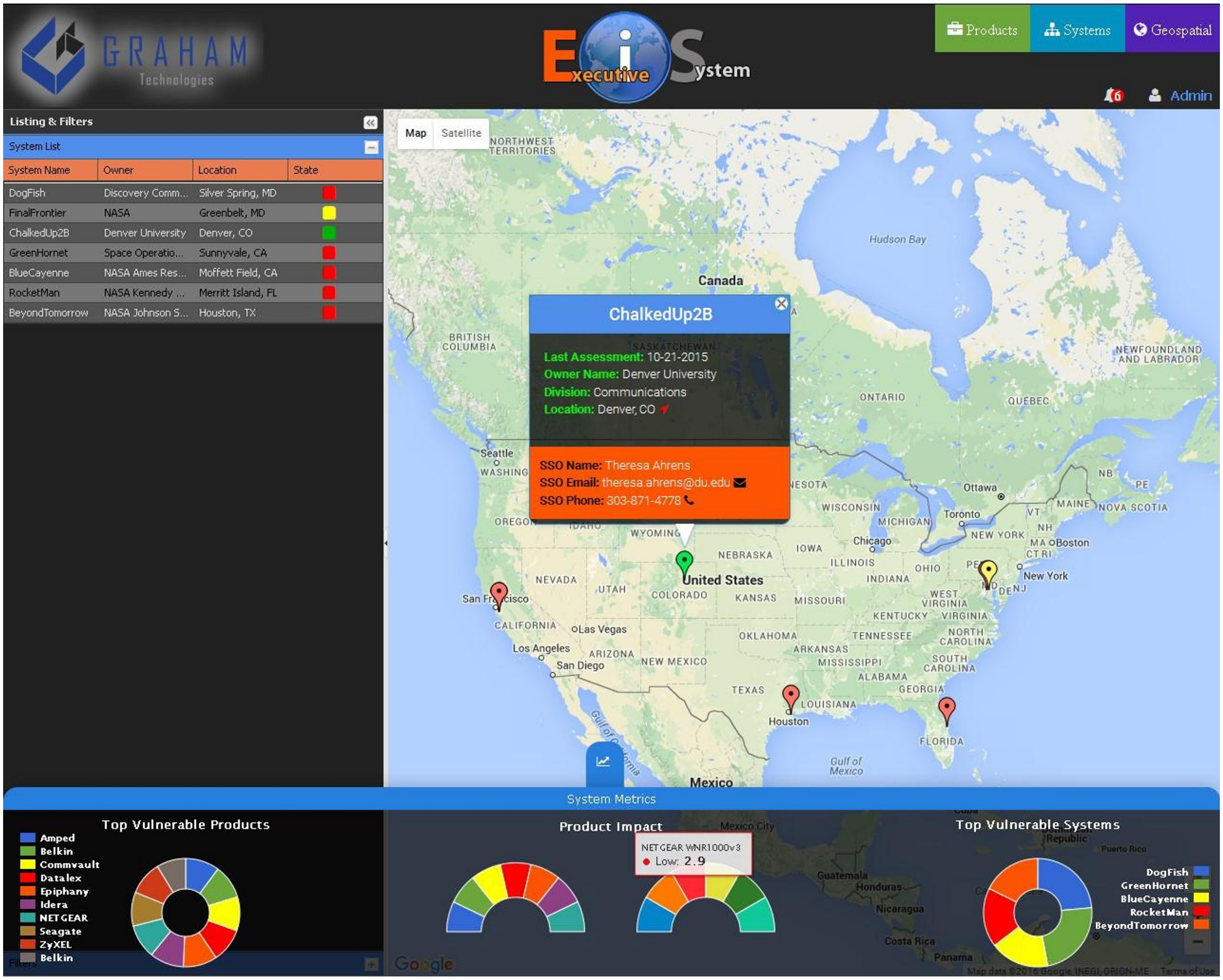
Graham is uniquely positioned with organizational discriminators and technical solutions to address the most disruptive and prolific industry issues as outlined within this document. Our discriminators include project policy, governance, and oversight, Agile operational effectiveness, software developing, system management, data analytics, workflow engineering and streamlining, systems architecture of hybrid solutions construction, system-agnostic interoperability and integration solutions, geospatial visualization, quality management, and improvement, security controls administration, database and data management for information accuracy, consistency, and quality through data validation, quality reviews, and knowledge sharing, alerts and reports, and enhancement and defect management.

Graham Technologies is a company that provides Information Technology (IT) and engineering support services. Graham Technologies is an ISO 9001:2008 and CMMI Level II certified company that mandates quality control disciplines internally, as well as externally on every aspect of each project engagement. Graham possesses over twenty years of information technology experience in providing services and solutions to a wide variety of government agencies. Through superior IT support services and application modernization, Graham has assisted customers in achieving their respective goals and objectives, increasing their return on investment (ROI) and maintaining efficiency and effectiveness of their information technology systems.

In business since 2007, Graham is an innovative, agile, full service IT services firm headquartered in Largo, Maryland.

For more information on Graham's solutions and services, please visit **www.graham-tech.net** or contact **William.graham@graham-tech.net**.

APPENDIX A: EIS COMMON OPERATING PICTURE



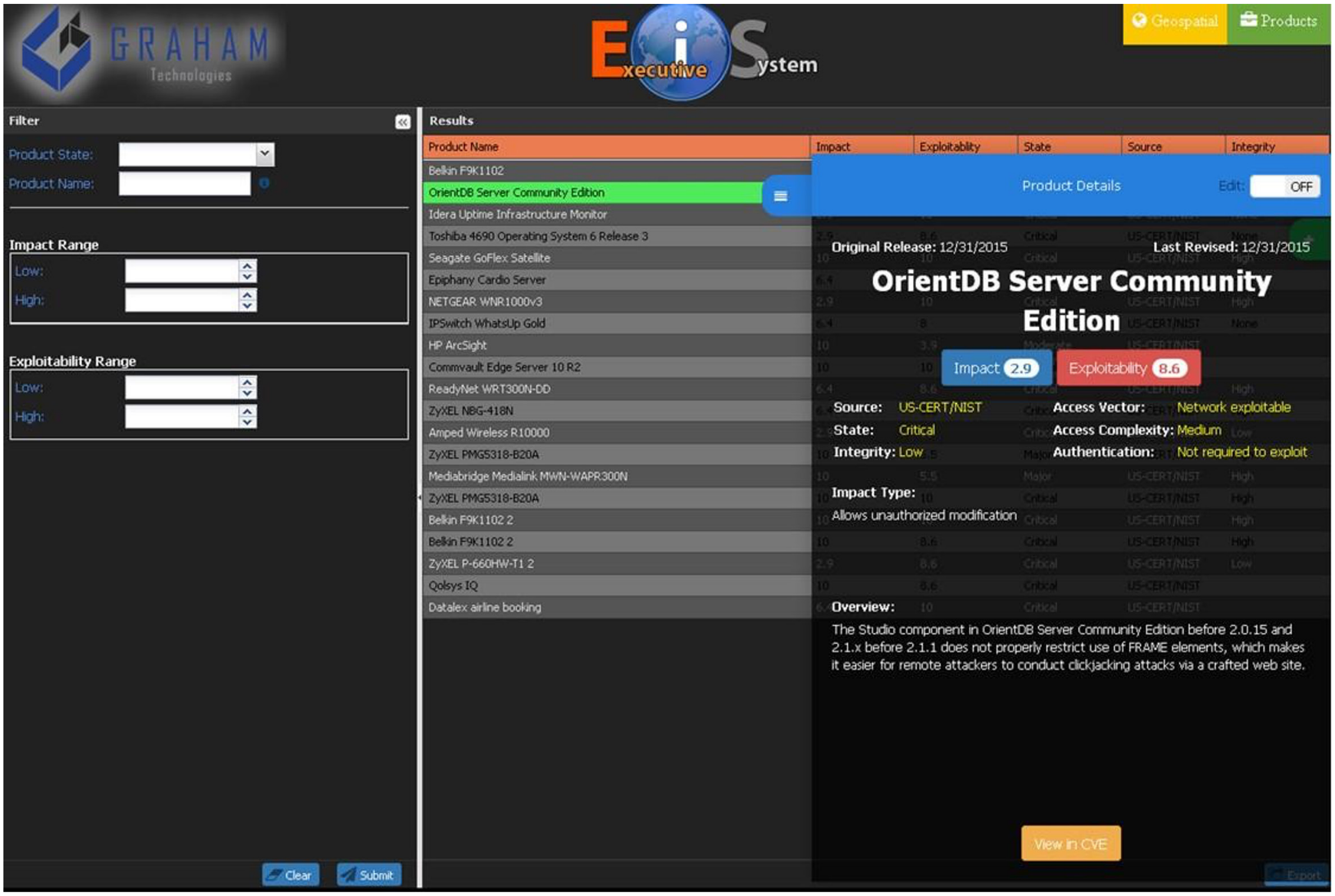
System List

System Name	Owner	Location	State
DogFish	Discovery Comm...	Silver Spring, MD	🟥
FinalFrontier	NASA	Greenbelt, MD	🟨
ChalkedUp2B	Denver University	Denver, CO	🟩
GreenHornet	Space Operatio...	Sunnyvale, CA	🟥
BlueCayenne	NASA Ames Res...	Moffett Field, CA	🟥
RocketMan	NASA Kennedy ...	Merritt Island, FL	🟥
BeyondTomorrow	NASA Johnson S...	Houston, TX	🟥

ChalkedUp2B

Last Assessment: 10-21-2015
Owner Name: Denver University
Division: Communications
Location: Denver, CO

SSO Name: Theresa Ahrens
SSO Email: theresa.ahrens@du.edu ✉
SSO Phone: 303-871-4778 ☎



Product State:

Product Name:

Impact Range

Low:

High:

Exploitability Range

Low:

High:

Product Name

Belkin F9K1102

OrientDB Server Community Edition

Idera Uptime Infrastructure Monitor

Toshiba 4690 Operating System 6 Release 3

Seagate GoFlex Satellite

Epiphany Cardio Server

NETGEAR WNR1000v3

IPSwitch WhatsUp Gold

HP ArcSight

Commvault Edge Server 10 R2

ReadyNet WRT300N-DD

ZyXEL NBG-418N

Amped Wireless R10000

ZyXEL PMG5318-B20A

Mediabridge Medialink MWN-WAPR300N

ZyXEL PMG5318-B20A

Belkin F9K1102 2

Belkin F9K1102 2

ZyXEL P-660HW-T1 2

Qolsys IQ

Datalex airline booking

Product Details

Edit: OFF

Original Release: 12/31/2015

Last Revised: 12/31/2015

OrientDB Server Community Edition

Impact 2.9

Exploitability 8.6

Source:	US-CERT/NIST	Access Vector:	Network exploitable
State:	Critical	Access Complexity:	Medium
Integrity:	Low	Authentication:	Not required to exploit

Impact Type:

Allows unauthorized modification

Overview:

The Studio component in OrientDB Server Community Edition before 2.0.15 and 2.1.x before 2.1.1 does not properly restrict use of FRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks via a crafted web site.

GRAHAM
TECHNOLOGIES

Headquarters
1401 Mercantile Lane
Suite 301
Largo, MD 20774

Phone: (240) 764-7899
Fax: (301) 560-6579
info@graham-tech.net

graham-tech.net