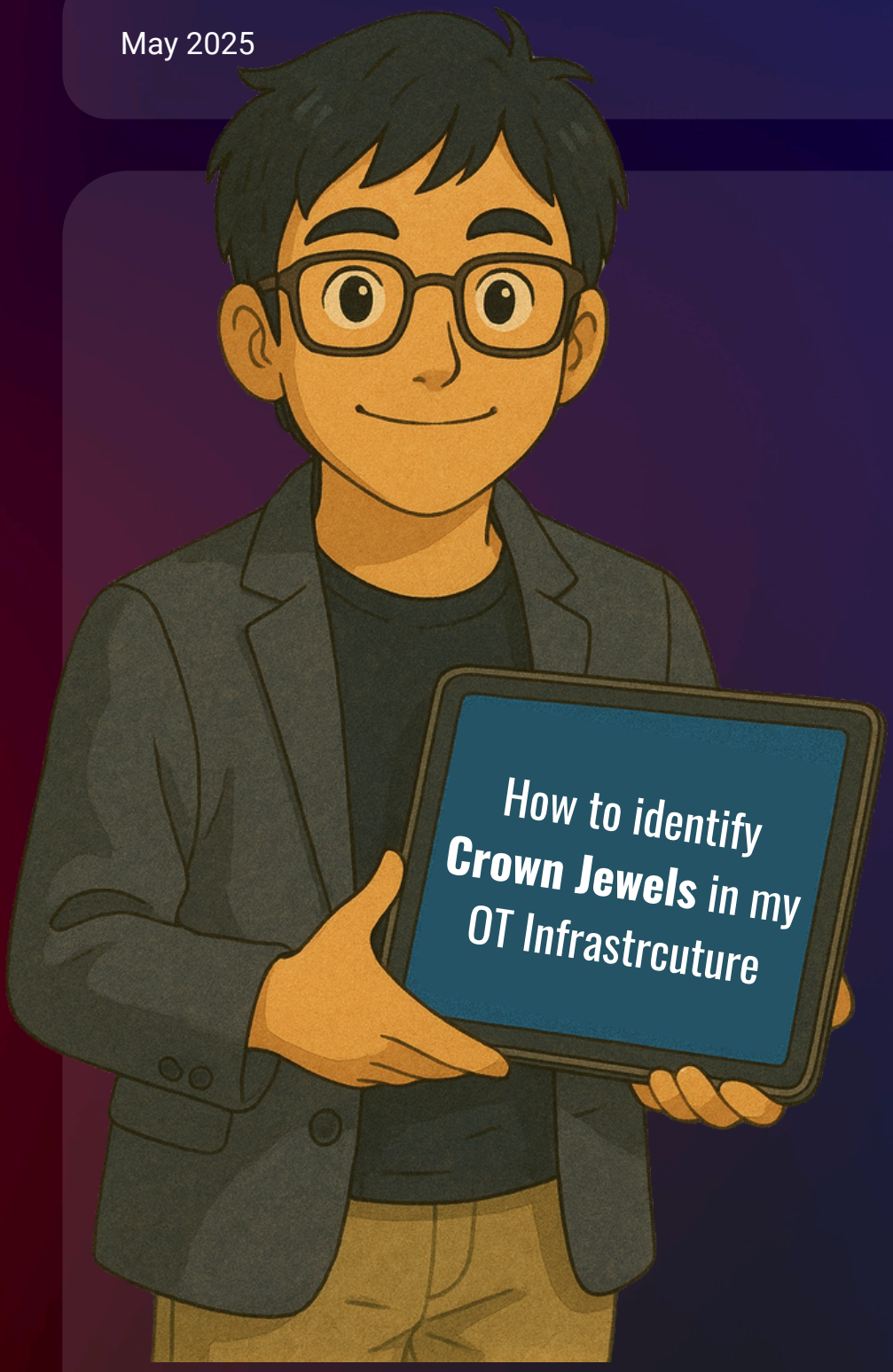
May 2025

Technical Series #1



A Guide to Identify Crown Jewels in your Organisation's Operational Technology

#otsecurityhuddle

OT SECURITY HUDDLE

www.syberwise.com

Disclaimer: This guide is intended for educational and awareness purposes only. It does not constitute regulatory advice or a substitute for a professional cybersecurity risk assessment. Organizations are encouraged to consult with qualified security professionals and tailor any recommendations based on their specific operational context.

What is this guide?

In this guide, we help organizations in critical infrastructure and industrial sectors identify their "**crown jewels**" — the most vital assets in their OT environments. These are the **systems, devices, or processes** whose compromise would cause the most damage to operations, safety, or reputation.

By pinpointing these high-value assets, organizations can make smarter decisions about where to focus their cybersecurity investments, apply controls, and prepare for incidents.

Why is this Important?

Not all OT assets are equal. Some are crucial to keeping operations running, ensuring safety, or meeting regulatory requirements. Identifying these assets is the first and most important step in:

- Risk assessments
- Network segmentation
- Incident response planning
- Compliance with regulations like NIS2 and India's CIIP framework
- Efficient use of cybersecurity resources

Without knowing what to protect, defenses may be misaligned, leaving the real targets exposed.

Standards and Guidance Referenced

This guide is built using best practices from globally recognized cybersecurity frameworks:

- IEC 62443: Industrial automation and control systems security (focus on risk-based asset identification and zoning)
- NIS2 Directive (EU): Emphasizes identifying and protecting critical digital infrastructure
- CISA (USA): Guidance on crown jewel analysis and OT risk management
- NCIIPC (India): Criteria for Critical Information Infrastructure protection in national sectors

These standards recommend a business- and risk-driven approach to critical asset identification.

Assessment Dimensions of Crown Jewel Identification

Before assessing assets, it's essential to understand the dimensions we evaluate:

1. **Asset Criticality**

Measures the inherent importance of the asset in maintaining operational integrity or safety. Assets directly involved in control, monitoring, or safeguarding industrial processes often fall into this category.

2. **Business Impact**

Estimates the consequences if an asset is compromised. Consider financial losses, regulatory penalties, service disruptions, and damage to reputation or safety.

3. **Threat Exposure**
Assesses how likely an asset is to be targeted or compromised. Factors include network accessibility, known vulnerabilities, outdated systems, and weak security controls.

4. **Process Dependency**
Looks at interdependencies and cascading effects. Some assets may not seem critical individually but could trigger large-scale failures if affected due to system coupling.

Questions

There are a total of 20 questions mentioned starting from page 7 of this guide.

Scoring Method

Each question is scored from 1 to 5. Use the following criteria:
ScoreMeaning

- **1** Very Low Criticality / Exposure / Impact
- **2** Low Criticality / Exposure / Impact
- **3** Moderate Criticality / Exposure / Impact
- **4** High Criticality / Exposure / Impact
- **5** Very High Criticality / Exposure / Impact

Final Asset Rating

Sum the scores across all 20 questions:

- 80–100: Critical Crown Jewel — Requires highest level of protection and continuous monitoring.
- 60–79: Highly Important — Prioritize controls and integrate in risk management.
- 40–59: Moderate — Apply baseline controls and monitor for changes in dependency/impact.
- <40: Low— Can be scheduled for longer-term improvement.

Assessment Questions Asset Criticality

Q. No	Category	Checklist Question	Scoring Guidance (1=Low, 5=High)	Scoring Levels
1	Asset Criticality	Which OT assets are responsible for essential functions in our operations?	1: Not essential – 5: Directly controls essential function	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
2	Asset Criticality	Would loss or failure of this asset immediately halt or severely impact production or safety?	1: No impact – 5: Causes immediate production/safety halt	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
3	Asset Criticality	Is this asset a single point of failure?	1: Fully redundant – 5: No redundancy, single point of failure	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
4	Asset Criticality	How difficult would it be to replace or restore this asset if it failed?	1: Easily replaceable – 5: Long lead time, hard to restore	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
5	Asset Criticality	Does the asset hold unique data or perform a unique control function that no other system can readily take over?	1: Replicable – 5: Unique, irreplaceable function or data	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High

Assessment Questions Business Impact

Q. No	Category	Checklist Question	Scoring Guidance (1=Low, 5=High)	Scoring Levels
6	Business Impact	What would be the operational impact if this asset were compromised?	1: No disruption – 5: Severe operational disruption	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
7	Business Impact	What financial losses could result from a breach or downtime of this asset?	1: Minimal loss – 5: Major financial impact	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
8	Business Impact	Would a security incident involving this asset violate laws or compliance requirements?	1: No compliance issue – 5: Severe regulatory violation	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
9	Business Impact	Could a compromise of this asset expose sensitive data or intellectual property?	1: No sensitive data – 5: Major IP or personal data exposed	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
10	Business Impact	How would an incident affecting this asset impact our company's reputation or customer trust?	1: No reputational risk – 5: Significant public trust loss	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High

Assessment Questions Threat Exposure

Q. No	Category	Checklist Question	Scoring Guidance (1=Low, 5=High)	Scoring Levels
11	Threat Exposure	Is the asset accessible from external networks or less secure environments?	1: Fully isolated – 5: Exposed to external/IT networks	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
12	Threat Exposure	Does this asset have known vulnerabilities or rely on outdated software/hardware?	1: Fully updated – 5: Known CVEs, unsupported tech	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
13	Threat Exposure	Do we have threat intelligence or history indicating this type of system is targeted by attackers?	1: No known targeting – 5: Widely targeted in the industry	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
14	Threat Exposure	What level of access controls and network segmentation protect this asset currently?	1: Strong controls – 5: Flat network, poor access control	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
15	Threat Exposure	Could an insider (malicious or negligent) easily misuse or damage this asset?	1: Unlikely insider risk – 5: High insider misuse potential	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High

Assessment Questions Process Dependency

Q. No	Category	Checklist Question	Scoring Guidance (1=Low, 5=High)	Scoring Levels
16	Process Dependency	Which critical processes or services depend on this asset's functioning?	1: No dependency – 5: Multiple critical processes rely on it	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
17	Process Dependency	If this asset is disrupted, what other systems would fail or be impacted?	1: No cascade – 5: Causes failure of many systems	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
18	Process Dependency	Are there alternative ways to perform the process if this asset is unavailable?	1: Multiple backups – 5: No workaround or backup	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
19	Process Dependency	Does this asset depend on other infrastructure that is outside our control?	1: Fully controlled infra – 5: High dependency on third parties	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High
20	Process Dependency	Would a compromise of this single asset cause a cascade of failures across the OT network?	1: No systemic effect – 5: High potential for cascading failure	1: Very Low | 2: Low | 3: Moderate | 4: High | 5: Very High

Liked our work??

Share your feedback on
info@syberwise.com