SECURING THINGS

FOR SMART & SAFER SOCIETY

Basic Best Practices Guidance for Implementation of Endpoint Detection & Response (EDR) Solutions in IT & OT/ICS Environments – a Vendor Neutral Prespective

09 April 2023 | Document Version 2.0

Author: **M. Yousuf Faisal** (IT & OT Cyber security Advisor/Consultant)

Founder, [Securing Things Limited]

[Email Contact]

Follow me on:

[LinkedIn] **|** [Securing:Things Newsletter] **| #SecuringThings**

Twitter - [@SecuringThings]

Table of Contents

List of Tables

1. Overview

Endpoint Detection and Response (EDR) solution, in addition to an essential security controls within an **enterprise/IT** on endpoints (servers, laptops, desktops), are now becoming also a critical need for securing endpoints within the critical infrastructure **Operational Technology (OT) / industrial Control systems ICS** environments, to provide adequate protection against growing and sophisticated cyberthreats like Ransomware and other forms of malware or malware-less attacks on the IT, OT/ICS or factory or automation or production control networks (all these terms are used).

However, implementing such EDR solution requires careful planning and execution to avoid any downtime or disruptions both to enterprise applications environment and to production operations.

Such projects are heavy in terms of time and resource requirements, lots of planning, coordination, discovery, getting multiple approvals, as well as Pre & Post deployment related administrative and technical activities.

Note: EDR solutions are not like Endpoint protection solutions which uses antivirus features, inspection of files for corruption, or analyse for suspicious behavior, against known signatures database, detect, and prevent mostly known attacks. EDR solutions uses Machine Learning (ML), Artificial intelligence (AI), behavior analytics and threat intelligence (TI) to detect threats and take the additional step of acting to eradicate threats and neutralize existing attacks by actively blocking and or isolating endpoints.

1.1. EDR Solution / Tool Selection:

But before that a key activity is to select the right EDR solution/tool for the IT & OT/ICS environments. There may be different scenario options to choose from and the decisions maybe based on some of the following considerations (not an exhaustive list):

#	Scenario Options & Decisions	Description / Considerations
1	**Scenario 1 – 1 EDR Solution**	**1 EDR Solution implementation for both in IT & OT/ICS** Existing EDR solution running in IT environment – validate if the solution has well known use cases for actual implementations in OT/ICS networks? *Tip: If the experience with the EDR solution in IT have been troublesome, perhaps best is to avoid experimenting in OT altogether – avoid additional trouble.*
2	**Scenario 2 – 2 EDR Solution**	**2 different EDR Solutions - Solution X implemented in IT and Solution Y in OT/ICS** Do consider the cons in such scenario – administrative overheads, added skills requirements, etc..
3	**Implementation Considerations - Influencing Decision process**	Decision is driven based on several considerations e.g.: • IT/OT Organizational Silos • feature set based on use cases / business needs. • Integrated IT/OT SOC or Separate SOC operations • ease of deployment • Skills set and learning curve. • Geographical support by vendor. • overall Cost and ROI and more.

Table 1 – EDR Implementation Scenarios and Decision Considerations

2. EDR Solution Project Lifecycle Execution Strategy

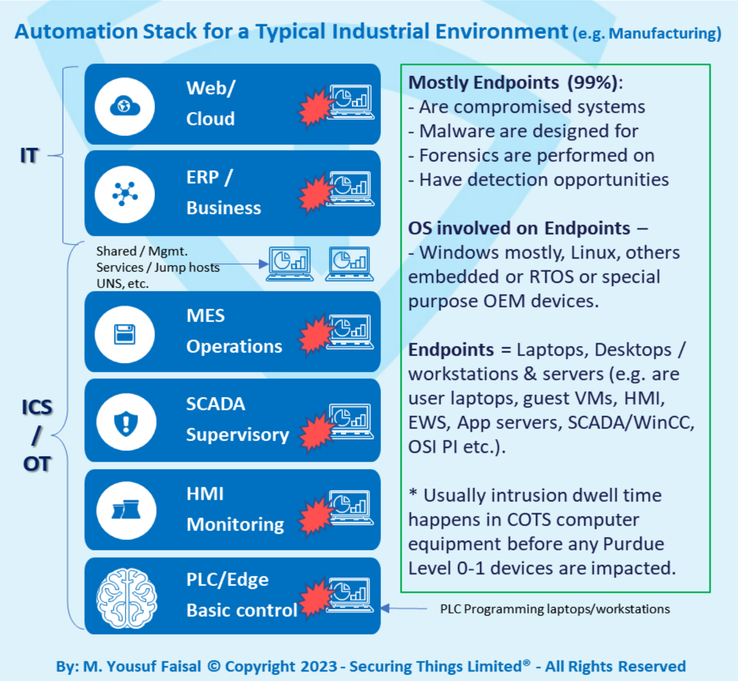
Assuming an informed decision has been made on the choice of selecting appropriate EDR solution(s) for both the IT and OT/ICS environments. Next steps are to create a safe, and as much as possible, an interruption free implementation in an OT/ICS/production control network operation, while also creating and maintaining OT/ICS critical applications exceptions and or exclusions strategy.

The following **3 Step or phased approach** can be adapted for both IT and OT deployments with minor differences in the approach:

(Please note there are many things to consider logistically, planning, budgeting, and resource wise – many of these details are not covered in this whitepaper).

2.1. Step 1 – Discover & Assess

The first step is to perform discovery activities, with a goal, to build a comprehensive inventory of all endpoints within the enterprise and OT/ICS/production control network environments (this includes endpoints in IT, OT DMZ, the factory network and on automation control network segments) and ensure existing network placement and network designs including zones/segmentation are evaluated.


Automation Stack for a Typical Industrial Environment (e.g. Manufacturing)
IT
Web/ Cloud
ERP / Business
Shared / Mgmt. Services / Jump hosts UNS, etc.
ICS / OT
MES Operations
SCADA Supervisory
HMI Monitoring
PLC/Edge Basic control
PLC Programming laptops/workstations

Mostly Endpoints (99%):
- Are compromised systems
- Malware are designed for
- Forensics are performed on
- Have detection opportunities

OS involved on Endpoints –
- Windows mostly, Linux, others embedded or RTOS or special purpose OEM devices.

Endpoints = Laptops, Desktops / workstations & servers (e.g. are user laptops, guest VMs, HMI, EWS, App servers, SCADA/WinCC, OSI PI etc.).

* Usually intrusion dwell time happens in COTS computer equipment before any Purdue Level 0-1 devices are impacted.

By: M. Yousuf Faisal © Copyright 2023 - Securing Things Limited® - All Rights Reserved

Figure 1 – IT & OT Automation Stack for an Industrial Environment

2.1.1 Methods to Use

Both manual (factory walkthrough/physical inspection against the existing asset inventory list) and automated means must be utilized to identify and validate these OT assets / endpoints.

#	Item	IT	OT/ICS
1	Asset Inventory with Application discovery	Gather via: - Existing Asset discovery or asset management tool - Active inventory scans - Application discovery - Pcap collection - Vulnerability Scanners	Gather via: - Asset inventory list (excels) - Passive discovery scans - Pcap collection - Vulnerability scanners / Active scans (used with caution)
2	Tools	- Free (open source or custom develop scripts) - Commercial tools	- Free (community based or custom scripts) - Specialized OT security tools (Anomaly detection or OT IDS) - App specific discovery (e.g., Siemens Simatic WinCC comes with a built-in tool called "Installed Software" utility

Table 2 – Methods for Endpoint Assets & Application Discovery

Regardless, of the tools used to discover, key objective is to get an accurate endpoint inventory including details on critical applications used (ideally with their paths).

Document the inventory in detail including but not limited to:

- make, model, OS / software version, and patch level of each endpoint.
- Subnetwork / gateway IP address
- Identify the network architecture and topology of the production control network.
- In addition, should also include list of all OT applications, databases, scripts, services, and associated project paths, running on the network.

Tip: Ensure to keep the inventory of endpoints & critical OT application up to date for each plant site (both during and after the implementation). Relevant IT/OT plant teams are responsible for ensuring this as business-as-usual (BAU) basis.

2.1.2 Identify Critical Processes and Applications

The next step, once an asset list is ready, is to review and identify the critical processes and applications that are essential to both the enterprise IT and to industrial operation of running at a facility/site.

For IT – This includes any business-critical applications e.g., ERP, Accounts Receivable / Payable, and or other important software.

For OT/ICS – Need to go a bit further in understanding the OT/ICS production process. This may include (but not limited to), any software or hardware that is critical to production, such as Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), Historians, OSI Pi, Engineering Workstations (EWS), and Supervisory Control and Data Acquisition (SCADA) systems software, MES software, OPC, Historian, and applications like WinCC, Factory talk, iFix, Proconwin, MSSQL server, and other critical applications running on the factory / automation or production control network. Make sure to Identify the dependencies between critical processes and applications.

For e.g., Siemens Simatic WinCC have several dependencies like, OPC, Microsoft SQL Server, Project files under a designated project paths defined for the specific OT/ICS environment.

Manual Method: To extract a list of important files/folders from these critical OT applications, can perform following:

- Open command prompt by right clicking & selecting "**Run as administrator**".
- Go-to the required application / project files folder **C:\cd <use_target_foldername>**
- Where, use_target_foldername is relevant application path e.g., SCADA/MES, WinCC, MSSQL etc.
- Type **C:\ use_target_foldername\dir /s /b /o:n > "C:\files&folderlist.txt"**

  Where, files&folderlist.txt = can be any filename of choice.
- Use the extracted list to identify potential files/paths for potential exceptions, exclusions in later step 3.

Use other means to extract software details e.g., in case of Siemens Simatic WinCC software:

- Run the **Siemens Simatic WinCC utility** called "**installed software**" and it will generate an output that can be extracted in .csv format. Refer to Video HERE.

2.1.3 Conduct Basic Risk Analysis

After identifying the critical processes and applications, project folders, dependent applications, scripts and tools, the next step is to do some basic risk analysis. This should involve analysing the security risks associated with each endpoint and application identified earlier. Prioritize the risks based on their potential impact to production. This may also involve identifying potential vulnerabilities, known exploits, and other security risks.

Build an application inventory per site / plant and against the endpoints. Based on the level of risk associated with each endpoint or application, this will help to prioritize any of the required exclusion, exception, and/or whitelisting strategy to be executed at later stage in the project lifecycle.

Tip: Many implementations miss these tasks at start of the project and usually perform this in step 3, typically in response to certain legitimate applications being blocked and processes interrupted / shutdowns and only to find several unhappy system owners, executives, and a bunch of escalations to deal with. Avoid these pitfalls.

2.1.4 Define Standards and Principles

If not already, its' recommended that certain best practices standards and principles are defined and documented that would help guide execution for reminder of the project:

Below table highlights example best practices standards & principles:

- All endpoints that are commonly affected by malware (e.g., Windows, Linux etc.) must be protected by EDR solution (both for IT and OT/ICS environments).
- Define Dos and Don'ts on when an endpoint OS is not compatible with EDR Solution

- Outline SLAs with internal/external SOC or team that'll be managing EDR.
- In addition, endpoints should also have following practices to be followed:
  - cyber hygiene industry best practices by changing all vendor default settings, removing / disabling all unused accounts, services, ports, applications/modules, features etc. and only use secure protocols or protocols over secure communication channels.
  - Enable logging and monitoring.
  - High availability, backup and restore processes and methods defined.

2.2. Step 2 – Architect/Design and Implementation

Now, with all the discovery work done. Time to design / architect the solution and execute implementation and deployment.

2.2.1 EDR Solution - Backend Management Components

Based on the architectural discovery done in Step 1, the placement of backend EDR solution components e.g., management console can be decided and how the EDR agents that will be installed on the endpoints should reach the management console to get the configuration and period updates would need to be designed.

Be prepared to make certain network changes – both at global and at the site level, as current design may be using old methods in terms of their network designs / architecture, not suitable for EDR solution implementations.

Most of EDR solutions are now cloud based, meaning that the management interfaces (consoles, aggregators, cores, threat intelligence packs and other components) are hosted in cloud managed by solution vendor. Several do offer the option to do a Hybrid deployment with on-prem and cloud setup.

Even if it's decided that same EDR solution is to be used for both IT and OT/ICS environments, it's recommended to at-least use different tenants to have a different set of policies, exceptions, exclusions, for IT endpoints (which are usually more restrictive) and for OT/ICS endpoints (which may require more customization), for better monitoring & management.

Note: The number of solution components, architecture, different from one solution to other. The types of architectures are not covered as part of this whitepaper.

Set up backend solution components (i.e., management consoles and access) per following:

- aligned with internal policies (e.g., naming conventions, password policies, MFA etc.)
- for multi-site deployment: ensure endpoint agents groups names reflect the naming convention and identify location easy for easy management support.
- Follow vendor recommended best practices guidelines.
- Allow specific IP, protocol/port specific firewall policies required to run solution.
- Change vendor defaults (e.g., passwords, unused user accounts etc.)

- Maintain strict access controls based on principles of least-privileges on a need-to-know basis and have access control trackers. Certain users only required read access should only have read access.

- Choose vendor recommended security policies and playbooks (most solutions come with built-in policies/playbooks out of the box – review them and tweak if required in consultation with the vendors for the specific environment).

- Integration with other solutions happens here as well – AD/LDAP, SMTP, SIEM etc.

2.2.2 EDR Solution – Agents

Use a script or an installer package with the agreed latest stable agent version of EDR Solution to be rolled out to in-scope environment. Ideally test, before deploying in production.

For IT environments typically this can be pushed via group policy to be installed on multiple endpoints at the same time. For OT/ICS environments, may or may not have the ability to do multiple or selective push to deploy the agent software (as many still don't have active directory environments), but in case an OT AD is present, be extremely careful on pushing the agents on selective machines that are for sure not going to cause operations downtime.

Tip: For older versions of Windows 8, 7, Vista, XP etc. may require certain level of patches to be installed and may require reboots, so consider the impact on endpoints and on any respective OT/ICS processes. May need to schedule such installs only during maintenance windows or in case of high-availability setup on backup/fail-over machines first.

For OT/ICS endpoints - By this time one should already have an idea that whether certain OT critical applications are in supported EDR Solution list. Consult OEMs / vendors. In many cases, they won't be supported. In such scenarios, the only resort is to perhaps apply full application exclusions.

Note: EDR solutions comes with pre-built policies for both running in monitoring mode (sometimes called Monitoring or Simulation or Alert mode) and protection mode (sometimes called Blocking or Protection mode). These terms may vary from solution to solution.

It's important to ensure that agent is running in monitoring/simulation/alert mode for certain time periods (2-to-4 weeks or maybe less) for the solution to learn the normal behavior.

2.2.3 EDR Solution – Documentation

Develop documentation around following elements:

- Site / plant implementation task completion status and Approval / sign-off.

- EDR Solution Architecture/Design, Implementation & Maintenance – For Backend teams managing / monitoring the EDR solution.

- EDR Solution Support Manual for End Users (IT and OT/ICS Site Teams) – For front end users or systems owners or plant / site teams.

- A clear guidance / process flow highlighting key point of contacts (email/phone support) needs to be provided as well for any urgent issues to be fixed. This can be on how to contact SOC and the SLA expectations outlined.

2.3. Step 3 – Monitoring and Management

Hopefully by now once the implementation (basic installs) is done, monitoring and management step begins.

There's a short transition period, where the deployment team continues with the project from site to site while tackling any issues that surfaces (e.g., blocked applications, addressing triggered events, applying exceptions/exclusions (next section) and more.

Monitoring and Response processes / procedures are defined. Here' they would vary between response processes for IT endpoints vs. endpoints in OT/ICS networks.

Usually, the implementation team is different than the team that's going to monitor and manage the EDR solution moving forward. Therefore, there needs to be a knowledge transition / transfer that would also occur between the teams (in most cases, Implementation consultants and the internal/external SOC teams). This is a daunting process, particularly in cases where there's been lack of documentation done in earlier stages.

Ensure all documentation is reviewed as part of the hand-over process, any missing elements are documented and agreed between the teams.

2.3.1 Review Events Triggered & Applying Exceptions/Exclusions

After running agents for a site for some time (at-least more than 48 hours), review the triggered events for a particular site/location/plant. Events triggered are the anomalous behavior that the EDR solution have discovered based on default/custom policies and threat intelligence applied on them.

Tip: Beware, there's always some false +ves. So don't think of it as install and forget exercise. From time to time, there's a need to review these events and approve legitimate activities.

For each triggered event, EDR may have detected a possible signature/behavioural issues with a file or process or activity. For each event, check and verify file hashes against resources like virus total and other similar services for known infections. Person performing these tasks, should be familiar with the tool capabilities and interpreting its logs and file activities.

Usually, management interface provides the ability to export these event details to be shared with systems owners and technical folks to verify whether it's a legitimate application, file or a program executable that requires any exceptions to be applied and or if there's a need for an exclusion list for EDR solution to ignore from inspection (usually because of computability issues).

For any exception or exclusions request, it's important to capture:

- Application name, version, path, and files where events were triggered.
- brief purpose / use of the application and
- the source from where the application was received/downloaded (e.g., CD, USB, download from vendor X website etc.).

Once the exclusion, exception, and/or whitelisting & protection strategy has been implemented, it is important to continuously monitor and test the production control network to ensure that the strategy is effective and not causing any disruptions to production. Test the EDR solution to ensure it is not causing any disruptions to production. Any issues or anomalies should be investigated and resolved promptly.

2.3.2 Periodic Reviews and Updates

Finally, it is important to periodically review and update the exclusion, exception, and/or whitelisting strategy to ensure that it remains effective against new and emerging threats. This can be done by conducting security assessments the production control network. Ensure the policy is up to date with any new or emerging threats.

On an ongoing basis, both the backend solution components and agents need to be updated to the latest release with security updates, bug fixes etc. A process should be in place for the review and deployment of these updates to the production environment.

By following this approach or methodology, organizations with both IT/enterprise and production control network / manufacturing facilities can have a smoother experience deploying an EDR solution in both environment and in particular a safe exception, and/or exclusion, strategy for their OT/ICS/production control network environment, while ensuring no downtime or disruptions to production.

2.4. Scope Applicability

This whitepaper may include some of the key work processes and security measures used throughout the project lifecycle of EDR solution from planning, design to implementation to monitoring to decommissioning to reduce the risks from cyber security threats to both the IT and the Industrial Automation and Control System (IACS) to levels deemed tolerable by an industrial organization.

2.5. Limitations & Exclusions

This whitepaper highlights only the key basic elements (a starting point), (may not cover entire set of tasks, activities, or requirements from running such an implementation project) – may be updated in future.

Excluded elements are (but not limited to): Functional, Configuration, installation steps, operational, Reliability, Maintenance, Hazards, Safety and environmental or project management requirements and non-security controls to be put in place for preventing unwanted events and project risks.

Hope this basic guidance would help in preparation for the first or next EDR deployment.

It's a great day to start "Securing Things" i.e., Endpoints in IT & OT/ICS production control networks.

--**END OF DOCUMENT**--