



SCADAfence



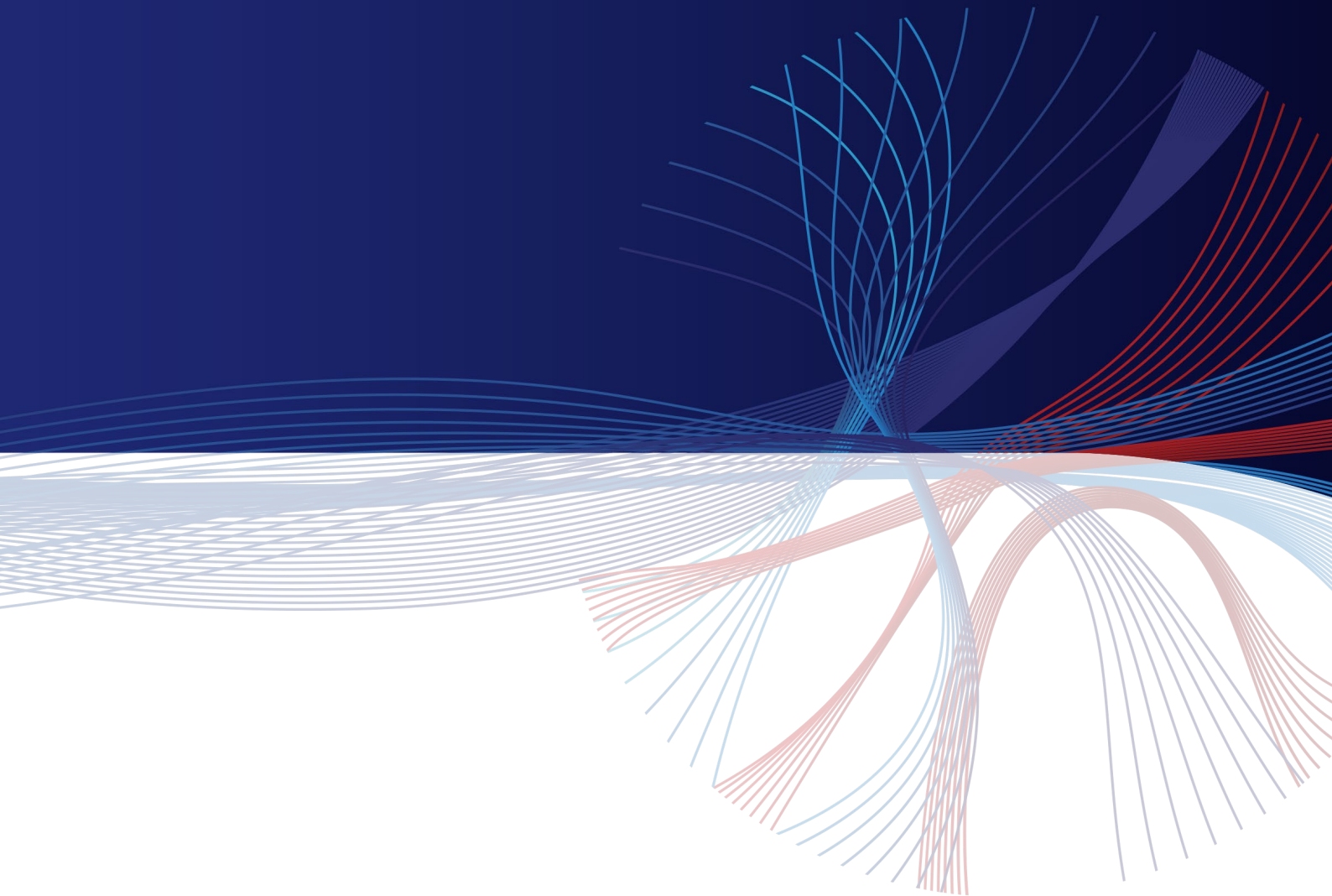
Version 2

www.version-2.com

二版

Technical Whitepaper

OT Remote Access Security



Securing Remote Access for OT Networks

SCADAfence and Barracuda Networks have joined forces to take the remote access security connections into OT Infrastructure one step further. Organizations can now gain visibility into remote access sessions inside their OT networks, accessing PLCs and controlling ICS processes. This enables them to get the full picture on all remote user activities.

Due to the COVID-19 situation, most of the global workforce has transitioned to working remotely. However, process availability and safety remain a major concern, while the attack surface is growing dramatically due to remote connections. Organizations that rely on industrial infrastructure have sent a large portion of their employees to work from home, while enabling them to continue their operations at the cost of operating under substantially higher cyber risk.

The Benefits for Your Organization:

- Enable safe remote access to critical OT environments.
- Increased visibility into remote users' activities in the OT network.
- Correlate between OT device level actions and remote connections.
- Detect unauthorized actions.
- Get detailed activity reports.

THE ONBOARDING PROCESS



Diagram #1: The onboarding process for a remote access security solution takes less than 2 days

The Challenge of Working Remotely

Working remotely means opening networks up to exponentially more external access – networks which were previously never opened to such access, or had very limited remote access to them.

In an instant, the exposure of OT networks has increased dramatically:

- **Increased Exposure** – The number of external connections, in addition to the fact that workstations used in remote access are also connected to the internet and can be compromised. This can give attackers access to critical assets - such as [this cyber-attack that we discovered on a remote server](#).
- **Hard Perimeter, Soft Belly Approach** – Once remote users log in, they can often access a wide range of critical hosts, without further access control.
- **Lack of Correlation Between Remote Users & Process Manipulation** – After initial authentication at the gateway, there is no way to associate OT sessions with the logged-in users. This lack of association and attribution creates substantial risk that is a challenge to manage.
- **Increased Complexity** - People accessing from home means more remote locations and end-devices. This adds complexity and thus further increases exposure.

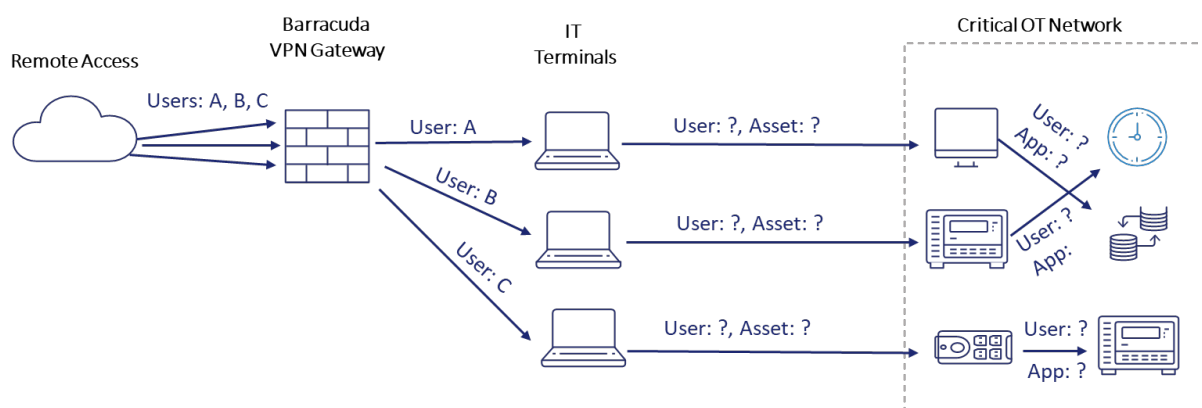


Diagram #2: Internal sessions are not attributed to remote access sessions and no logging is kept

How SCADAfence and Barracuda Networks Can Help

The SCADAfence Platform integrates with the Barracuda VPN gateway to increase the security of OT networks in the era of intensive remote access connectivity / mode of operations.

Full Attribution & Correlation Between Remote Users & Internal Actions

- The SCADAfence Platform interfaces with Barracuda's VPN gateway to classify and identify remote access connections. This adds an additional layer of security that correlates between the end-users and their activities in the network. The SCADAfence Platform also provides the security staff with correlation between their users and their activities while performing remote work.
- In addition, the SCADAfence Platform creates a forensics log containing internal actions, users and timestamps, all attributed to the remote session. This allows for an investigation in retrospect.

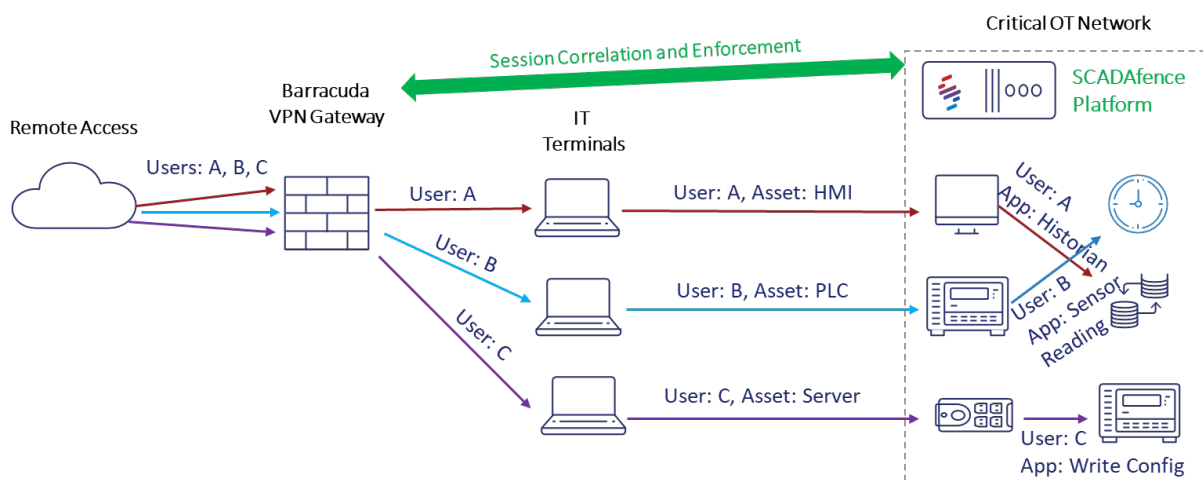


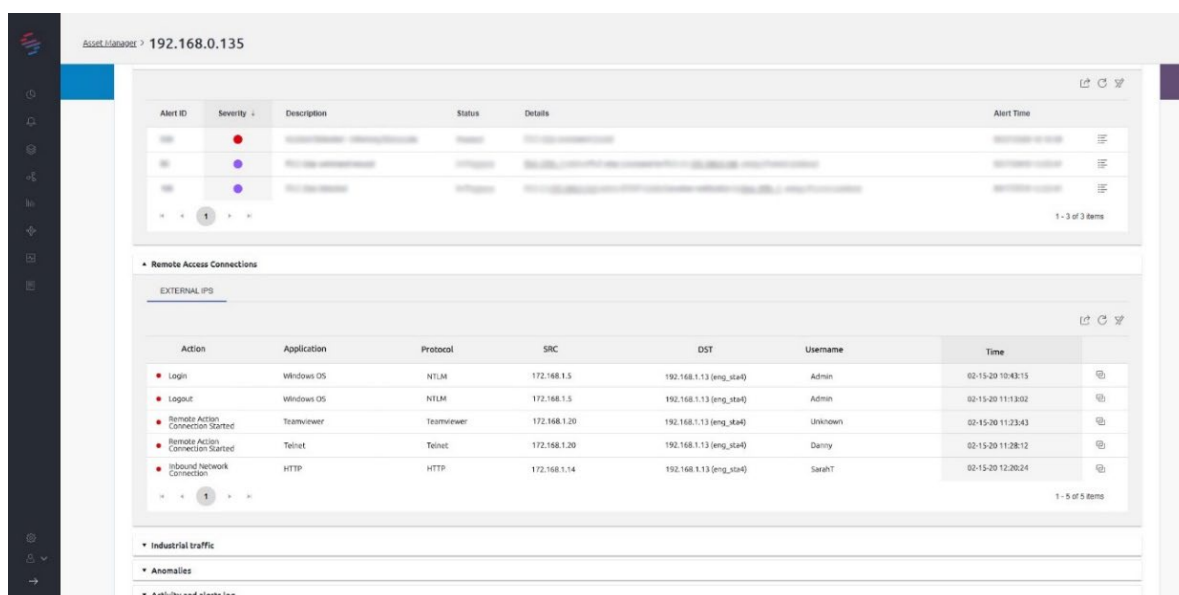
Diagram #3: The integrated solution understands remote user activities inside the OT network

Identifying the Accessed Asset

The SCADAfence Platform automatically creates a detailed asset inventory, including OT asset profiling – providing insights on the target devices that are accessed by the remote users.

Understanding the Activities Performed

The SCADAfence Platform's DPI engine, enables security teams to understand the activities performed on the industrial devices. The analysis provides insight on logins and logouts as well as on the industrial protocol activities, down to the industrial protocol command.



The screenshot displays the SCADAfence Platform interface for the asset 192.168.0.135. It features a sidebar with navigation icons and a main content area with several sections:

- Alerts:** A table showing three alerts with columns for Alert ID, Severity, Description, Status, Details, and Alert Time.
- Remote Access Connections:** A section with a sub-table for EXTERNAL IPS.
- Activity Logs:** Sections for Industrial traffic, Anomalies, and Activity and alerts log.

The EXTERNAL IPS table contains the following data:

Action	Application	Protocol	SRC	DST	Username	Time
Login	Windows OS	NTLM	172.168.1.5	192.168.1.13 (eng_ata4)	Admin	02-15-20 10:43:15
Logout	Windows OS	NTLM	172.168.1.5	192.168.1.13 (eng_ata4)	Admin	02-15-20 11:13:02
Remote Access Connection Started	Teamviewer	Teamviewer	172.168.1.20	192.168.1.13 (eng_ata4)	Unknown	02-15-20 11:23:43
Remote Access Connection Started	Telnet	Telnet	172.168.1.20	192.168.1.13 (eng_ata4)	Danny	02-15-20 11:28:12
Inbound Network Connection	HTTP	HTTP	172.168.1.14	192.168.1.13 (eng_ata4)	SarahT	02-15-20 12:30:24

Diagram #4: The SCADAfence Platform provides insights on all remote access activities

Detection and Response

- The SCADAfence Platform detects and alerts on anomalous or unauthorized actions in the OT network and provides security teams with the association to the user names, originating workstations and applications.
- The Barracuda VPN gateway is informed on the breach, and it can immediately disconnect the malicious user/s from the network.

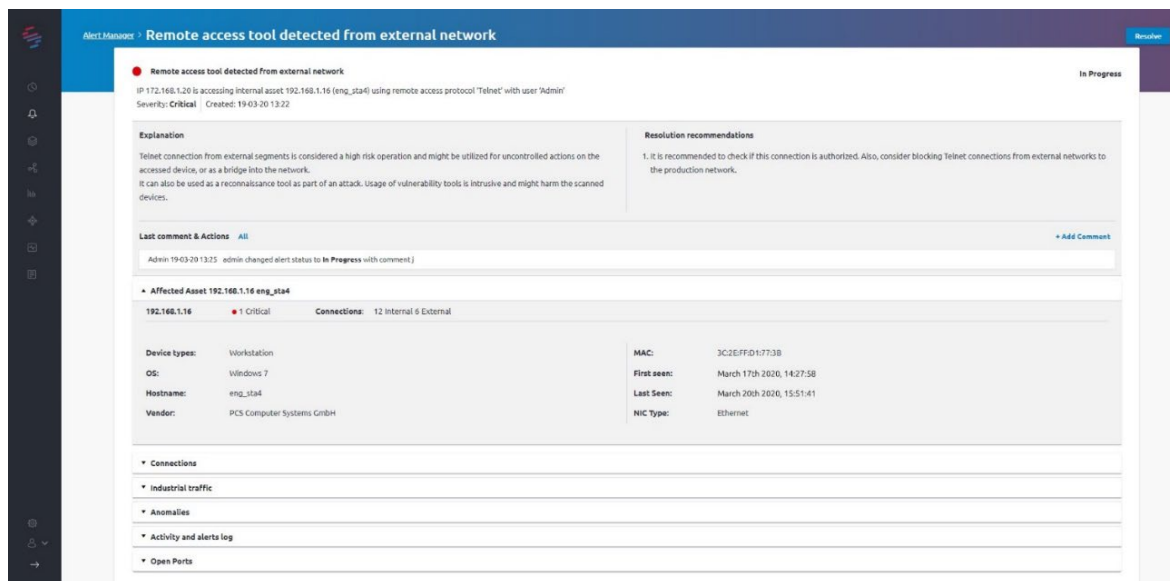


Diagram #5: The SCADAfence Platform detects & alerts on anomalous or unauthorized actions in the OT network

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives. SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in manufacturing, building management and critical infrastructure industries to operate securely, reliably and efficiently. To learn more, go to www.scadafence.com