Payatu

ICS/SCADA (OT) Security Datasheet



OVERVIEW OF THE SERVICE

OT generally referred to as Operational Technology, is a sophisticated network of interactive ICS (Industrial Control Systems) that includes Sensors, Controllers and Monitoring/Control Applications.

ICS describes the integration of software and hardware with network connectivity for supporting critical infrastructure. It is used in oil/gas, manufacturing plants, chemical/pharmaceutical plants, water/waste-water treatment plants, and wherever industrial automation and continuous/batch processing are needed.

ICS technologies include SCADA which is short for Supervisory Control and Data Acquisition. SCADA is a system of hardware and software elements that help in processing data in order to make smarter decisions, maintaining efficiency, and communicating system issues for mitigation of downtime. It is used in pipeline monitoring, traffic signals, electricity power generation, etc.

Lately, more and more of these systems have been exposed to an elevated threat landscape, leaving a wider scope for hackers to make way for their attacks.

Securing these systems is of prime importance due to the criticality of their nature, as any threats are not just limited to financial loss or brand name destruction, but also go to the extent of loss of life and even threat to national security.

Payatu is a leading security assessment provider for ICS/SCADA(OT) Security.

KEY ATTRIBUTES

Payatu's objective is to assess the current posture of the critical infrastructure of the client to help in improving overall level of security of the systems and what sets this service provider apart is -

A combination of realistic and abstract approach

Having substantial experience and understanding of OT protocols paired with learning the infrastructure conceptually helps Payatu Bandits to define a process and roadmap specific to the client.

Reports that go beyond reporting

Generalized reporting is a drawback that can make any OT security assessment futile. With Payatu, clients get a detailed report consisting of the findings, criticality ratings, granular breakdown of the implications, and even recommendations.

End-to-end defining of the scope

It is important for Payatu to address all types of potential attacks and gaps in the client's systems, which is why its scope covers everything ranging from Maturity review, Risk Assessment using standards like NIST 800-82, ISA/IEC 62443, Passive Scanning, Solution Implementation using Industrial Firewalls, Unidirectional Gateways, etc.

Ultramodern tech integrations

Payatu strives to widen the testing surface to ensure the identification of all vulnerabilities, and it does so by integrating different internal, external, and modern third-party tools and software for building SOC with OT Capabilities.

The Payatu Extra Mile

Payatu goes an extra mile by offering guidance to the in-house security team of the client on the mitigation and recovery plan, getting the compliance of the systems with the mandated standards, and a lot more.

Payatu

KEY BENEFITS

A weak security posture of OT systems can lead to breaches causing production downtime, revenue loss, disruption in operations, safety hazards, environmental disasters, and even endangerment to human life and public safety. It is crucial for ICS companies to operate with a robust cybersecurity posture, in order to combat any cyber-attacks coming their way. Payatu can be an asset to such companies in helping them achieve their desired cybersecurity goals and posture.

01 Maturity Review for Identification of all Security Gaps

All the processes and practices of the client's ICS and SCADA systems undergo a maturity review. Payatu reviews the current measures and supporting evidence to ensure that the systems are assessed thoroughly for all security gaps.

02 Identification of all Potential Flaws with Risk Assessment

To help the clients in addressing all potential security flaws, Payatu starts with a review of ICS Cybersecurity Implementation Technology, and moves on to finding potential flaws, validating technical findings, and reviewing the network topology & architecture and OT Systems.

03 Finding Unexpected Communications with Network Testing

To detect unexpected communications in the client's network, a thorough technical network assessment of the client's OT networks is conducted, followed by discovery of primary vulnerabilities and environment specific vulnerabilities (e.g. All Assets at Level 0, 1, 2 and 3 including PLCs, DCS, RTU, SCADA Applications, Servers and Gateways).

04 No Disruption to the Organization with Passive Scanning of OT Environments

Intrusive testing methods can interrupt the day-to-day working of organizations, leading to huge downtime losses. Some OT-specific security characteristics that clients get with Payatu are – passive observation, deep SCADA understanding, unintrusive insertion resulting in no disruption or downtime, behavioral analysis, and continuous monitoring.

05 Top-tier OT Security Offerings

Payatu offers high-end OT security services offerings inclusive of technical testing (Product level assessments), solution implementation (SIEM for OT - Design, Development and Implementation of centralized tools for OT visibility, asset inventory, Threat and Vulnerability Management), advisory, and ICS training.

06 Granular Understanding via Extensive Documentation

In the documentation, the details of the test cases, scan results, vulnerabilities found, and proof of vulnerabilities are captured along with an overview of the current security state of the target and how the customer can improve it.

07 Build Brand Confidence for Users

Clients can make security their value proposition in the competitive digital market by establishing trust within their users/clients by offering security as their brands' proposition.

08 High-Quality Testing

9 out of 10 industry leaders have made it a point to recommend Payatu's services to other pioneers because of the experiences they had while getting their OT systems tested. This has been made possible because of the best-in-class hires who have proved their mettle by going beyond their scope of work, even before they're hired.

Payatu

Top Customers

NXP SSMC

ENGAGEMENT MODELS

You choose what works best for you!

Payatu offers different engagement models to let the client decide what floats their boat when they avail themselves of the ICS SCADA security assessment service. They can choose from

01 Time-boxed Approach,

where the client shares the details of the scope of assessment with Payatu and the service provider evaluates the time and investment required to execute the project.

HIGH LEVEL ASSESSMENT	DETAILED ASSESSMENT
Network Architecture Review	Network Architecture Review
Risk Assessment Based on NIST 800-82	Risk Assessment Based on NIST 800-82, ISA/IEC 62443
Manual Config Review of Hosts, Firewalls (Sampled Systems)	Passive Scanning Using Tools (for OT Assets < 100 for 1 site)
Policy/Procedures Review	Host Audit Using Tools In-Scope
	Policy/Procedures Review
Duration: 5 Working Days	**Duration: 8 Working Days**

02 Staff Augmentation,

where the client leverages the skillset of Payatu's security consultants and has them work with their in-house security team for an agreed-upon period of time.

03

Master Services Agreement

Minimum duration & projects commitment,

where Payatu conducts a T-shirt sizing of the client-proposed minimum scope and classifies each project as per complexity.

Minimum T&M effort commitment,

where Payatu proposes investment mapped with resource skill, resource experience, duration of T&M engagement, based on the client-proposed minimum commitment.