Calhoun: The NPS Institutional Archive

DSpace Repository

Acquisition Research Program | Acquisition Research Symposium

2020-04-27

Acquisition Data Analytics for Supply Chain Cybersecurity

Maule, Randy

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/64761

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

SYM-AM-20-057

PROCEEDINGS
OF THE
SEVENTEENTH ANNUAL
ACQUISITION RESEARCH SYMPOSIUM

Acquisition Research:
Creating Synergy for Informed Change

May 13–14, 2020

Published: April 13, 2020

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Data Analytics for Supply Chain Cybersecurity

Randy William Maule—has been with the Naval Postgraduate School since 2000, serving as naval and joint forces enterprise developer, knowledge manager, and technical analyst in joint forces and coalition exercises where he has conducted systems test and measurement. His enterprise is tool suite and measurement architecture operated on ships, in maritime and network operations centers, and in forward-deployed commands for nearly 15 years. Prior to this, he spent 10 years in Silicon Valley high technology industries working with intelligent networks and service architecture, and prior to this developing enterprise knowledge systems and AI at a federal supercomputer center. [rwmaule@nps.edu]

Abstract

Cybersecurity is a national priority, but the analysis required for acquisition personnel to objectively assess the integrity of the supply chain is highly complex. This paper presents a process for supply chain data analytics for acquisition decision-makers, addressing data collection, assessment, and reporting. The method includes workflows for acquisition decision support from initial purchase request through vendor selection and maintenance across the life cycle of an asset. The research presents options for analysis, analytic tools, results visualization, and artificial intelligence to help acquisition decision-makers manage the complexity of supply chain management.

Research Objective: Discuss platforms, techniques, systems, tools, and workflows to empower acquisition departments for supply chain data management with analytics for cybersecurity compliance and information assurance.

Research Questions: Can tools for supply chain data analytics and results visualization be integrated into acquisition workflows to address information assurance across the supply chain? Will information assurance audit models be sufficient for acquisition departments to implement cyber controls in the purchase process and across the supply chain?

Introduction

The analysis required for acquisition personnel to objectively assess the integrity of the supply chain and cybersecurity for the technologies purchased through that supply chain is multifaceted and complex, requiring many different types of expertise. Such a role has not traditionally been the purview of acquisition departments. Yet, as the arbiter in purchase decisions across the life cycle of an asset, it may be logical to expand the acquisition role to accommodate such responsibilities, especially given failures in current approaches which tend to stovepipe cybersecurity, therein leaving gaps.

The common element across the life cycle of a technology—from initial requisition, through deployment and implementation, to contracting for technical support and maintenance—is the acquisition role. However, this role does not have the resources or technical expertise to accomplish comprehensive and continuous cybersecurity assessment. Fortunately, new analytic methods and system resources, when coupled with artificial intelligence (AI), can support such an endeavor.

This paper presents a process for supply chain data analytics for acquisition decision-makers, addressing data collection, assessment and reporting. The method includes workflows for acquisition decision support from initial purchase request through vendor selection and maintenance across the life cycle of an asset. The research includes a discussion of integrity analysis, data analytic tools and report methods with visualization, and AI to help acquisition decision-makers manage the complexity of supply chain cyber and information assurance.

Background

Naval and joint forces systems analysis has identified significant risks within the supply chain (Military & Aerospace Electronics, 2020; Villasenor & Tehranipoor, 2014). Compromised chips, manufacturer and vendor selection, and post-purchase systems maintenance all contribute to the problem. Previous research established a framework to extend the acquisition role to supply chain management with security audits across the life cycle of a system (Maule, 2019a, 2020a). As a budget authority, the acquisition role is logically positioned to oversee the supply chain—from initial requisition to maintenance contracting. The complexity of the task and multiple levels of technical expertise required can be mitigated through software.

AI integrated into acquisition decision support systems provide a solution. This would involve automation of the test and measurement process, together with expert systems for equipment, vendor, and contract selection. Results would be rendered into a dashboard for easy understanding by acquisition decision-makers. This paper continues previous research in this area and advances a method to operationalize the decision support components of the previously established framework and workflow.

Acquisition

Previous research established variables and metrics for supply chain cybersecurity assessment from purchase request, through vendor selection, to maintenance audits (Maule, 2019b, 2020a). An “analytics grid” or distributed service architecture for systems assessment was successfully deployed to afloat and shore commands to evaluate new technologies and system upgrades for more than a decade (Maule & Lewis, 2010, 2011). The next step would be to extend such capabilities to the acquisition role where cybersecurity may be addressed from a budget perspective. The method advances multidisciplinary research to evaluate all variables that were found to impact the validity of naval systems and data under operational load (Maule, 2015, 2016, 2017).

Something to note is the relationship between systems, components, and other systems is typically nonlinear. It is not possible to precisely define the inputs such that there is a direct relationship to the outputs. Cause–effect relationships are probabilistic and can be determined only within technical, operational, and environmental context. Additionally, systems performance tends to exhibit divergent patterns under stress—such as challenged communications, jamming, or electronic attack, and of course cyber and electronic manipulation. Similar to our naval experiments, the acquisition decision support software will need to address such contexts.

Adaptive systems are characterized by the capability to learn from experience. Machine and deep learning are an example and these tools that can be applied to help understand complex relationships. We observe adaptive behaviors in naval exercises as we instrument networks to monitor complex data flows across geographic regions. Components of systems interact, with the result of those interactions dependent on dynamic variables. For example, changes made as services adapt to tactical scenarios. Evaluation addresses the dynamic interplay of variables, in context, over time. Failure to address this complexity results in an inability to recognize performance variance or cyber compromise, or to adapt the analysis to changes in operational or environmental context.

This research therein advances digital tooling and analytic methods for supply chain integrity analysis to include data collection, results visualization, and decision support. The acquisition role is advanced as an arbiter of supply chain validity. AI tools integrated into acquisition workflows will help acquisition decision-makers address cybersecurity compliance and information assurance across the life cycle of an asset. Techniques are derived from lessons learned in naval, joint forces and coalition exercises, and industry best practices.

Decision Support

The level of decision support required for a task as complex as cybersecurity assessment throughout the supply chain and across the life cycle of an asset may be best realized through AI and automation. Probabilistic algorithms have been found to be effective in addressing multiple dimensions of analysis when contexts are dynamic and expanding (McMullen, 2015).

Figure 1 summarizes major trends that have evolved AI capabilities, beginning with the early works in general intelligence for computer decision support, to content (Goldberg et al., 1992) and group filtering (Resnick et al., 1994), to the recommender systems (Resnick & Varian, 1997) popular today in search and online transactions (Koren, Bell, & Volensky, 2008).

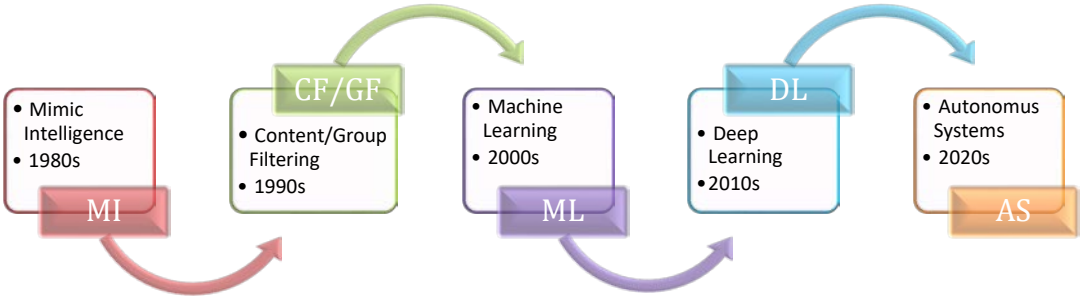

Figure 1. Evolution of AI for Acquisition Decision Support

A Department of Defense (DoD) example is the content filtering AI that we used on a daily basis for technology assessment in the naval exercises, integrating quantitative network and system technical measures with qualitative user analysis (Maule, Gallup, & Jensen, 2010). An extension of this AI to include machine and deep learning with autonomous collection and processing would provide support for an acquisition supply chain decision system.

Machine learning can add user behavior into the software development process, building capabilities by example rather than direct programming (Dietterich, 2003). The algorithms excel in settings where specifications for desired program behavior are not available but where examples of this behavior are available.

Figure 2 illustrates the different programming approaches. Expert systems, filtering, and intelligent decision support are facets of early AI but are still popular today in search engines and recommendation algorithms. Also, with a long history but more recent in practical application due to their costly processing requirements are machine learning and deep learning where we structure reinforcement and enable self-learning, respectively.

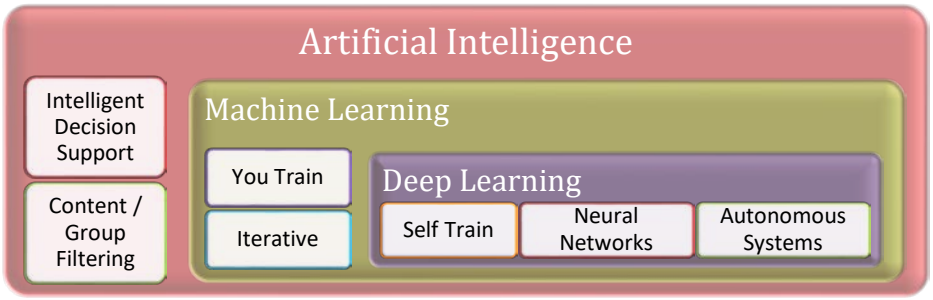

Figure 2. Machine and Deep Learning for Acquisition Decision Support

In machine learning, the algorithm is taught to make an accurate prediction. An operator provides guidance through positive and negative reinforcement—for example, to determine

whether an anomalous behavior has occurred, or a data synthesis is incorrect. Deep learning is a subset of machine learning that is even more computer-intensive. The algorithm learns to predict by itself using a brain-like artificial neural network structure but requires massive datasets (Farsal, Anter, & Ramdani, 2018) since the algorithms extract features independent of an operator (Microsoft, 2020). In machine learning, small amounts of data can be used to train the machine to make predictions, so it is more appropriate to begin this work. In recent tests we achieved more than 80% prediction accuracy with as few as a dozen data sets (Maule, 2020b).

Figure 3 provides an example of the machine and deep learning workflow, beginning with data collection and processing, applying the algorithm, then evaluating the results. If machine learning is employed the data is split in the training phase, generally about a 75/25 split—with the former training the model that is applied to the latter. The process iterates until the correct decisions are achieved.

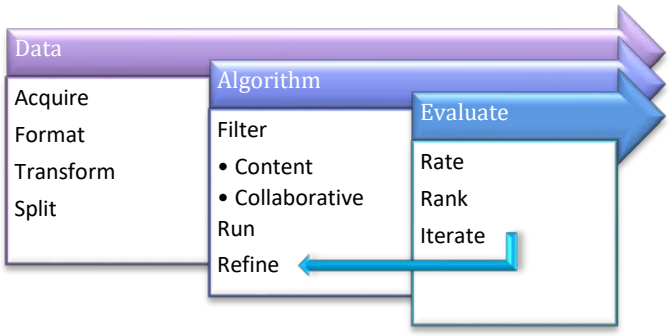

Figure 3. Decision Support Machine Learning Workflow

Applied to acquisition decision support is the additional benefit that through machine learning the necessary expertise from the multiple technical specializations required for comprehensive supply chain analysis can be modeled. So, models are trained by experts and then integrated into the decision support system. With the addition of deep learning. the models can independently evolve, continuously learning to improve decision support with ever more efficient predictions.

Method

The workflow begins with conceptual models and architecture, then procedures for technical assessment with tooling for data monitor and analysis. Applications address in-service audits for cybersecurity and information assurance, systems verification, and data validation. Technical models are integrated with audit workflows for comprehensive life-cycle systems assessment.

Data analytic tools appropriate for supply chain information assurance apply known capabilities, proven for test and measurement in the fleet. These tools are generally industry best-of-breed. Intelligent recommendation algorithms build upon knowledge management practices successfully applied in naval, joint forces, and coalition operations.

Collectively these techniques will help acquisition decision-makers from: (a) initial purchase request, to (b) vendor selection, through (c) implementation and maintenance. Artificial intelligence is advanced to assist data analytics and provide decision support.

Analytics

Previous research has established a workflow for acquisition supply chain audits (Maule, 2019a, 2019b, 2020a). The left side of Figure 4 illustrates this workflow, showing the pre-

acquisition process before and after cybersecurity enhancement (box “A”). Box “B” shows the addition of test and measurement (T&M) within the workflow for monitoring, maintenance, and compliance reporting across the life cycle of the asset.

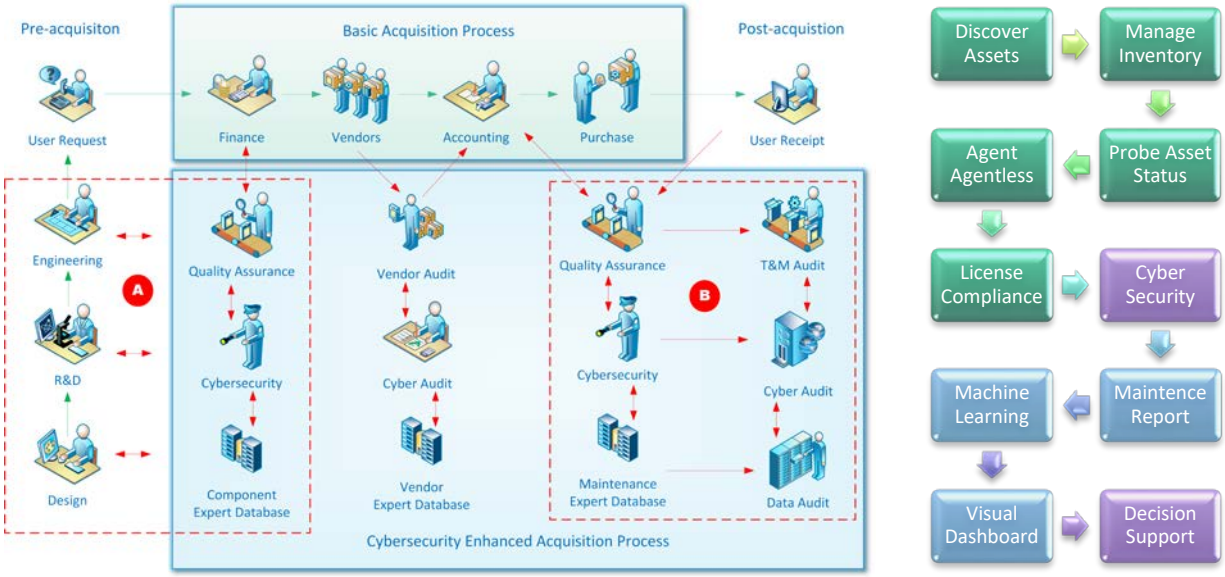

Figure 4. Acquisition Supply Chain Cybersecurity Rest and Measurement Workflow

On the right side of Figure 4 is the operationalization of the workflow that is the focus of this paper. Specifically, the process through which assets are discovered, analyzed for compliance, and decision support rendered. AI is presented as a means for asset management (intelligent agents), management of test processes, generation of results, and automation of the decision support process (machine learning).

Architecture

Analytic functions for large system environments typically involve the collection of system logs (SysLogs) that help determine the overall status of a system. After an incident has occurred, the SysLogs can be complied with other data to achieve a detailed understanding of the problem and context. SysLogs are correlated with communication logs from switches, routers, firewalls, and gateways for both radio frequency (RF) and wired connections.

The information environment is modeled and events correlated against the models for monitoring, detection and prediction. Fortunately, this process can be largely automated so that only high-level reports reach the acquisition decision-makers. Individual events typically have a drill-down into detail for root cause analysis.

Tools with this capability include application performance monitors (APM), information technology (IT) infrastructure monitors (ITIM), IT operations models, network performance monitors and diagnostics, and digital experience monitors (Rich, Prasad, & Ganguli, 2019). Figure 5 provides an example of the tools integrated into an architecture for data collection, analysis, and acquisition decision support.

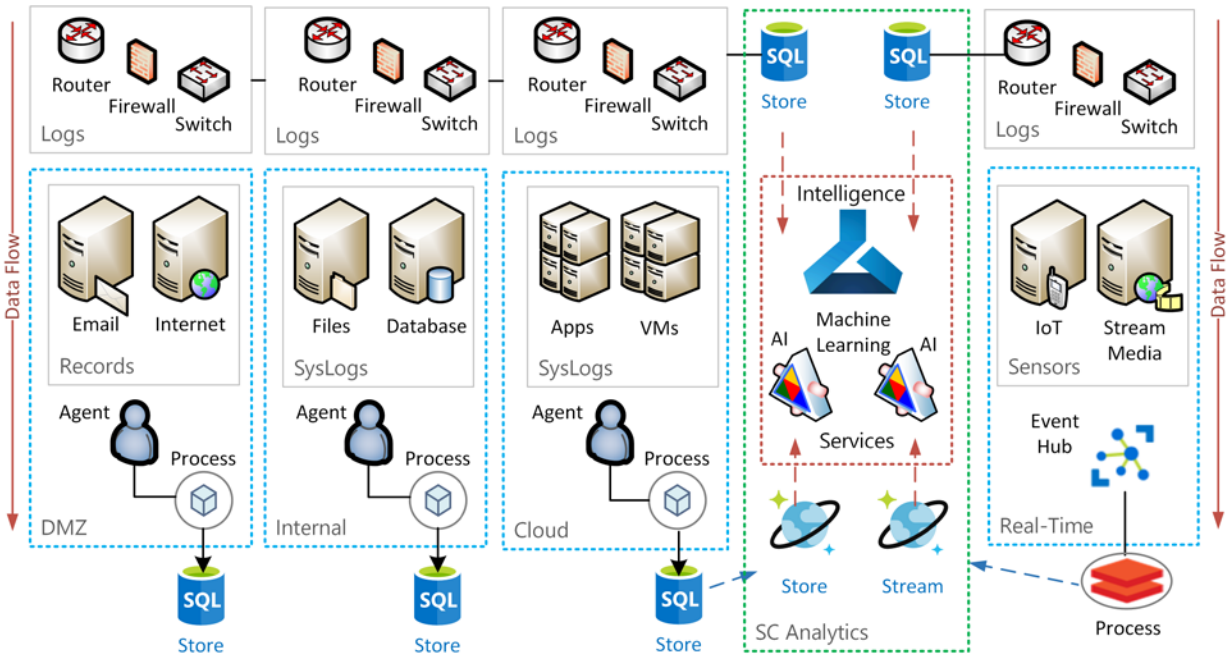

Figure 5. Acquisition Supply Chain (SC) Assessment High-Level Architecture

Communication analysis begins with data drawn from routers, firewalls, switches, gateways, and interconnection devices. Network tools aggregate metadata into storage and transfer data to analytic engines where events are correlated. Results are often visualized. The more expensive tools have multiple levels of built-in AI to evaluate patterns and detect anomalies. We can extract events of interest. In the full architecture, the network and server layers are replicated for each node in the enterprise. Each switch, and the devices that connect to that switch, are a node. So, in a large enterprise, there are thousands of nodes; hence the need for professional-grade tools. Firewalls and routers are usually shared across nodes/switches.

There are both agent and agent-less approaches to collect data. Both are automated but the systems onto which intelligent software agents are loaded tend to produce more insightful information. The more comprehensive analytic tools provide a tight linkage between report consoles and collection agents, with the agent not only collecting data but processing that data before storage or further processing. Agents are best for systems with access to the public Internet, for example in a demilitarized zone (DMZ) within a company. For the internal systems, as well to help detect cyber incidents, mission critical streaming services can use a tap and agent-less approach to not interfere with time critical data where milliseconds can make a difference. Cloud operations tend to be a cross between public and private, depending on the configuration and security controls.

On the far right are the real-time and streaming services, typically from sensors, video, audio, news feeds, and other just-in-time media. Internet of Things (IoT) and edge devices would be included, such as cell phones and other mobile devices. The intent here is for real-time analysis so the data is typically streamed through an event hub to a processing node configured with real-time analytics. Data is simultaneously streamed into the acquisition supply chain analytics.

In the analytics center various algorithms and machine learning capabilities are enacted to look for particular events or suspicious activities, machine anomalies or system failures, irregular data patterns or cyber intrusions, maintenance and protection alerts, etc. This is where

our acquisition supply chain management resources are housed, acting independently for the acquisition mission but reaching out into the enterprise. Table 1 categorizes some of the basic forms of analysis:

Table 1. Acquisition Supply Chain Analytic Algorithms

Incident	Analytics
System alarms	Clustering and pattern matching algorithms
Cause analysis	Decision trees, random forest, graph analysis
Abnormalities	Statistical, probabilistic analysis: univariate/multivariate analysis, correlation, clustering, classifying, extrapolation
Irregular patterns	Correlation/prediction from historical and/or streaming data through clustering or grouping
Context	Topology patterns displayed through graph data to establish relevance and hidden dependencies

Information assurance begins with contextual analysis of the data and visualization of the service environments. Alarms can be managed through clustering and pattern matching algorithms. Root cause analysis can be done through decision trees and graph analysis. Most professional collection and monitoring equipment have built-in AI for abnormality detection and provide a drill-down into events of interest (BMC, n.d.) so all we need is a means to aggregate the results to a decision portal and integrate those results into our supply chain decision process. Once this is done the decision support system can predict from those correlations. Additionally, many tools provide topology analysis with context to assess linkages and dependencies across applications, networks, and databases.

Traffic flows are monitored for protocols, devices, and users. Details on load, latency, errors, and sessions are analyzed. Suspicious events are correlated with SysLogs and user social media (chat logs, service requests, forum posts, etc.). Results are rendered into service dashboards for acquisition decision-makers, for example, to assess the need for proactive maintenance. System health status, alarm history, and usage metrics support the decisions.

Service dependency maps ensure client-server relationships and system integration contingencies are understood (NETSCOUT, 2019). Compliance can be attested, for example, ensuring the proper number of licenses are active. Power consumption can be integrated for cost-benefit analysis. Inventory reports can be generated for tracking, implementation, and maintenance and then, integrated with usage, cost, and life-cycle metrics. Device security can be monitored continuously, including for mobile devices. If cyber compliance is not in order, the devices can be locked or wiped (BMC, 2018).

Since intelligent analytics, machine learning, and other probabilistic techniques are prone to false positives, bias, and other errors, the supply chain analytics process will continuously test for efficiency; hence, the need for automation. Over time the machine and deep learning algorithms will improve to enable further automation—even to the point of being able to correlate seemingly non-connected events (Ixia, 2017).

Collection

T&M begins with asset discovery from sensors that are collecting information about technical, operational, and environmental factors that will impact supply chain analysis. For reference, we will assume a tactical application with live, deployed assets. Figure 6 presents the radio and network sensor monitors that provide the first step to understanding the context for our analysis. Sensors monitor the network devices in the architecture.

Figure 6. Spectrum Radio and Network Data Monitor and Capture

Sensors can be grouped by region and reported by mission. RF and network collection devices monitor and collect data for asset performance, interference, and cyber or electronic attack. The T&M tools will automatically discover/classify assets, determine data and network conditions, and analyze data usage patterns/users for potential risk.

AI techniques can be applied to learn normal patterns and therein spot abnormal behaviors, making judgments and predictions from deviant events. For example, to detect supply chain fraud or a cyber-breach. Agents aggregate metrics across data streams and perform both real-time assessment and cognitive/predictive analysis. Acquisition decision-makers review reports when purchase requests are initiated or alerts indicate a need for action.

Next is dissection of the data pulled from the radio and network sensors and the systems (Figure 7). Analysis includes control logs, user roles and services, and security policies. Fortunately, this process can be automated such that acquisition decision-makers merely access reports as needed. Applications are monitored through passive and active taps and agents, records, and SysLogs. Asset monitors validate license compliance and cybersecurity for information assurance. Service monitors assess processing routes, message transformations, and data integration.

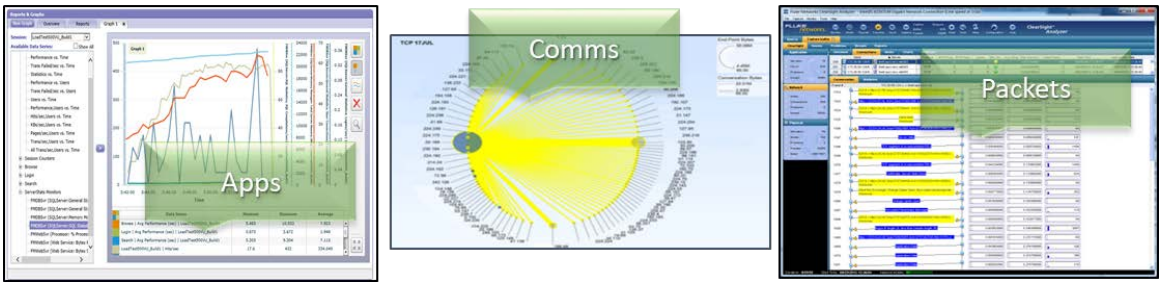

Figure 7. Sensor Communication, Application, and Packet Analysis

Packets can be decomposed to analyze their data. Status reports, along with real-time event streams, can be aggregated for continuous systems, cyber, and performance assessment

(Figure 8). In addition to status reports the acquisition decision-maker can apply predictive algorithms to determine whether systems or data has been compromised.

Figure 8. Event Analysis Through Performance and Function Monitors

Once events and data are normalized and correlated, the analytics detect data and user anomalies. Cognitive algorithms assess usage patterns to derive behavior profiles, integrating user, system, and network information to provide decision intelligence. Processing agents at each of the tactical nodes aggregate and filter data, then synchronize with the acquisition supply chain analytic servers (as portrayed in Figure 5). Data science is automatic as resources pass through the tactical processing nodes. This includes the cyber status along with cyber test and measurement results (Figure 9).

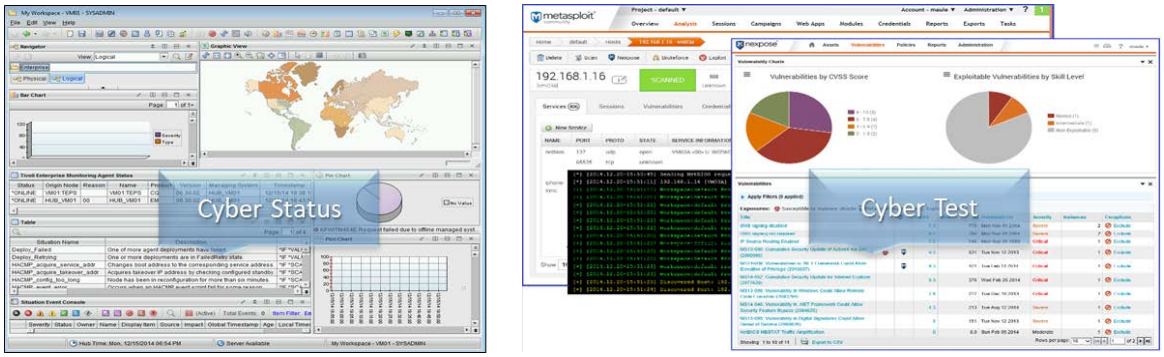

Figure 9. Cyber Status Monitors With Automated Cyber Stress Testing

Conclusion

This paper presented a process for acquisition supply chain analytics, addressing data collection, tooling, and decision support. The workflow is largely automated such that reports for systems and components are presented to acquisition decision-makers across the life cycle of an asset. This understanding will help ensure cybersecurity compliance, systems viability, and data validity across the supply chain—from initial purchase request, through maintenance, to obsolescence and destruction.

Analytic methods and tools were discussed, along with strategies to build AI into the analytic process to help acquisition decision-makers manage the complexities of supply chain management and to automate the workflow. Algorithms pertinent for supply chain assessment were discussed, integrating user, system, and network information to provide decision intelligence.

A path was presented for the integration of predictive algorithms that identify variables that may impact acquisition decisions. The architecture integrated real-time event data within technical, operational, and environmental context. Future research may further examine the intelligence algorithms for decision support or prototype the development of these online services to support acquisition supply chain analytics.

References

BMC. (n.d.). *Beyond the hype—How do you really put AI to work for ITOps?* Retrieved from http://documents.bmc.com/products/documents/91/51/509151/509151.pdf

BMC. (2018). *Client management datasheet*. Retrieved from http://documents.bmc.com/products/documents/05/74/480574/480574.pdf

Dietterich, T. (2003). Machine learning. In A. Ralston, E. Reilly & D. Hemmendinger, (Eds.), *Encyclopedia of computer science* (pp. 1056–1059). Hoboken, NJ: Wiley.

Farsal, W., Anter, S., & Ramdani, M. (2018). Deep learning: An overview. In *Proceedings of the 12th International Conference on Intelligent Systems* (pp. 1–6).

Goldberg, D., Nichols, D., Oki, B., & Terry, D. (1992). Using collaborative filtering to weave an information tapestry. *Communications of the ACM*, *35*(12), 61–70.

Ixia. (2017). Validating machine learning and security analytics. *Keysight.* Retrieved from https://www.ixiacom.com/sites/default/files/2017-08/Ixia-S-PB-Machine-Learning-Analytics.pdf

Koren, Y., Bell, R., & Volinsky, C. (2008). Matrix factorization techniques for recommender systems. *Computer*, *42*(8), 30–37.

Maule, R. (2015). *Lifecycle methodology for system of systems engineering capability and integration analysis*. OPNAV. Washington, DC: Department of the Navy

Maule, R. (2016). Complex quality of service lifecycle assessment methodology. In *Proceedings of the IEEE International Congress on Big Data* (pp. 462–469).

Maule, R. (2017). *SEA cyber figure of merit (CFOM) tactical systems cybersecurity assessment*. San Diego, CA: Space and Naval Warfare Systems Command.

Maule, R. (2019a). Acquisition cybersecurity management framework. In *Proceedings of the 16th Annual Acquisition Research Symposium* (pp. 1–16).

Maule, R. (2019b). QoS for supply chain cyber management. In *Proceedings of the World Congress in Computer Science, Computer Engineering, & Applied Computing* (pp. 3–9).

Maule, R. (2020a, February 10). Cybersecurity audit framework for information assurance [Paper presentation]. *Institute for Operations Research and the Management Sciences (INFORMS) Conference on Security*. Monterey, CA.

Maule, R. (2020b). *Persistent learning environment* [Unpublished manuscript].

Maule, R., & Lewis, W. (2010). Security for distributed SOA at the tactical edge. In *Proceedings of the IEEE Military Communications Conference* (pp. 13–18).

Maule, R., & Lewis, W. (2011). Performance and QoS in service-based systems. In *Proceedings of the World Congress on Services Computing* (pp. 556–563).

Maule, R., Gallup, S., & Jensen, J. (2010). Knowledge engineering experimentation management system. In T. Sobh (Ed.), *Innovations and advances in computer sciences and engineering* (pp. 573–578). New York, NY: Springer.

McMullen, T. (2015). It probably works. *Communications of the ACM*, *58*(11), 50–54.

Microsoft. (2020). Deep learning vs. machine learning. Retrieved from https://docs.microsoft.com/en-us/azure/machine-learning/concept-deep-learning-vs-machine-learning

Military & Aerospace Electronics. (2020). U.S. military authorities face replacing compromised chips in military computers. *Military & Aerospace Electronics*, *31*(2), 9.

NETSCOUT. (2019). nGeniusONE service assurance platform. Retrieved from https://www.netscout.com/sites/default/files/2018-12/EPDS_025_EN-1801-nGeniusONE.pdf

Resnick, P., Iacovou, N., Suchak, M., Bergstrom, P., & Riedl, J. (1994). GroupLens: An open architecture for collaborative filtering of netnews. In *Proceedings of the Computer Supported Collaborative Work Conference* (pp. 175–186).

Resnick, P., & Varian, H. (1997). Recommender systems. *Communications of the ACM, 40*(3), 56–58.

Rich, C., Prasad, P., & Ganguli, S. (2019). Market guide for AIOps platforms. Gartner. Retrieved from https://www.gartner.com/doc/reprints?id=1-1XRR9HDN&ct=191115&st=sb

Villasenor, J., & Tehranipoor, M. (2013). The hidden dangers of chop-shop electronics: Clever counterfeiters sell old components as new, threatening both military and commercial systems. *IEEE Spectrum.* Retrieved from https://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net