CASE STUDY

inVIEW WebSCADA and Security Convergence

Continuous third party security offensive testing is necessary to enforce highest security availability for inVIEW WebSCADA platform. Together with RAS-IT and PreCog Security team, we are confident that our partners and clients will be able to enjoy state of the art data acquisition, monitoring and control while being protected from attackers.

OBJECTIVE

Provide Highest Security Availbility for Web SCADA InView Customers

INDAS is a company that deals with automation for more than 25 years as a vendor independent system integrator. With more than 70 employees, mostly engineers and software developers, INDAS is a **top SIEMENS partner** and leading company in South East Europe in its field of expertise, with references in several hundreds of automation projects in various industry areas. INDAS' solution inVIEW WebSCADA (http://www.inviewscada.com) offers state of the art monitoring, control and data acquisition based on web technologies. Some of the features and value of this system is No clients needed, only browser.

Multiplatform solution available on smart phones (android, iPhone), tablets (android & iPAD) and PC computers, including MACs and notebooks (LINUX or Windows) Available anywhere with internet connection, Available as standalone SCADA server or as CLOUD service.

" We built Web SCADA InView based on our vast engineering knowledge, customer needs and trust. We understand that clients are looking for functionalities to solve business problems, but they need to trust that SCADA system is secure and regularly tested by security experts."

SOLUTION
Continuous Security Assessments by Security Specialists and Practitioners

"We did not want to settle down with basic security protocols or automated vulnerability assessment. In order to achieve highest available security for our WebSCADA system at all times we implemented ongoing third party offensive security testing "

When picking the right security company to do penetration testing for WebSCADA, few things come to mind:

1. Do they understand SCADA systems, its controls, regulations and customer needs?
2. Are they security specialists and practitioners or just generalists?
3. Are they able to perform offensive penetration testing with ethical hacking techniques or are they just doing automated vulnerability assessment?

"Our team was impressed with RAS-IT and PreCog Security team credentials and expertise. We chose their security assessment as a service (sAAAs) model which ensured that our systems are tested regularly through rigorous techniques such as: cross site scripting (XSS), SQL injections, remote code executions"

"We welcomed the opportunity to elevate security readiness for inVIEW WebSCADA. We were impressed with the level of engineering and functionality this system offers. At the same time we were able to bring security value to the system, elevate its security posture and minimize the risk of unauthorized access."

OUTCOME
Highest Security Availability for Web SCADA InView Customers

" We are very happy with the outcome which helps us maintain A security score when tested by third party organizations. What is even more important is that we are confident that besides state of the art modern Web SCADA platform we also have a secure solution for our partners and customers". Feel free to contact us to learn how inVIEW WebSCADA can solve for your business and industrial needs at **office@inviewscada.com**

INDAS team and its inVIEW WebSCADA are a great example on how to approach highest security availability. They understood best way to truly elevate and maintain A score, reduce risk of attacks and provide secure solution to customers is through ongoing third party offensive testing and security assessments with RAS-IT and PreCog Security" said Dejan Levaja CEO of RAS-IT and Alex Paunic CEO of PreCog Security Inc. - strategic partners with operations in North America and Europe. Schedule your free security assessment demo at **office@precogsecurity.com.**