Radiflow

Breach & Attack Simulations (BAS) in OT environments

CIARA, THE FIRST OT-BAS PLATFORM

RANI KEHAT, CISO,
RADIFLOW

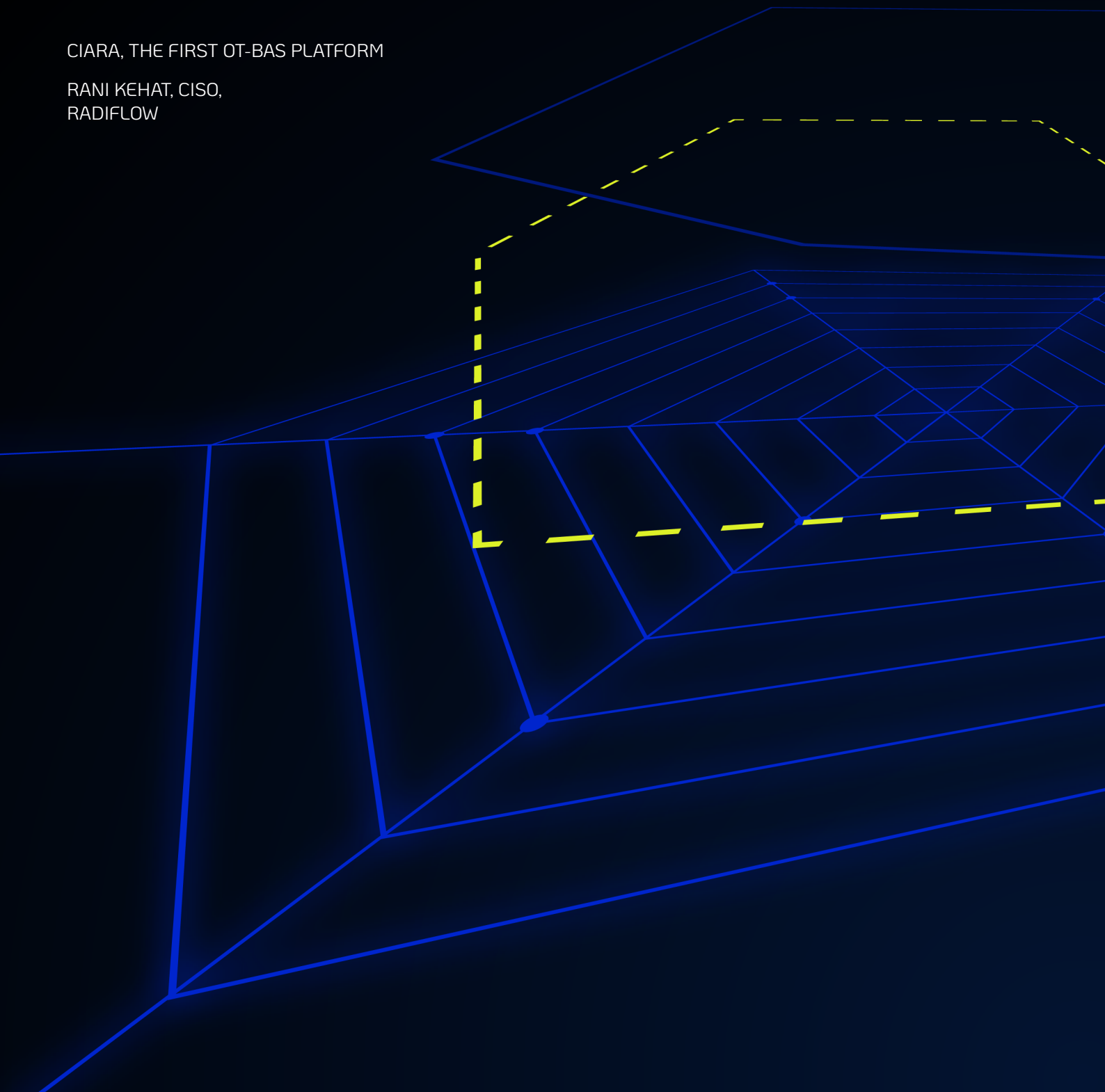

Table of Contents

Executive summary

The situation

The importance of Cybersecurity in the Operational Technology (OT) World

Attacks on operational technology (OT) have increased as connectivity to external networks has grown, requiring many industrial organizations to upgrade their security tools for their systems and networks.

While OT cyberattacks occur less often than IT attacks, they are more devastating and difficult to resolve.

The challenge

For OT security teams, the inability to test attack scenarios on a live site presents significant challenges. How do you identify and remidiate a large number of vulnerabilities without testing attack scenarios directly within the network environment? Historically, “trial and error” was the only method of determining security priorities — a recipe for long cycles that may lead to financial loss. The following questions lingered without concrete answers:

1. Given this limitation, how do CISOs prioritize security vulnerabilities so they can invest their resources most effectively?
2. How do CISOs know which maintenance activities to prioritize during the next security system maintenance scan?
3. And finally, how can industrial organizations achieve the most ROI for their security activities?

The solution

The non-disruptive breach simulation uses a digital network image. Raidlfow CIARA OT-BAS is the first-of-its-kind automated breach assessment tool to meet the challenges addressed above.

"CIARA enables OT security teams to perform safe, non-disruptive OT-BAS (Breach & Attack Simulations) using a digital (twin) image of the OT network. The digital image, created by Radiflow's iSID IDS using mirrored ICS data-streams from across the OT network (or optionally from select CMDB tool), represents the network topology including the vulnerabilities in assets and protocols.

CIARA's OT-BAS provides the ability to prioritize the most effective mitigation controls, based on each network's unique threat landscape and existing security controls, as well as the network owner's risk mitigation preferences and budget constraints.

A breach and attack simulation platform performs many of the same critical functions as red and blue teams, but in a continuous and automated fashion, requiring less manual effort.

Breach assessment tools: general description and use

Introduction

> **A breach of security = when something that is normally protected is no longer secure.**
>
> **(Oxford dictionary)**

The cyber-threat landscape is constantly changing with countless new vulnerabilities and attack tools exposed daily. To prepare for a completely different attack method or tactic, the cybersecurity management system (CSMS) must be adaptive and dynamic.

Deploying what-if scenarios enable security teams to prepare for attacks without past precedence. Historically, however, using what-If scenarios within the OT network was difficult to deploy due to the potential destructive nature of simulating the behavior of threats in the live network.

By using a digital image of the OT network, rather than simulating breach attempts in the live network, CIARA'S OT-BAS solves this challenge.

Security professionals can now mitigate future attacks and stay ahead of current APTs by simulating what-if scenarios in the virtual digital image, which accurately depicts the network including topology, zones (in compliance with IEC 62443), protocols used, connections, asset properties and vulnerabilities.

Once a digital image is obtained, a full breach & attack simulation (BAS) derived through analysis of hundreds of APTs can be conducted. Given this simulation, security teams can assess potential attack vectors and the network control (defense/mitigation) level needed to fend off these attacks.

With a digital image of the production environment, security teams can also test updates without risk.

Current breach assessment tools

Many of the current BAS offerings are multi-function tools. Below is a list of tools categorized by their capabilities.

a. **Auto Pen – Test**
   Auto Pen tests automate the process of "how can we get in". The advantage of this method is consistency with predetermined attack workflows. However, pen testing lacks the ability to go beyond predetermined testing parameters to assess large numbers of eventualities and edge cases.

b. **IT BAS**
   IT-BAS is used for automated testing of installed security controllers. Simulators play a sequence of actions to check the full adversary tactics and techniques (ATT) kill chain and to detect security controller misconfigurations or failures.

c. **Vulnerability Scanners**
   VA scanners, which are less intrusive than IT-BAS solutions, initially focused on scanning the network for known vulnerabilities and security controller misconfigurations. Current BAS and VA offerings are beginning to overlap.

d. **Red-Team**
   Red-teaming is a human-driven process, so it's not preconfigured to simulate pre-defined attack flows and attack tools. In addition, it allows quick adoption of new attack vectors upon encountering security controls and the creation of new tools.

OT-BAS: the newest breach assessment tool for OT Networks

OT-BAS follows these steps to perform a risk analysis:

CIARA overcomes the problem of OT environments' sensitivity to intrusive actions (even simple scans) by using digital image of the production network.

1. Vulnerabilities in the assets and in the protocols in the ICS digital image are mapped out and added to the CIARA algorithm.
2. CIARA's Machine learning (ML)-based simulation algorithm on the digital image simulates the attack success rates of relevant adversaries' APTs (based on geo-location and industrial sector).
3. At the same time, CIARA simulates "sister" networks' digital images (similar to the digital image of the analyzed network) to create control groups for benchmark scoring.
4. Different mitigation controllers are then added to the ML simulation to prioritize the optimal security controllers for risk reduction.

Comparing Functionality between Breach Simulation Tools

Category	OT BAS	IT BAS	VA Scanners	Auto P. T	Red-Team
Network Impact (attack tests, etc.)	NONE (Virtual Digital Image)	YES (In-network, "controlled" attack tools)	PARTIAL (In-network, Scanner)	YES (In-network, "controlled" attack tools)	YES (In-network, "controlled" attack tools)
Relevant Threat landscape	Yes	Yes	Partial	No	Yes
"What-if" simulation	Yes	Partial	No	No	No
Risk scoring (impact & likelihood)	Yes	Yes	Partial	No	Yes
Prioritization of security controls	Yes	No	No	No	No
Compliance management	Yes	Yes	Partial	No	Partial
Secure design review for new projects	Yes	No	No	No	No
Auto Update of Attacks	Yes	Yes	Yes	No	No

The use of BAS in OT environments

CIARA's OT-BAS platform enables organizations to frame their cyber risk management process in a number of ways:

Optimize planning of security controls

OT-BAS automates the process of acquiring data. Data regarding threat sources is obtained from threat intelligence sources like MITRE or ICS CERT, where each APT group is modeled in the simulation for full kill-chain.

Threat events are derived by simulating the APTs' activity within the digital image, providing the probabilities of the APTs' success rate in a loss scenario.

Following the IEC62443 methodology, you can **logically partition the production system using customer key criteria** such as:

- Impact
- Tolerable risk
- Health/safety/environmental regulations compliance
- And more

With OT-BAS, you can now **optimize** your cybersecurity controls and risk mitigation processes according **to customer key criteria** per zone and for the overall system being evaluated.

By simulating different APTs, you can obtain the threat likelihood of specific threat events directly related to the customer's key criteria.

This means, you can now answer questions such as:

- Has the SolarWinds attack affected my residual risk in high-impact zones?
- If we invest in implementing the security controls specified in NIST 800-161 for supply chain risk management, how much would it reduce the risk of this attack vector?
- If we want to reduce our residual risk to a tolerable level, do we have to invest in all NIST 800-161 security control domains, or can we stop investing once we reach the point of risk tolerance?

With the above processes in place, you can more easily plan a security road map for technology and a cyber policy for processes and procedures based on risk reduction.

With OT-BAS, you can also determine the best ROI for each cybersecurity control mitigating a threat event.

Simulation of newly-discovered threats

BAS solutions use known APTs (a known chain of ATTs) to assess systems' control levels.

By using the digital image in OT-BAS, you can run new ATTs (zero-days) discovered by threat hunting platforms to instantly reveal the potential risk to an ICS system.

By modeling the new ATT's behavior, you can assess the vulnerability targeted (if at all), the effectiveness of the security controls in the target system, the adversary's desired loss scenario, and more.

OT-BAS simulators will use the above input to assess the relevance of the new ATT to your network ,i.e. the impact on the target asset and cyber risk score.

Qualitative and quantitative risk analysis

OT-BAS enables you to establish a data-driven methodology for quantifying the probability of cyber threats in your OT system.

Simulating adversary techniques and tactics (ATTs) on the digital image gives you the ability to assess unmitigated and mitigated risk, assuming that verification of configuration and correct implementation are regularly performed.

When you implement OT-BAS to quantify threat likelihood, you can also add quantitative impact data (magnitude of loss) and establish a fully quantitative OT risk matrix.

Compliance with OT security assurance levels ISA99 / IEC62443

Once you define the security levels qualitatively, you can compare and manage the security of zones within your organization.

"As more data becomes available and the mathematical representations of risk, threats, and security incidents are further developed, the selection and verification of security levels (SL) will exist on a more quantitative level.

A quantitative analysis benefits end-user companies as well as IACS and security products vendors. They can better select IACS devices and countermeasures for zones as well as identify and compare zone security levels and measures in different organizations across industry segments." (James D. Gilsinn & Ragnar Schierholz / Security Assurance Levels: A Vector Approach to Describing Security Requirements ISA99)

Security assurance levels (SAL)

Setting different security assurance levels per zone requires data. By benchmarking your digital image to other networks that have different vulnerabilities, topologies, threat landscape and security controllers in place, you can generate data regarding SAL targets, design, and capabilities.

To quantify threat likelihood in OT systems, BAS scenario simulations produce datasets that can be used to set security assurance levels (SAL).

Create benchmark scores

1. Divide the system under consideration (SuC) into zones
2. Input impact values to assets and zones
3. Simulate hundreds of APTs on the digital image and in hundreds of simulated "sister" networks

The above creates a vector between impact, vulnerabilities, adversaries (APTs), and risk mitigators (be it security controllers or process & procedures).

Once the BAS creates a virtual benchmark and produces unmitigated risk scores, you can set your tolerable risk levels for the different zones.

By comparing the simulated risk level of a zone to your tolerable risk level, you can now simulate mitigation controllers to reduce the risk to the desired tolerable level.

Using the above data-driven approach, you can better assess your investment in security controls and processes, and avoid over-investing in cyber mitigation beyond your needs.

Industry benchmarking

A maturity model is a set of characteristics, attributes, indicators or patterns that represent capability and progression in a particular discipline.

A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability regarding its practices, processes and methods. A maturity model also sets goals and priorities for improvement.

But for OT security professionals, it's difficult to create this benchmark and to take the necessary steps for risk framing because of the lack of shared cyber data on OT maturity levels and cyber breaches.

To overcome this obstacle, CIARA simulates "sister" networks, changing attributes such as topology, threat landscape and vulnerabilities to benchmark your specific system.

Organizations can benchmark their performance by examining the capabilities of their member organizations.

Summary - Benefits of OT-BAS

- Gain real-time data: Monitor risk continuously and consistently and receive reports to make data-based decisions
- Improve ROI: Invest in mitigation controllers for high impact/high threat likelihood zones, rather than over-invest in security controls and processes beyond tolerable risk levels in other zones
- Evaluate new attacks: Determine quickly your exposure to newly reported threat scenarios
- Score and measure: Quickly determine your cyber control and maturity level of chain of supplies and potential M&A
- Meet industry regulations: Comply with industry standards and regulations