iSID Intrusion Detection System
Field Deployment Study

MAY 2017

BLACK & VEATCH
Building a world of difference.®

Executive Summary

Black & Veatch was tasked with assisting Radiflow in evaluation of their IDS solution (iSID) in the context of an actual customer field proof-of-concept deployment. The customer, Western Farmers Electric Cooperative (WFEC) based in Anadarko, OK and part of the U.S. Western Electricity Coordinating Council (WECC) is considering the deployment of the Radiflow IDS and Gateway Firewall solutions. The evaluation by Black & Veatch focused on the qualitative observations of WFEC's use of the product with those findings summarized in this report.

Human Factors product evaluations typically include conducting a simulated or actual field test, in which prospective users are asked to operate the device or solution in a meaningful and realistic way. For WFEC this means observing their use of the solution as it was deployed to 3 separate sub-station locations and subsequently operated over several months. In this context, the Black & Veatch Network Services team solicited direct customer feedback at three points during a 4 month proof-of-concept test window. However, our findings also include a high-level lab evaluation of the solution's user interface and primary features, as well a User Guide review.

The findings in this report are contained within four groupings:

- **Findings Overview**

  General observations of the solutions overall behavior and capabilities in the hands of actual end users including: Installation**,** Network Adaptability, Documentation/Vendor Technical Support**,** Functions/Features Value**,** NERC CIP Compliance Value**,** Existing Security System Integration**,** Staffing and Sustainment Requirements.

- **Customer Field Use Experience**

  Our evaluation of the customer's use of the iSID solution occurred over a 4 month operating window. At least three code version iterations of the product were installed for use by the over that time. At each of these version update stages, a customer interview was performed to assess how well the solution performed. While observations cover many aspects, they are focused around the support of approximately 30 features/criteria which, with the cooperation of Radiflow, the customer defined at the start of the product evaluation.

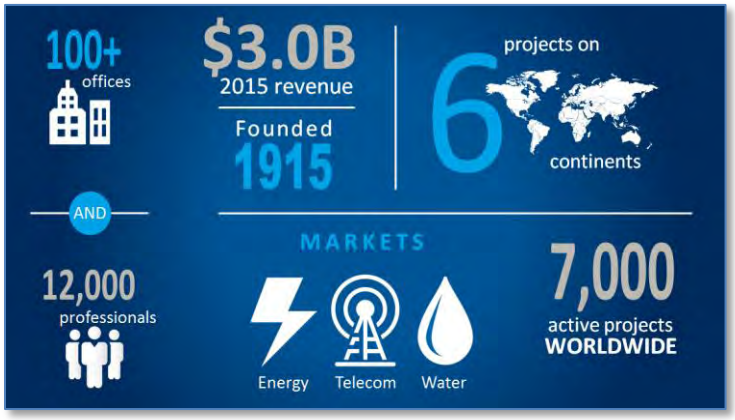
- **Black & Veatch Lab, User Interface Review (Annex)**

  Black & Veatch was given the opportunity to install version 4.4.3.16_1 of the iSID solution in our testing lab in order to do an evaluation of the solution's basic operation, feature set and user interface characteristics. This evaluation was intended to be qualitative in nature, not quantitative, focused on customer interaction and perception of the solution verses quantitative performance and functional capabilities. We utilized the opportunity point out function limitations or advantages of the iSID product but most testing focus was concentrated on human factors.

- **Black & Veatch User Guide Review (Annex)**

For any solution which is relatively new to a market, particularly complex networking and cybersecurity related solutions, a well-constructed User Guide is a vital component for customer support influencing the field experience. For this reason Black & Veatch also provides in its findings generalized commentary about the User Guide and include as an addendum a marked up commented copy of that guide. Examples of those comments will be examined in this section.

Our methodology for these types of product evaluations is based upon best-practice systems life-cycle management concepts and perhaps equally as important, Black & Veatch's unsurpassed field experience working with both customers and OEM solutions deployed around the world within Industrial Control Systems environments covering electric and gas utilities, transportation, mining, smart integrated infrastructure and more.



FINDINGS SUMMARY

Black & Veatch Network Services Group believes that the Radiflow iSID industrial Intrusion Detection product provides a much needed set of foundational features that effectively capture and display cybersecurity telemetry which our utility customers may find compelling. In real terms deploying the iSID solution should help customers increase their overall field network cybersecurity posture while bringing additional strong information collection capabilities to operations functions. While the product has much to offer, we also find that like many recent entrants in to the rapidly evolving critical infrastructure sector, iSID would experience immediate market benefits by improving some aspects within their user documentation, further evolving their web console user interface through the use of common design and controls behavior standards, refining how some existing features operate and adding some key additional new features and/or capabilities. While not included in this study, Radiflow's ruggedized 3180 Gateway product can be used in conjunction with the iSID, extending capabilities beyond detection and flow visualization by enabling policy enforcement for the monitored infrastructure. This is accomplished through support of IPSec VPN tunnels and a firewall function with service-aware inspection of SCADA protocols.

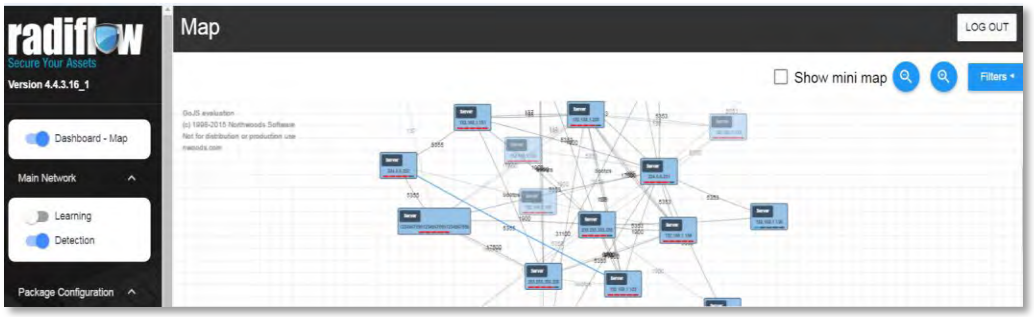
FINDINGS DETAIL

It is clear from all the interviews, recorded customer observations and lab evaluation that the iSID product provided many features and functions with have proved invaluable to the

customer's pursuits of improved cybersecurity protections and operations. We offer summary comments for a set of specific product execution areas:

1. **Installation** – Straight forward and comprehensive. When installed on a platform with the proper specifications, customers will experience few issues as a successful installation requires little external customer actions. While there is a current design limitation regarding updating operating systems on large numbers of deployed iSID's, neither the customer, nor the Black & Veatch team had any difficulty while performing multiple installation and a few installation sites.
2. **Network Adaptability** – Implementation of the solution within the context of a typical utility field site data network infrastructure was straight forward and encountered no shortcomings. There were no methods or procedures required for integration which would present anything new to competent network engineers.
3. **Functions/Features Value** – A look at the customer criteria ranking column within the raw data spreadsheet and within tables provide in this report clearly identifies which are considered most valuable to this customer and how well the customer believes Radiflow has executed in support of them within the product itself. While all customer criteria is rated in this way, those rated as 'Essential' received the following customer evaluations:
   - Industrial Protocol monitoring 1.1.3 - Good
   - Protocol errors 1.1.9 - Adequate
   - Real-time alerting 1.3.1 - Good
   - SYSLOGGING 1.4.1 - Good
   - Application Flow Source/Destination Reporting 1.5.1 - Exceptional
   - Application Flow ICS Protocol Discovery 1.5.2 - Good
4. **Documentation/Vendor Technical Support** – The User Guide provided good factual data about how the product operated. While providing valuable tabular formats for displaying lots of important operations data, the guide was perhaps too succinct in its description of practical operational procedures and/or use examples. The Guides use of language while appropriate and accurate from the OEM iSID functional perspective, perhaps lacked some perspective from actual, practical field use applications. Some of these issues are discussed in more detail in the User Documentation section.
5. **Staffing and Sustainment Requirements** – The iSID solution is simple to operate and present information within the interface that is relatively clear and easily interpreted by a cybersecurity professional with moderate practical ICS experience of 2-3 years. This suggests the iSID solution is, relative to other products within the same category, a very easy to deploy and operate solution with highly accessible actionable current state and base line variation information necessary to achieve improvements in cybersecurity posture monitoring as well as cybersecurity operations. While not required, some knowledge of Linux command line can increase understanding of the solution's operation within the infrastructure.

6. **NERC CIP Compliance Value** - Mapping functions present in the management and monitoring consoles main screen provides unique and valuable instant feedback about the protected infrastructure via an application flow view, a perspective often missing in competitor's offerings.



Our opinion was validated through field use observations with this feature being rated as 'Exceptional' by the customer. The feature provides the primary source of baseline application data flow identification and is used in concert with the notification console, which also provides baseline deviation notification in the form of alerts for unauthorized and/or unknown flows. It is easy to imagine a variety of possible enhancements for this application flow mapping feature, so it is no surprise that Radiflow is already concentrating development efforts in this area.

In support of specific compliance efforts and general cybersecurity operations, we find that the product offers some key essential benefits for meeting compliance requirements, both through the mapping feature and using the alerting console. Both features combine to support NERC CIP-005, Cyber Security Electronic Security Perimeters, by providing essential records as to the state of the Electronic Security Perimeter and any flow changes that might indicate a violation. We believe Radiflow is on the right path with these features. As the product evolves additional value in the area of refined compliance, reporting output can be provided and can make the evidence gathering and reporting requirements even easier.

Within the User Action logging, we also find audit trail information for user activity within the solution – a valuable source of information. Translating this output into a pre-defined specific change-control report would add additional value. In any case, the product provides verification of changes of cybersecurity protections provisions, which are required under CIP-003 Security Management Controls. The alerting console provides foundational support for CIP-008 Incidence Report and Response. The SYSLOG feature provides additional compliance evidence encompassing CIP-003 and CIP-005 and some elements of CIP-007 Security Systems Management. There is also some support via logging messaging for CIP-010 Configuration Management. Here we'd expect that as the solution continues to evolve, we might see the SYSLOG message base extended to include even more coverage for CIP-010. There may also be an opportunity to provide ICS protocol baseline variation alert logging (perhaps with manually adjustable baseline deviation thresholds), which would further enhance the already valuable logging features.