KDM Analytics

BUSINESS CASE

Automate, Prioritize, and Quantify CyberSecurity Risk

Automated NIST RMF Assessment for Operational Technology

Reduces solution provider's cost of service by 80%; increases value-add to end-client

Synopsis

Acquired Data Solutions (ADS) used KDM Analytics Blade RiskManager (BRM) to automate the risk assessment phase of a cybersecurity product assessment for a large defense and aerospace developer. By optimizing the process, BRM reduced ADS's cost of service by 80% and decreased required manhours by 80%—all while increasing the robustness and scope of the assessment.

Applying the NIST RMF to Operational Technology

A large defense and aerospace client turned to Acquired Data Solutions (ADS) to assess the cyber risk exposure of a test and measurement system. The client required an assessment of its system's cyber risk within three key areas of the NIST Risk Management Framework (RMF) standard. These were:

- NIST 800-53 REV4 – information technology (IT) cybersecurity
- NIST 800-82-REV2 – operational technology (OT) cybersecurity
- NIST 800-30 REV1 – risk assessment guidance

"Our clients depend on us to help establish their security posture and make sound decisions about how they manage the implementation of controls," says Steve Seiden, President at ADS. For this project, his team determined that a traditional manual risk assessment would not be feasible.

Steven Whitcomb, Operations Manager at ADS, notes that, "Manual risk assessments, even with guidance, create concerns. They can be costly, resource-intensive, and time-consuming and do not assure that a comprehensive assessment will result. It may not be possible to understand and itemize the various attack patterns that can compromise a system. Risk modeling also requires iterative assessment that can lead to many mistakes when performed manually."

For this reason, ADS sought a solution to automate the cyber-risk assessment element of this project. "We wanted to more efficiently and robustly conduct a risk assessment," Whitcomb adds.

A Comprehensive Solution to Automate the Risk Assessment

Using the Federal Information Processing Standard (FIPS) 199, ADS established a security categorization of "High" for the project, then created a System Security Plan to establish the current state of the client's organization and target system. Next came the cyber-risk assessment.

Goals for the assessment included:

- Align client's initiatives with the NIST Risk Management Framework
- Organize cybersecurity activities within the organization

Industry Sectors

- Defense
- Aerospace
- Operational Technology
- Industrial Control Systems

> ***"With Blade RiskManager, we could quantify risks in a way that we could not have done with a manual process. That gives everyone confidence, including the client."***
>
> *– Steve Seiden, CEO, Acquired Data Solutions*

Automated NIST RMF Assessment for Operational Technology

Reduces solution provider's cost of service by 80%; increases value-add to end-client

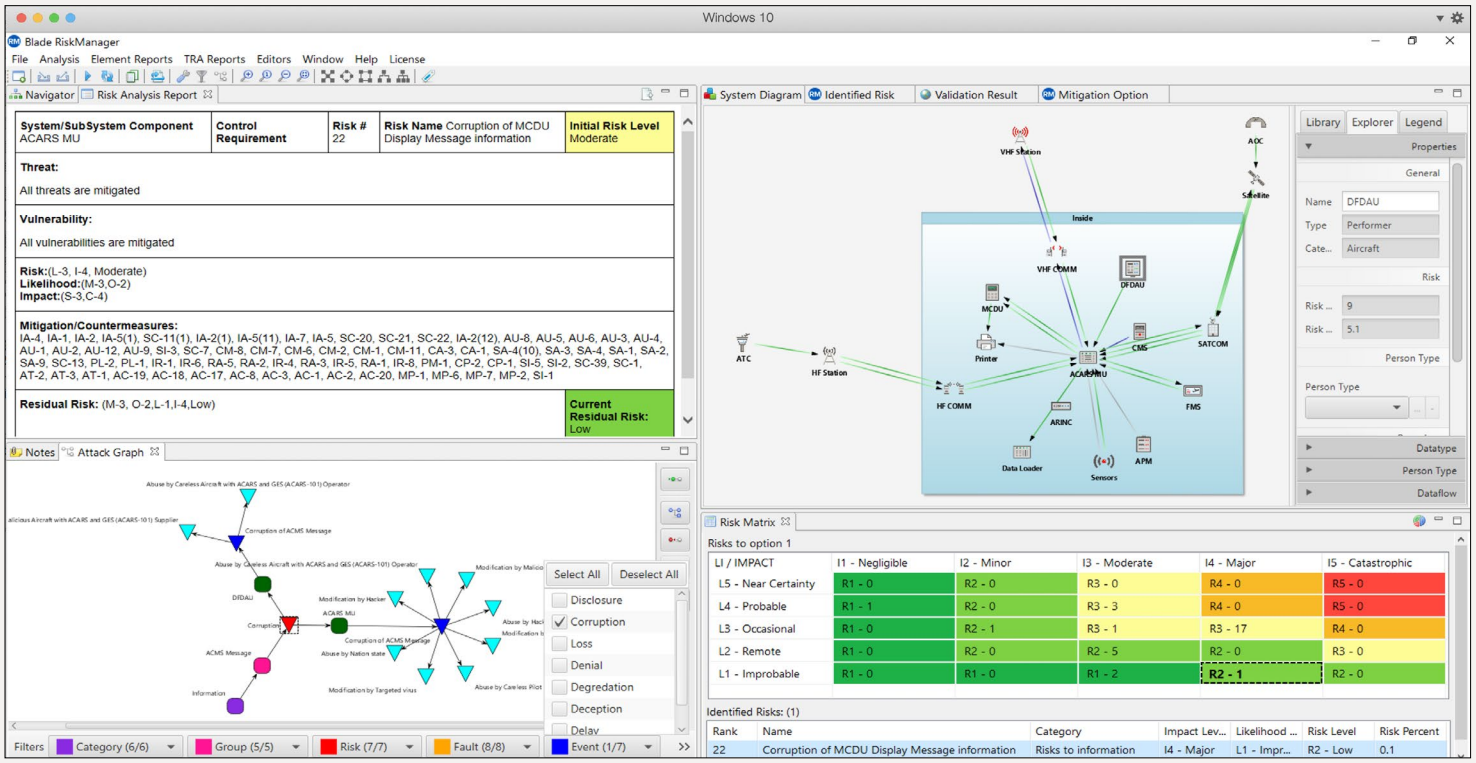

Figure 1: Example of visual system diagram produced by Blade RiskManager

- Create a cybersecurity plan for the industrial control system and evaluate its cybersecurity posture
- Prioritize and focus which security controls should be implemented

ADS outlined its requirements for a solution to automate the risk assessment while helping to meet those goals. It needed:

- An evidence-based, model-driven assessment
- Adaptability to assess the components of operational technology
- An extensive cybersecurity knowledge base
- Ability to prioritize control measures
- A quick but comprehensive assessment tool

"KDM Analytics Blade RiskManager checked all the boxes, and then some," says Dr. Tony Barber, who led the risk assessment for ADS. "BRM has a unique way of pulling in the system architecture, it has an extensive cybersecurity knowledge base so we didn't have to do that research ourselves, the workflow of the software is very intuitive, and the reporting capabilities were excellent."

Fast, Efficient, and Easy to Tailor

Although it was ADS's first time using BRM, the team found it efficient and intuitive to learn. Whitcomb notes that "BRM uses a system engineering approach that makes a lot of sense. It enabled us to describe the system and the data flows through the system, and to use that as a model that we could input into the product. It is a very natural way of assessing risk."

> ***"BRM revealed five potential risk-mitigation strategies and gave us the time to think through those options."***
>
> *– Tony Barber, Risk Assessment Lead, Acquired Data Solutions*

Automated NIST RMF Assessment for Operational Technology

Reduces solution provider's cost of service by 80%; increases value-add to end-client

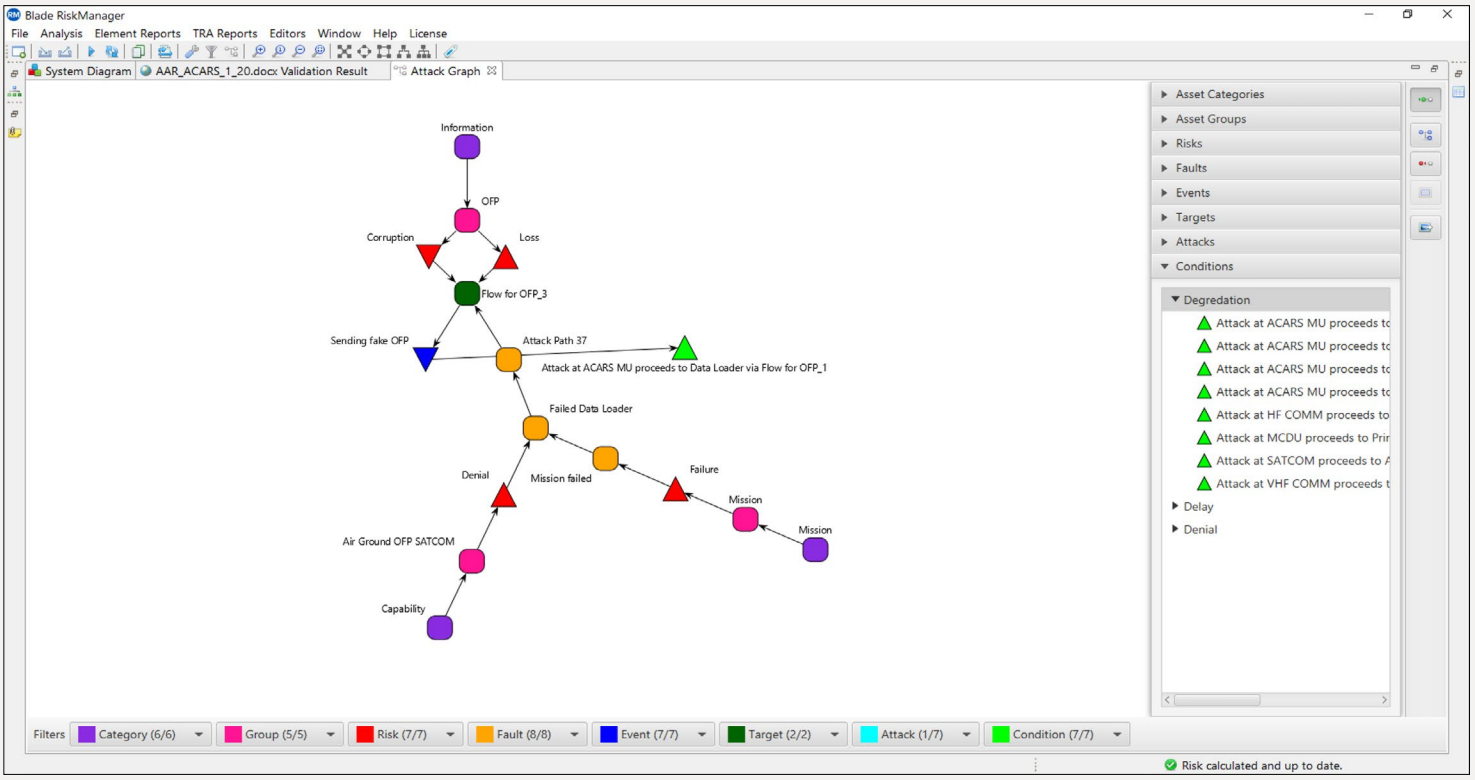

Figure 2: Blade RiskManager interface with a visual attack graph and scoping based on selectable filters

Barber agrees that BRM provided several helpful features. "It was easy to format our inputs into a word table and feed that into BRM," he says. "Inputs included system description, data types, data sensitivities, information exchanges, data flows and so on. BRM rendered that data as a visual system diagram. That was a nice way to ensure that the data we input was a good representation of the system and its boundaries."

Likewise, Barber found "the visual attack graph that BRM created made it easy to understand where to focus risk-mitigation efforts by focusing on specific categories, groups, risks, and faults, then examining and tailoring that output."

BRM made quick work of identifying and calculating the client's system risk in accordance with the NIST RMF standard, freeing Barber to focus on applying his strategic knowledge. "Literally at the push of a button, BRM gave us a solid risk queue and associated vulnerabilities. That allowed us to sit back and determine if the output made sense given our knowledge of the system and the client. BRM let us tailor those outputs as needed."

Finally, the ADS team used BRM to quickly model several mitigation strategies—essentially running "what-if" scenarios—and choose the best one for its client. "We were able to set our control baselines, develop mitigation options, and use BRM to see how different mitigation efforts changed the risk assessment."

> ***"Literally at the push of a button, Blade RiskManager gave us a solid risk queue and associated vulnerabilities."***
>
> *– Tony Barber, Risk Assessment Lead, Acquired Data Solutions*

Quantifiable ROI in Three Areas

BRM helped Barber shave more than 2,000 identified risks down to 58 priorities to mitigate. BRM identified the ten top risks and 35 unique attacks within those top ten. BRM also highlighted the top ten attackers.

Automated NIST RMF Assessment for Operational Technology

Reduces solution provider's cost of service by 80%; increases value-add to end-client

"BRM's outputs really helped us tell the story to the client," Seiden says. "With BRM we could quantify risks in a way that we could not have done with a manual process. That gives everyone confidence, including the client."

Importantly, BRM also enabled the ADS team to focus on its true value-add: strategy. "BRM revealed five potential risk mitigation strategies," Barber explains. "We had time to think through these options to mitigate risks and make a solid recommendation tailored to the client, focusing on the highest impact risks with the least amount of effort."

ADS says the return-on-investment (ROI) of Blade RiskManager is measurable in three areas:

1. **Productivity** – the ability to focus on analysis and insight rather than investigation and research.
   ROI: 80% decrease in cost of service.
2. **Optimization** – the ability to augment mitigation models with faster recalculation of risks.
   ROI: 80% decrease in person-hours.
3. **Coverage** – BRM's extensive knowledge base of current vulnerabilities, threats, and attack patterns increased the scope and robustness of the assessment ADS delivered to the client.
   ROI: greater client value with minimal effort.

Overall, ADS reduced its cyber-risk assessment resource requirements from five people and 2,000 manhours to one person and 390 manhours. "And that was on initial use of BRM," Whitcomb notes. "The manhour requirement will be further reduced as we increase our familiarity with the product."

ROI:

- 80% decrease in cost of service
- 80% decrease in person-hours
- Delivered greater client value with minimal effort

About Acquired Data Solutions

Acquired Data Solutions—now a KDM Analytics reseller partner—has over 20 years' experience providing technology solutions for the engineering life cycle to government agencies and the commercial sector. Its expertise in test, integration, automation and cybersecurity has made the company invaluable to customers requiring solutions to improve their development environments, manufacturing processes, and product and system quality. www.acquireddatasolutions.com

About KDM Analytics

KDM Analytics products help organizations save time, save money, and focus their risk-assessment resources. We automate the NIST risk management framework (RMF) assessment for operational technology (OT) systems. KDM Analytics provides the only cyber-risk management solution to automate both top-down and bottom-up analysis. This helps organizations achieve rapid, repeatable, and evidence-based cybersecurity risk assessment. www.kdmanalytics.com

KDM Analytics

For more information, please visit www.kdmanalytics.com or contact us at info@kdmanalytics.com

Ogdensburg, NY, U.S.A.
Phone: (315) 605-1059
Fax: (866) 238-0184

Ottawa, Ontario, Canada
Phone: (613) 627-1010
Fax: (866) 238-0184