OT INSIGHT – THE OT MONITORING SOLUTION

Ilya Tillekens from Hudson Cybertec looks at how to protect operational technology infrastructure from cyber threats

> **CURRENT** threats require tank terminal organisations to be aware of security at all times. Do you know how secure your operational technology (OT) infrastructure is at this moment? Specifically of your OT network? Is your infrastructure adequately protected against cyber threats like unknown or rogue devices, (new) vulnerabilities and malware like ransomware? To protect your OT network environment, threats must be identified and acted upon as soon as they are detected. Suspicious network traffic must be analysed and measures taken before an incident occurs. This requires a 24/7 approach to monitoring OT network infrastructure, while keeping in mind the specific dependencies of your OT network infrastructure.

An increasing number of tank storage organisations realise that they need to continuously monitor their critical network infrastructure so that deviations in the network traffic of critical network infrastructure can be detected. To accomplish this goal, it is essential to establish a baseline that include at least your networked assets and their associated risk profile. This ensures that threats are identified as soon as they occur. For tank storage organisations, where the technical (OT) infrastructure is often static, this is a good approach to get an insight in the deviations of your network traffic (often called anomaly detection).

Only then can you respond in a timely manner to threats and take the appropriate measures to protect your network infrastructure and the integrity of your OT infrastructure as a whole. This approach ensures that you stay in control of your OT network as well as compliant with existing and future policies, laws and regulations.

ANOMALY DETECTION AND MORE

Anomaly detection alone is no longer sufficient. Organisations expect more from their OT monitoring solution than anomaly detection in regular network traffic. They expect additional functionality like monitoring communication quality so that they can solve potential connection or configuration problems. People also expect support for asset management, to which a good OT monitoring solution can contribute.

'It is evident that an OT monitoring solution must understand protocols specific to an OT environment flawlessly,' says Marcel Jutte, managing director of Hudson Cybertec. 'Solutions built for IT environments do not or insufficiently process and support these specific OT protocols, and this results in an incorrect interpretation of network traffic.'

If entire communication flows are misunderstood or wrongly interpreted by the OT monitoring solution, it results in an incomplete picture of those assets that are vital within a tank storage terminal's OT infrastructure. An OT monitoring solution must therefore recognise all protocols within the OT environment of a tank storage terminal. A solution that is developed entirely from an OT perspective is therefore essential.

LAWS AND REGULATIONS AROUND OT

Organisations with OT infrastructure are increasingly demanding OT monitoring solutions tailored to their operations due to greater cyber security demands from specific sectors and government. Laws and regulations regarding digital resilience of vital or critical infrastructure is just one example of the changing outlook on cyber security. Take, for example, the EU's Network Information Security (NIS) directive, which went into effect on 9 November 2018 and is applicable to all EU member states. This directive requires member states to identify so called 'essential services'. Organisations that are designated as 'essential services' are required to take appropriate cyber security measures.

Such organisations must report cyber security incidents with a significant impact and have a duty of care for cyber security. This simply means that their digital resilience should be in order and demonstrable. They typically use standards frameworks such as IEC 62443, ISO 27000 and local standards like BIO, VEWIN or CSIR (in the Netherlands) to ensure compliance. By taking the right measures based upon recognised standards they increase digital resilience and demonstrate that they comply with applicable laws and regulations.

THE GAME CHANGER

So, OT monitoring is essential. Since using an existing monitoring solution that was not designed and developed for OT environments may expose an organisation to unwanted risks, Hudson Cybertec developed a new solution, OT Insight. OT Insight is a game-changer in the field of monitoring OT infrastructure. It offers the standard functionality expected from existing solutions, but what makes this solution unique is that the monitoring platform also detects and reports deviations in the aforementioned standards to the asset owner.

Jutte explains: 'The majority of our customers are in vital infrastructure, in oil, gas, or tank storage. They want to, or must, comply with these laws and regulations. OT Insight is an ideal solution for them. Also, other organisations that have OT environments understand the need for a secure OT environment and often use the IEC 62443 for guidance and compliance. An OT monitoring solution that supports monitoring against such standards and laws and regulations is of great benefit.'

With OT Insight, there is a clear dashboard showing agreement or compliance with the different standards frameworks based upon the organisation's requirements. In addition, organisations can easily see where action is required. The system provides a notification as soon as an abnormality is found, so that it can be can be acted on. Detailed information is available with a simple mouse click.

> Organisations with OT infrastructure are increasingly demanding OT monitoring solutions tailored to their operations due to greater cyber security demands

OT Insight is a modular OT monitoring solution, allowing comprehensive monitoring of OT network infrastructure, supportings connections to different data sources and applications. Detailed analysis within OT Insight with in-depth support is available when needed, with the presentation of the findings through customisable dashboards that show customised information relevant to the organisation.

Another unique property is that it is a fully Dutch/German (European) development, something which is required in some jurisdictions.

'For the security of the Netherlands is it important that organisations with OT environments have access to a fully European solution. Companies in need of an OT monitoring solution for cyber security should not only depend on technology from non-European countries,' explains Jutte.

This requirement is also seen in, for example, the telecom sector where equipment from certain countries is banned to prevent possible espionage in the telecom network infrastructure.

STAKEHOLDERS AND INCREASING INTEGRATION OF SYSTEMS

Organisations need a locally built custom solution matching their specific wishes regarding digital resilience. Inside an organisation, stakeholders have different interests. A maintenance engineer of an OT environment needs very different information than a security officer or management team. OT Insight delivers the right information at the right time to different target groups. For each target group a specific dashboard can be created that shows the relevant information.

OT Insight helps to make the OT environment digitally resilient. In an environment where the integration of all kinds of systems through the technical network is increasing, a monitoring solution that adjusts and grows with an OT environment is not a luxury, but a necessity, especially since more and more building-related systems such as access control systems, HVAC and even fire alarm and burglary detection systems are using the same infrastructure. The trend is to integrate these systems in order to correlate the findings of those systems or to ensure safe interaction between these different systems.

IN PRACTICE

OT Insight has been deployed effectively at various organisations within the EU, giving those organisations a good overview of their compliance for the NIS directive, using existing standards like the IEC 62443. Where gaps were detected, remediation plans were established, executed and successfully implemented. Anomalies in traffic were detected and led to prompt corrective actions and tightening of exiting measures (either technical or organisational). With OT Insight, you do not only get a technical solution, but analysis and support by Hudson Cybertec's experienced OT cyber security professionals.

Tank terminal organisations should be vigilant, and take control of their OT network infrastructure through a monitoring solution that has been specifically designed and created for an OT environment, in order to protect their assets and infrastructure from cyber threats and ensure compliance with laws and regulations.

'In the end, cyber security is largely about insight. Only if you know what's happening in your OT environment, you can really be in control,' says Jutte.

For more information:

This article was written by Ilya Tillekens, senior security consultant at Hudson Cybertec. Hudson Cybertec is the independent cyber security consultancy and services provider for operational technology (IACS) specialised in critical infrastructure, including the tank terminal sector. For more information on the company and on OT Insight, please visit https://www.hudsoncybertec.com/en/tsm.