How Are You Monitoring SCADA?

P2P1-R14: How Are You Monitoring SCADA?

Gib Sorebo, Security Consulting Senior Manager, Accenture

How Are You Monitoring SCADA?

With the heightened concern about cyber attacks on critical infrastructure, many have concluded that we have little visibility into industrial control systems to detect malicious or inappropriate activity. This session drew on the experience of participants to understand what industry control system (ICS) security detection technologies they're exploring, what works, and what technologies and techniques need more improvement.

The objectives included:

- Understand where in an Operational Technology (OT) environment to monitor to detect threats
- Come away with a process to implement a holistic monitoring program for OT
- Learn the various monitoring techniques for proprietary OT devices

What are the indicators, events, or other parsable data that would give you more events on those underlying processes? How can you get that data? What tools are you using? Do you understand how to configure them? Do you have people with the requisite knowledge of the underlying processes that can (1) create the use cases, and (2) provide ongoing monitoring support? What level of monitoring support do you have for your organization or your customer? These were some of the questions we attempted to answer in this peer to peer session.

It turns out that OT security monitoring is still somewhat limited. For example, a pre-conference survey of seven respondents found that four were monitoring security events from ICS. While this is clearly a small sample, the twenty-five individuals attending the session demonstrated that only a small number were addressing this issue. Some this may reflect the fact that the RSA Conference tends not to attract attendees from some of the core industries where ICS technology is heavily used (e.g., utilities, oil/gas), and where they do attend, they are often not coming from the OT side of the organization. For many of the attendees, common challenges like having an accurate inventory of their OT assets and being able to work across IT/OT divides predominated. And once those issues were resolved, the participants highlighted technological limitations in the ability to scan many of these devices, which are often old and fragile.

Not surprisingly, many of the issues facing IT environments were apparent in this discussion. For example, the participants' organizations struggled with defining and applying hardening guidance as well as keeping things patched. Given the 24x7 nature of many of these environments, finding adequate time windows to test patches on production systems or adequately simulating a production system to demonstrate the consequences of a patch remain as major obstacles in this environment. Like IT environments, attendees were worried about the threats posed by ransomware and were using those examples are part of their awareness campaigns. That also includes better integrating threat intelligence into their operations to catch the latest ransomware outbreaks. As recent reporting indicates, malware protection vendors were a bit slow to catch LockerGoga, the recent ransomware that struck Norsk Hydro and other manufacturers.

Finally, there was limited experience with OT specific monitoring tools like Nozomi, Claroty, SecurityMatters, Indegy, CyberX, and others. Some have started to use these products with others using traditional IT security monitoring tools like Intrusion Detection Systems (IDS) and Security Information Management (SIEM) systems. But the key takeaway is that more education is needed. Most organizations still have a lot of work to do to gain visibility of their OT environments. And that starts with having conversation with all the stakeholders to understand all the key assets and the best way they can be monitored.