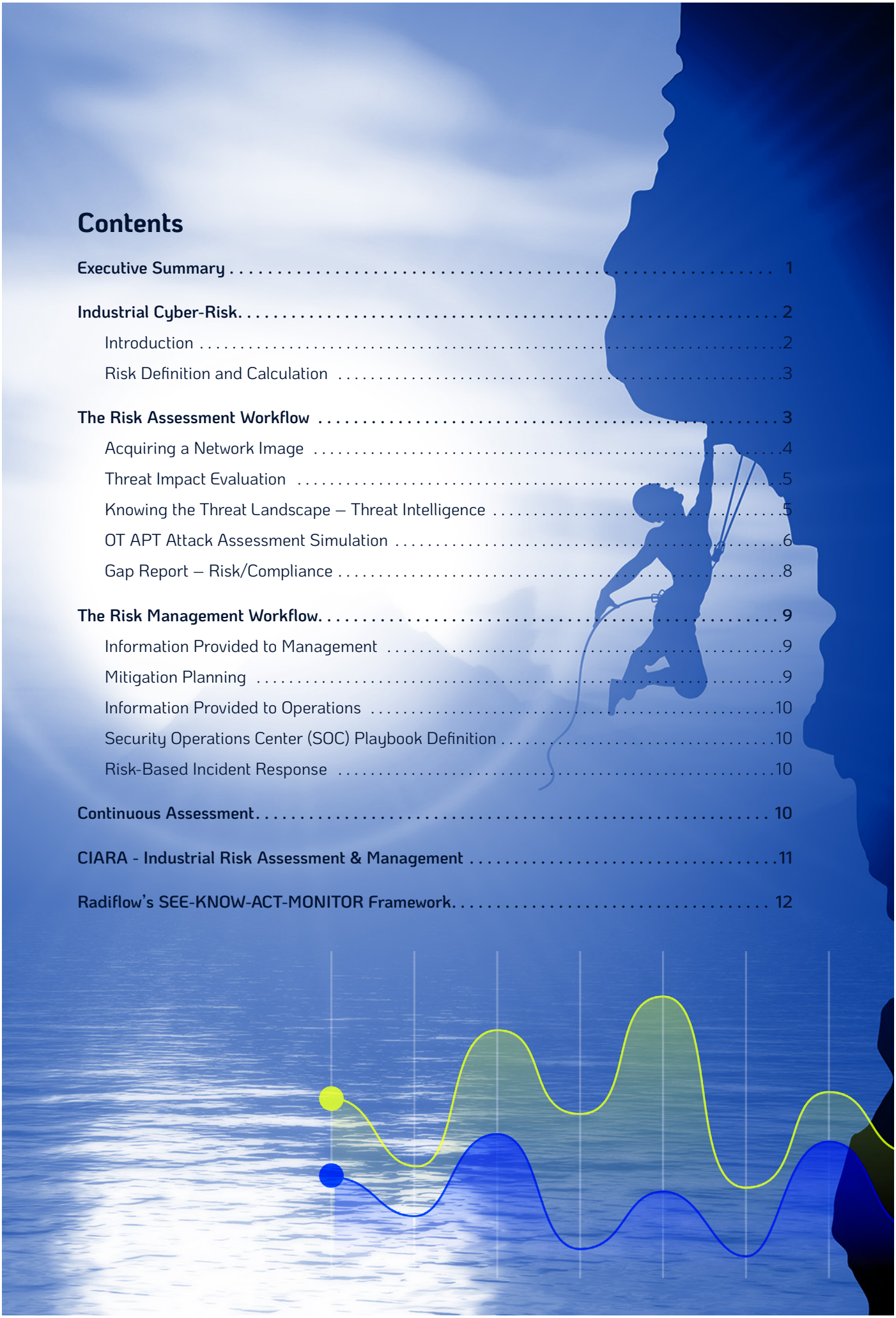
Radiflow

Risk Assessment & Management for Industrial Organizations

Contents



Executive Summary

According to the American National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), "Cyber-actors have demonstrated their continued willingness to conduct malicious cyber-activity against critical infrastructure."

Cyber incidents related to industrial and critical infrastructure have a tangible real-world impact: they can endanger lives, disrupt both day-to-day life and business operations and impose financial damages on industrial firms (as an example, the cyberattack on the Colonial Pipeline forced the company to cease operations while the incident was investigated, which in turn caused fuel shortages across the US east coast as well as millions of dollars in losses.)

As OT networks become more complex and digitized as they transition to Industry 4.0, managing OT cyber-risk also becomes more and more challenging. There's a dire need for a more methodical approach to industrial risk assessment, for handling and using large amounts of data and producing actionable insights for management and operations.

This guide, based on industry best practices and standards as well as on Radiflow's extensive experience in risk management, is designed to help industrial operators implement risk assessment and management processes.

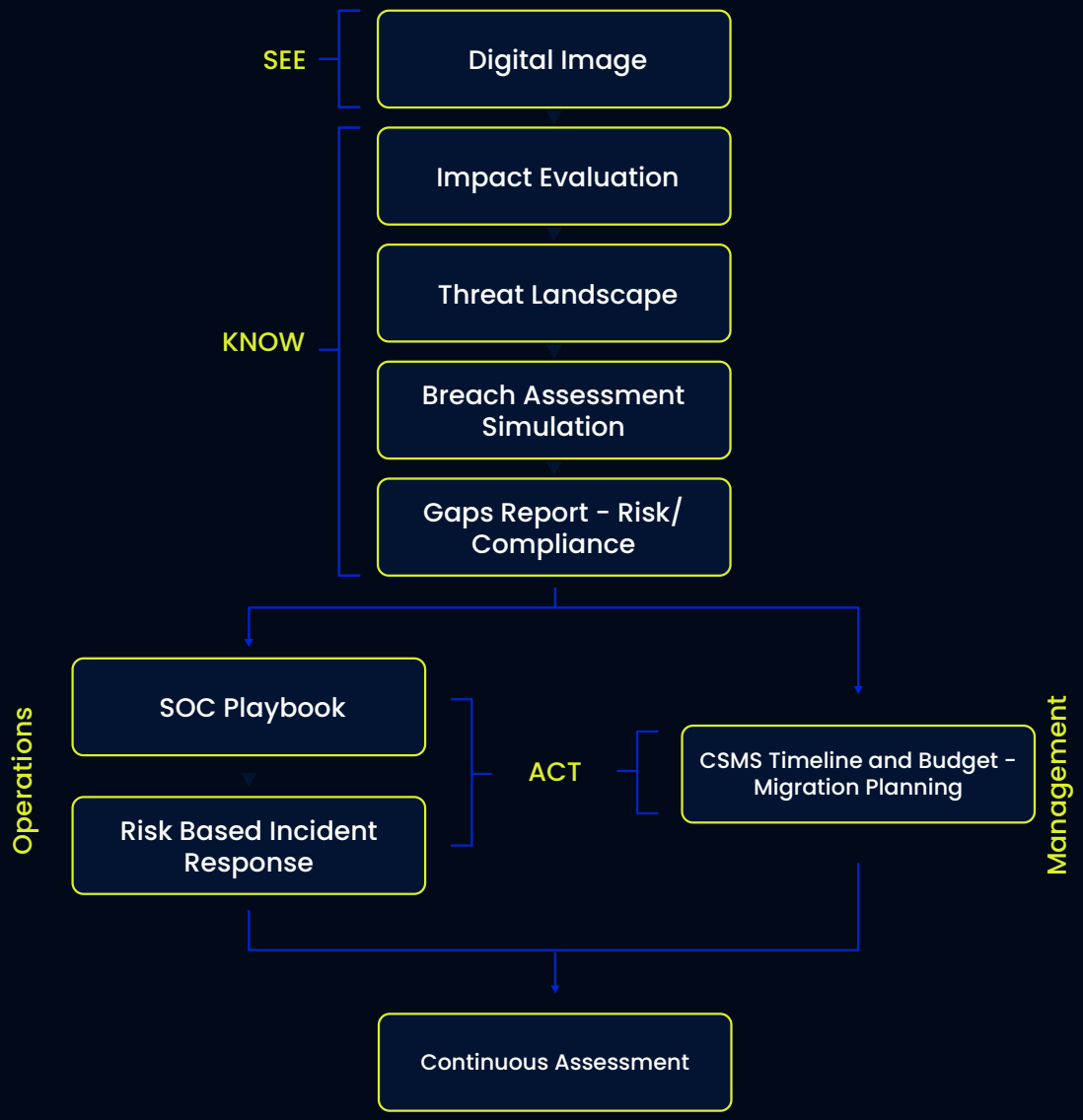
The methodology presented herein encompasses all steps involved, from gathering relevant information and intelligence, through mitigation planning and implementation, and finally continuous risk assessment and management.

Industrial Cyber-Risk

Introduction

In recent years the increasing digitization of the production floor (Industry 4.0) has led to a tide of cyber threats—all while risk assessment processes, which up until now were done manually, have failed to address the full scope of the issue. The complexity of today's Industrial networks, as well as the complex standards ICS networks are required to follow, calls for an automated cyber risk management process. Simply put, the era of "eyeballing" network risk is long–gone.

The methodology presented in this guide covers obtaining visibility of the entire OT network being assessed, including all devices and connections, through knowing all the information needed for an accurate assessment - your network risk posture, system vulnerabilities and compliance gaps, to action - drafting and implementing a cyber-security roadmap which prioritizes the actions needed for optimal mitigation.



Radiflow's Risk Assessment & Management Workflow

Risk Definition and Calculation

Before approaching the “how” of cyber risk assessment, it’s important to establish the “what” – the various factors that makes up risk in the context of Operational Technology (OT) network risk assessment and management.

In this document, impact is defined as a safety hazard, damage to property, denial of control, loss of availability, loss of control, loss of productivity and revenue, or any other harm that can occur as a result of a failure in the OT network.

To calculate the risk to assets in the OT network, two factors must be taken into consideration: the likelihood of a successful cyber attack and the impact of the attack. In the case of OT networks, a cyber attack can have both a business impact and a real world impact, as OT networks control physical assets.

The equation is as follows:

Likelihood

- Threat & adversary characteristics
- Organization's locale & sector
- Network vulnerabilities detected
- Mitigation controls installed

×

Impact

Assessment of the damage caused by a cyber-attack, per zone and network-overall

=

Risk

Used by CISOs/stakeholders to assess the state of the OT network and the effectivness of security measures

Using the resulting risk scores, decision makers can create a long-term network security plan which accounts for both cyber and business considerations, and prioritize mitigation measures based on criticality, impact on overall security and available resources.

The Risk Assessment Workflow

The risk assessment workflow proposed by Radiflow is based on simulating numerous combinations of advanced persistent threats/ tactics (APTs) relevant to the System under Consideration (SuC) and their corresponding mitigation measures. Radiflow’s proposed APT simulation method uses as inputs:

- A network digital image, as an alternative to simulating attacks on the production network itself
- Threat intelligence data about relevant attackers and attack tactics
- Specific network characteristics, as reported by the user
- CVE vulnerability database

Acquiring a Network Image

To perform an OT network risk assessment, you need to be able to see the network; therefore an image of the SuC must be created.

Industrial networks consist of multiple devices of different types. Each device has its own software, vulnerabilities, operating system and other properties. Networked devices also share information and commands using communication channels. All of this information needs to be collected and shaped into an accurate network image.

Digital network images are self-learned network models that include all devices & device properties, device-specific vulnerabilities, connections and ports, communication protocols and any other network characteristic. Radiflow's risk assessment uses a digital image generated in its iSID industrial threat detection & monitoring system. The digital image is constructed using mirrored streams of all network data over a representative period.

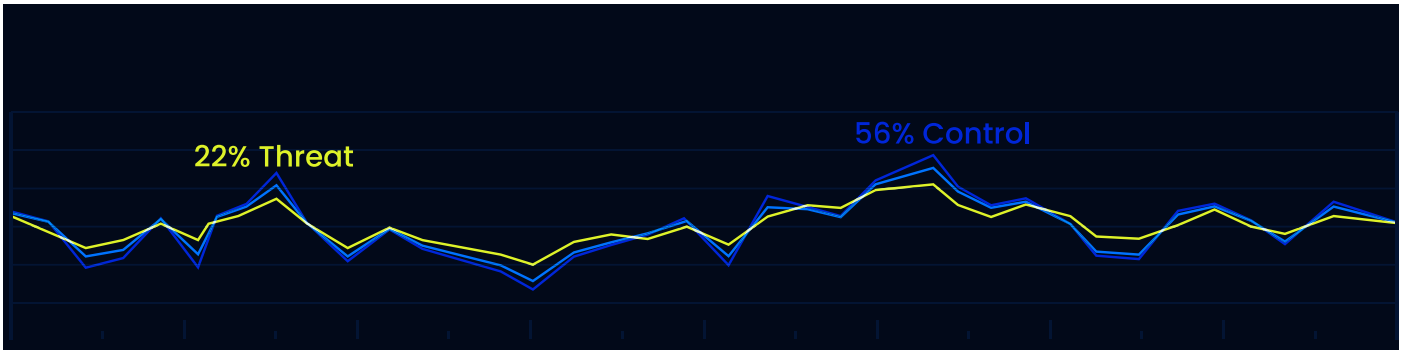
Digital network images are also deterministic: As the properties of industrial networks remain constant unless a change is made to the network, the digital image can be used as an accurate representation of the network for prolonged periods of time, enough for running a thorough breach simulation. This makes digital image-based APT simulations a preferable option to other simulation methods, as it poses no danger whatsoever to the network, while producing accurate results.

Another advantage of running a digital image-based simulation is that it provides flexibility to perform both unmitigated (i.e. not accounting for mitigation measures) and mitigated breach simulations, to test the effectiveness of mitigation controls.

In addition to serving as an input for risk analysis, the digital image of the ICS network is used as a baseline for anomaly detection (indications of breaches and/or other changes to the network) and for presenting the user with a visual "map" of the network, showing all connections, network levels and business processes, down-drillable to each and every device's full properties.

As per the ISA/IEC 62443 standard, the SuC is required to be divided into zones (network segments that represent business units that share the same security requirements) and communication conduits, which need to be reflected in the network image. The added value of this practice is that it enables risk assessment and mitigation per zone/business process.

The obtained digital image, being a true representation of the network, enables running a full OT APT attack simulation of hundreds of possible attacks. Given this simulation, security teams can assess potential attack vectors and the mitigations needed to fend off these attacks.



Threat Impact Evaluation

Radiflow's breach & attack simulation also assesses the potential overall impact on each and every zone and business process, based on the impact to business operations, safety and worst-case scenarios in which the SuC has been compromised.

Radiflow recommends the following scale for zone impact:

1-2	Minor business impact
3	Medium business impact
4	High business impact
5	Safety/HSE impact

The threat impact to different zones determines each zone's tolerable risk, which in turn serves as the basis for zones' Target Security Levels (SL-T).

Knowing the Threat Landscape – Threat Intelligence

Threat intelligence (TI) is knowledge that allows companies to prevent or mitigate cyber attacks. TI provides context: who might attack, what their capabilities are, and what indicators of compromise in your SuC to look for. This helps to make informed decisions as to hardening the OT network.

TI data is continuously gathered by specialized organizations that track attackers' motivations, the tools they use, the internet servers they own and more.

There are three types of TI: strategic, tactical and operational.

Strategic Threat Intelligence

Strategic TI consists of high-level information that helps risk managers understand current risks and identify upcoming risks, of which they are yet unaware. This may include the financial impact of cyber activity, attack trends, historical data or predictions for each threat actor's activity.

Companies should obtain strategic TI that is both generally relevant to them like malicious cyber campaigns that are globally widespread, as well as more focused data about current threats to their sector and geographic location. Using this information, industrial operators can weigh the risk posed by each possible threat and allocate budgets and resources for mitigation.

Tactical Threat Intelligence

Tactical threat intelligence includes domains, IP addresses and file hashes, and is normally consumed through security sensors. Tactical TI feeds are used to update the organization's investigative or monitoring sensors, e.g. firewalls and domain filtering, by blocking attempted connections to malicious servers.

Operational Threat Intelligence

The third type of TI is operational threat intelligence. This type is used to share information about how threat actors conduct attacks. Operational TI is used by incident responders to ensure that their defenses and their investigation capabilities are up to date with the latest attack methods.

Operational TI is often obtained by reading technical white papers or by communicating with peers in other organizations who have observed attacker behavior.

A widely-used modeling framework is MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK), designed to identify the most reliable indicators of sophisticated attacks. The framework presents commonly-observed adversarial tactics and techniques, based on intelligence gathered on many advanced persistent threat (APT) groups.

In this framework, tactics represent types of adversaries' actions (e.g. reconnaissance, initial access and more); and for each type/tactic, the framework details its exact methods of operation, or techniques. For example, techniques for performing initial access include: spearphishing attachment and exploit public-facing application, among others. MITRE also released a dedicated model for ICS, called ATT&CK ICS.

Combining information from multiple TI types can provide a holistic view of the threats to a specific sector in a specific region.

In some cases, it can also provide quantitative information about the loss magnitude of a cyber event or the threat event frequency. Using tactical and operational TI is especially important to the next step required for a comprehensive risk assessment – Breach Assessment Simulation.

OT APT Attack Simulation

Knowing the threat landscape provides important information about the potential threats to the SuC, but it doesn't provide insight into the SuC network's vulnerabilities or other properties, which are imperative for efficiently transforming the TI into actionable information.

Organizations such as NIST, ISA and CSA have developed methodologies for helping organizations to better understand and improve their cyber-risk management. The first step in these methodologies is identifying network vulnerabilities. This is done by imitating an attacker's behavior – looking for the same "holes" in the network that a hacker would look for. Organizations often use actual (ethical) hackers to perform active penetration testing for detecting security flaws in the network. Analysis of the TI data allows security personnel to properly define pen-testing test cases to imitate each attacker's activity and to ensure that the protected network has sufficient defenses in place.

The combination of threat intelligence and an aligned penetration testing plan provides a strong mechanism for identifying network weaknesses. However, while active penetration testing is absolutely necessary for completing the TI-based identification phase, it is considered dangerous – the risk of accidental damage during testing may actually be higher than that of an actual attack (accounting for the low frequency of real-world attacks).

As an alternative to active penetration testing, a threat intelligence-based APT simulation can be performed. This method consists of two stages:

1. Constructing a highly-accurate virtual network model, including all devices, security products, software, protocols used, ports, connections and other properties, as well as known threats.
2. Simulating each attacker's activities within the network model, based on their known capabilities and activity patterns.

As mentioned, the simulation should include three main inputs:

1. **The network image of the OT network**: A virtual representation of the SuC, as discussed above in the first step of the risk assessment
2. **Currently-deployed security controls (as self-reported by the user)**: The IEC 62443 standard determines how to implement protective measures based on the four Security Levels (SL) for each zone and conduit, grouped into seven fundemental requirements (FRs):
   - Identification and authentication control (IAC)
   - Use control (UC)
   - System integrity (SI)
   - Data confidentiality (DC)
   - Restricted data flow (RDF)
   - Timely response to events (TRE)
   - Resource Availability (RA)

   Using this standard allows determining the Security Assurance Level for each zone and conduit, which in turn affects the network's risk score. When conducting the simulation, it is recommended to perform it first without accounting for security controls (i.e. unmitigated) to assess the most severe scenario.

   Determining the unmitigated risk score first, with no consideration to the security measures in place, helps calculate the maximum risk impact score, while the complete risk assessment, based on simulations that account for installed security controls, will produce the network's actual risk score.
3. **The adversaries and threats typical to the network's sector and locale**: Radiflow's breach and attack simulations deprioritizes attackers and tactics that are not relevant to the SuC's sector and region.

As part of the assessment, all of the attacker's possible moves should be simulated, iteratively simulating the attack "moving" between devices. Modeling attacker capabilities is an essential step in estimating the person's route through an ICS network.

Radiflow recommends identifying three levels of attacker capabilities for exploiting various protocols:

- Low – attackers who are capable of only exploiting common IT protocols
- Medium – attackers who are capable of exploiting both IT and OT protocols. However, they are only capable of exploiting OT protocols that have open specifications
- High – attackers who are capable of exploiting both IT and OT protocols, including reverse-engineering proprietary OT protocols.

Likewise, attacker capability can be modeled by the attacker's ability to exploit device vulnerabilities in order to affect a device's functionality. For example, a three-level attacker capability ranking for exploiting device vulnerabilities could be:

- Low: attacker is capable of exploiting only publicly known vulnerabilities with publicly available exploits
- Medium: attacker is capable of developing their own exploits for known vulnerabilities
- High: attacker is capable of performing extensive research to find zero-day vulnerabilities and is capable of exploiting them

At the end of this step, each device in the network should be assigned a base score for compromise likelihood.

The overall likelihood of targeting the company's network should also be taken into consideration, with respect to other possible networks from the same region and sector. A thorough APT threat assessment should also include an evaluation of the likelihood of different scenarios such as damage to property, decreased safety or loss of revenue.

Each scenario has unique attributes, which makes it possible to estimate the likelihood of the scenario to materialize.

The likelihood metric reflects the probability of compromise. It should be calculated based on the compromise likelihood of all zones' assets, taking into consideration each zone's attack surface, vulnerabilities, links, protocols and security events, as follows:

Low Probability of Disruption (0%- 40%): 1-5

Medium Probability of Disruption (41% -75%): 4-6

High Probability of Disruption (76%-100%): 7-10

Gap Report – Risk/Compliance

The OT APT Assessment process assigns a risk score, breach likelihood, impact and SLA (achieved security level) to each zone in the SuC. After assigning an SLT (target security level) to each zone, reports in different level of detail are issued, indicating existing security gaps, as well as for security and compliance parameters.

Recommended reports include:

Report	Information included
SuC Visibility	Devices and their properties
High-Level Risk Assessment	Zones, conduits, SLTs
Detailed Cyber Security Risk Assessment	Threats, vulnerabilities and security controls, as well as a detailed assessment of unmitigated risk, tolerable risk, STL, SLA, residual risk, likelihood & impact
Network Risk Assessment	Assets, protocols, open ports, remote connections, vulnerabilities, business processes, operational activity, cyber events, recommendations for security posture improvement, hardening plan

The Risk Management Workflow

In order to transition from assessment to action the data collected during the assessment must be made availebla and presented to both the management and the operational sides of the company. Both sides greatly impact the way risk is managed, so providing them with relevant actionable data as possible, is crucial.

Information Provided to Management

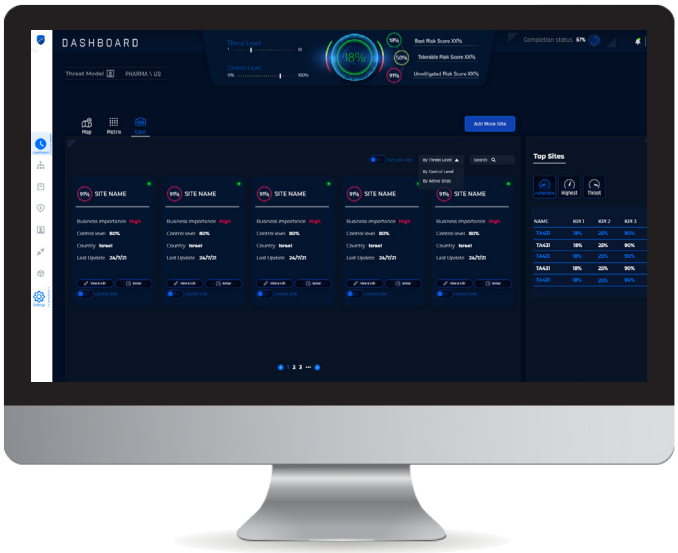
Typically, management reports present high-level findings: overall risk scores for zone and conduits, business processes' risk scores, likelihood of different scenarios, etc. Management should also be made aware of the resources available and needed for risk mitigation, as well as the possible impact different security measures will have on the overall risk.

Providing management with different combinations of the assessment data and mitigation possibilities – for example, the attack likelihood score along with the potential impact score and mitigation plan aimed at reaching a certain risk score – will enable decision makers to make data-driven decisions and act accordingly.

Mitigation Planning

Once the risk assessment is completed, management can turn its attention to planning the right mitigation steps for lowering risk scores. The mitigation steps can focus on lowering either the likelihood or the impact of an attack, and should be prioritized by different considerations such as the importance of the relevant scenario to the business, lowering the overall risk score and budget constraints.

Assessing the effectiveness of different mitigation steps can be extremely difficult. That is why it is very important that the risk assessment data and the assessed impact of different mitigation steps is easy to understand and compare.



At the end of this step, a mitigation plan is drafted. The plan should include action items, target dates for implementation and budget as well as post-mitigation achieved and target security levels (SLA & SLT) for each zone.

Many companies lack the resources and/or the expertise needed for deploying and maintaining security measures in their industrial networks. Using a CSMS will help manage the process, better plan expenditure, and assist in choosing mitigations that maximize cybersecurity ROI. The CSMS should display the risk scores, SRs and more, by different prioritization categories.

The system should also allow the user to enter cost and target completion date for each security control, to meet budgetary constraints.

In addition, using a CSMS should enable the user to examine different "what if" scenarios and see their impact on the risk score and the SuC's operation without making changes to the actual network, which may have real-world impact such as high costs and downtimes.

Information Provided to Operations

The data gathered during the risk assessment is extremely valuable to the cyber security operations side of the company. Information about assets, vulnerabilities and impact can help in planning incident-handling processes, incident triage and more.

Security Operations Center (SOC) Playbook Definition

An incident response playbook is a set of actions to be executed when triggered by certain cyber events. SOC Playbooks are designed to help SOC teams respond to incidents. Using the risk assessment data, the playbooks can include information such as risk scores of zones and business processes according to different scenarios, which will help in triaging and responding to incidents.

Risk-Based Incident Response

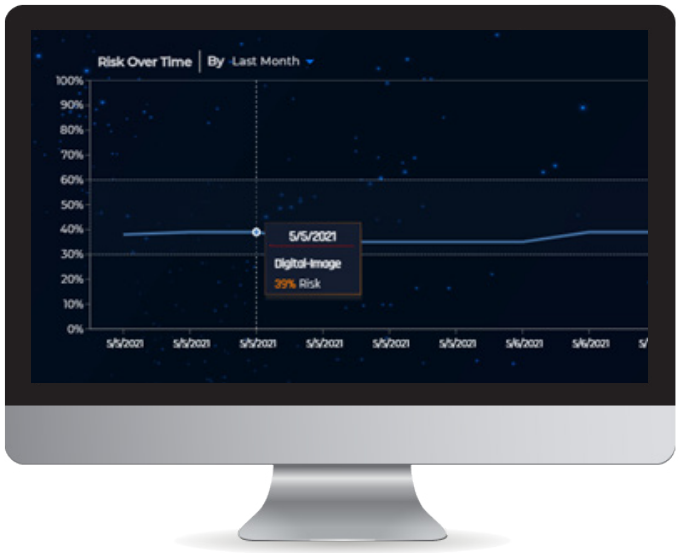
Companies use security event systems to manage the alerts received from multiple security measures. During the risk assessment, data is gathered on each asset and security control in the SuC, and it is recommended to add that data to the security event system. Information such as risk score, breach likelihood and potential impact on the SuC and business processes can help in triaging alerts, helping prioritizing the response to alerts and incidents while taking into account both technical issues and business priorities.

Continuous Assessment

Networks' risk score change over time due to different factors:

- Addition or removal of devices, changes to security controls, changes in zones, etc.
- Discovery or receiving notification about new vulnerabilities and attacks, degradation of countermeasures, breach in security layers, and the inherent security properties of devices and systems pending review, update, or upgrade

These changes require companies to perform risk assessment on their SuCs regularly, thus making sure their mitigation plan is still relevant and their risk stays low in the face of continuous changes in the threat landscape.



CIARA – Industrial Risk Assessment & Management

Serving as a stakeholder decision-support tool, CIARA empowers users to increase the effectiveness of their risk-mitigation measures throughout the entire system lifecycle through attack simulations, TI-based analysis and generation of a clear, actionable roadmap toward optimizing OT-cybersecurity expenditure.

Indicators for overall Risk, Threat and Control levels

Risk Matrix by impact & likelihood, color-coded for severity

Security Control completion for all IEC-62443 Fundemental Requirements + other standards

Changes to risk level over time

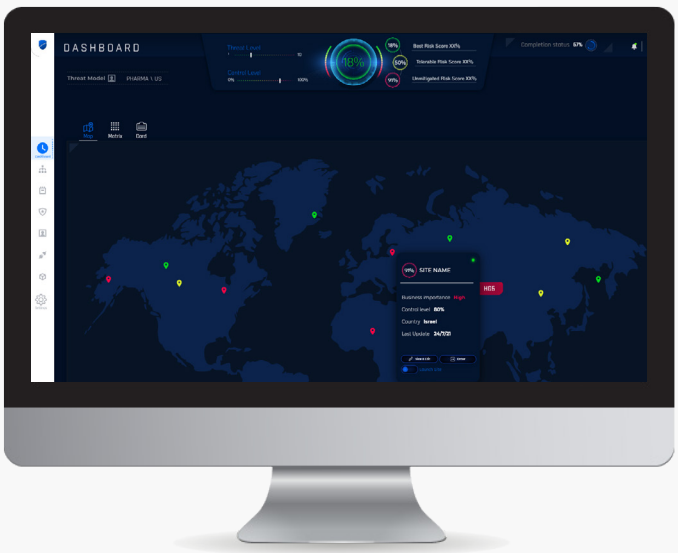
Top Attack Scenarios, including likelihood and impact, per business process

Prevelance of different attack groups & tactics in different regions, for benchmarking and multi-site risk management

Most commonly used techniques by prevelance and breach activity type

Descriptors for attack groups, by relevance, capabilities and affiliation

Multi-site risk management with high-level KRI's and direct access to each location's risk dashboard



Radiflow's SEE-KNOW-ACT-MONITOR Framework

Covering all aspects of industrial cybersecurity, Radiflow's SEE-KNOW-ACT-MONITOR framework provides solutions and workflows designed to provide network visibility, protection and management tools, while ensuring maximum cyber-security ROI.

First, Radiflow's **SEE** solution provides full visibility of the OT network, including all devices, connections, and assets, without interfering with critical operations. SEE enables gaining in-depth visibility into devices' properties to obtain important data regarding network vulnerabilities and aberrations from normal baseline behavior, using a self-learned digital image of the network.

Radiflow's **KNOW** solution automatically calculates the impact of hundreds of the most commonly-used security controls against a simulation of hundreds of cyber threats, while modeling against dozens of features in the digital network model including protocols, vulnerabilities, firmware versions, topology, device types and more.

These risk assessments are then factored against common OT risk scenarios including loss of availability, loss of control and damage to property (among others). The result is a matrix of tens of thousands of potential permutations that simply cannot be analyzed by humans, and enables the evaluation of the SuC risk and generation of comprehensive, actionable reports in a matter of minutes.

Radiflow's solutions are valuable for both the management and the operational side of industrial cyber-security. On the management level, **ACT** presents the user with information relevant for long-term mitigation planning. For operations, ACT can add valuable data and insight, enabling taking into account risk and impact when handling cyber incidents.

Finally, **MONITOR** provides tools for ongoing monitoring of highly configurable alerts on network changes and abnormal behavior. MONITOR solutions were designed for corporate or MSSP SOCs, with a convenient multi-system dashboard for direct access to any iSID IDS belonging to a single or multiple entities.