CLAROTY

Use Case

INCIDENT RESPONSE FOR REMOTE USER ACTIVITY

with The Claroty Platform

The Claroty Platform is a complete industrial cybersecurity solution powered by our Continuous Threat Detection (CTD) and Secure Remote Access (SRA) solutions. The platform provides a full range of industrial cybersecurity controls that integrate seamlessly with existing infrastructure, scale effortlessly, and support the unique needs and priorities of both operational technology (OT) and information technology (IT) personnel alike.

Further extending the value of these controls is the fact that The Claroty Platform is also the industry's only such solution to offer fully integrated remote incident management capabilities that cover the entire incident lifecycle. The following use case demonstrates one example of how IT security operations center (SOC) and OT personnel can use the platform to more effectively detect, investigate, and respond to OT incidents across the broadest possible attack surface from any location.

Use Case Background

The respective roles and responsibilities of the IT SOC personnel and OT personnel in this example include:

IT SOC Personnel

- OT cybersecurity risk management
- Monitor & respond to OT remote access incidents
- Uses CTD to detect anomalous activity on OT network

OT Personnel

- OT availability, reliability, & safety
- Uses SRA to remotely access & service OT assets
- Relies on IT SOC to detect anomalies on OT networks

Part 1

An OT engineer submits a management of change (MoC) ticket requesting authorization to connect to an engineering workstation to conduct maintenance on a programmable logic controller (PLC) via SRA. The OT manager then receives the engineer's MoC ticket and authorizes the request directly within the SRA Secure Access Center (SAC).

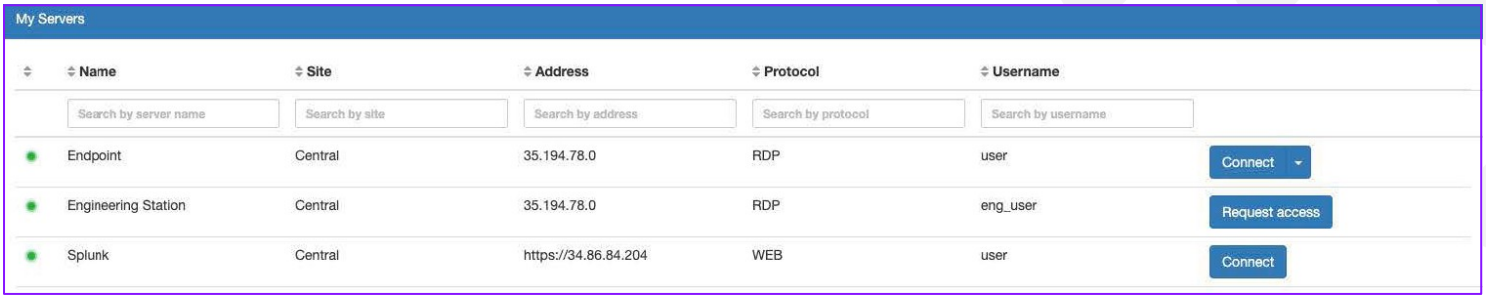

Image 1: This image shows SRA from the perspective of an OT engineer who requests access to an engineering workstation in order to conduct maintenance on a PLC. SRA enables the implementation of granular authentication and access controls for all users based on the security principles of zero trust and least privilege.

Part 2

While using SRA to access the engineering workstation in order to conduct maintenance on a PLC, the OT engineer mistakenly downloads a new configuration to the PLC. Since this operation was not included in the MoC ticket and was not authorized, it immediately triggers a configuration download alert in CTD.

As with all Claroty alerts, this alert contains contextual information including root-cause analysis, the associated indicators, assets, and SRA session, as well as an alert score that reflects the level of risk posed to the OT environment in which the alert was triggered. This information helps reduce false positives and expedite triage and investigation processes.

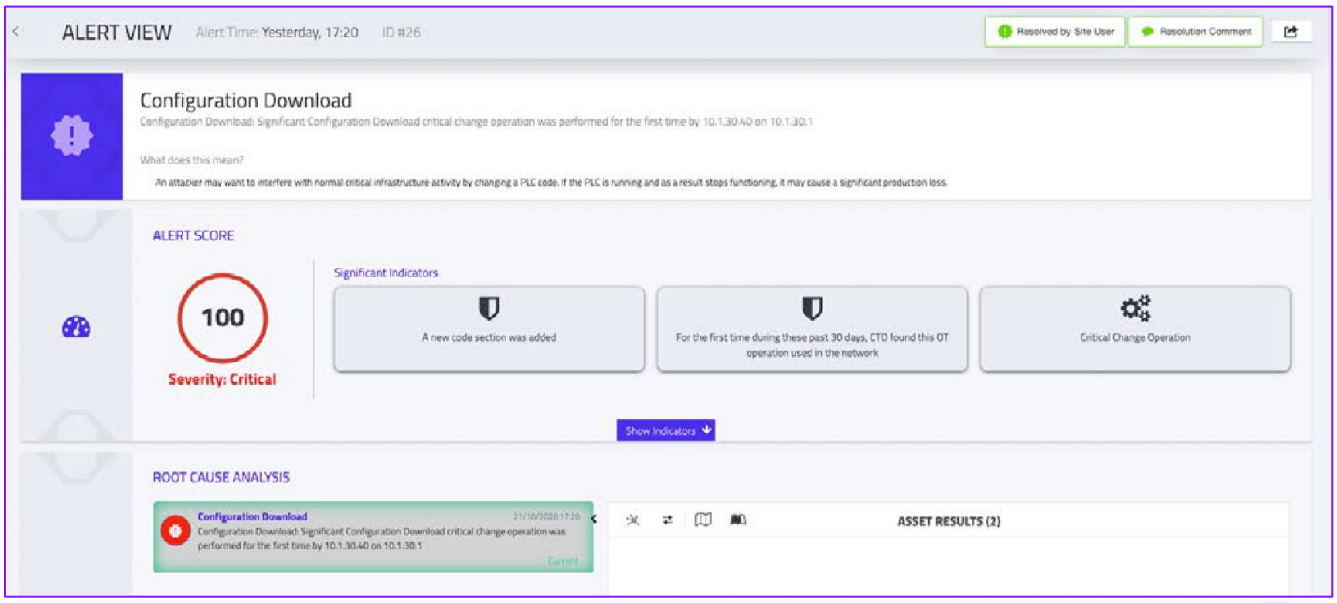

Image 2: This image depicts the root-cause analysis, indicators, associated assets, and risk score of the alert caused by the OT engineer's mistake. This alert is visible in CTD where it is quickly reviewed by an IT SOC analyst.

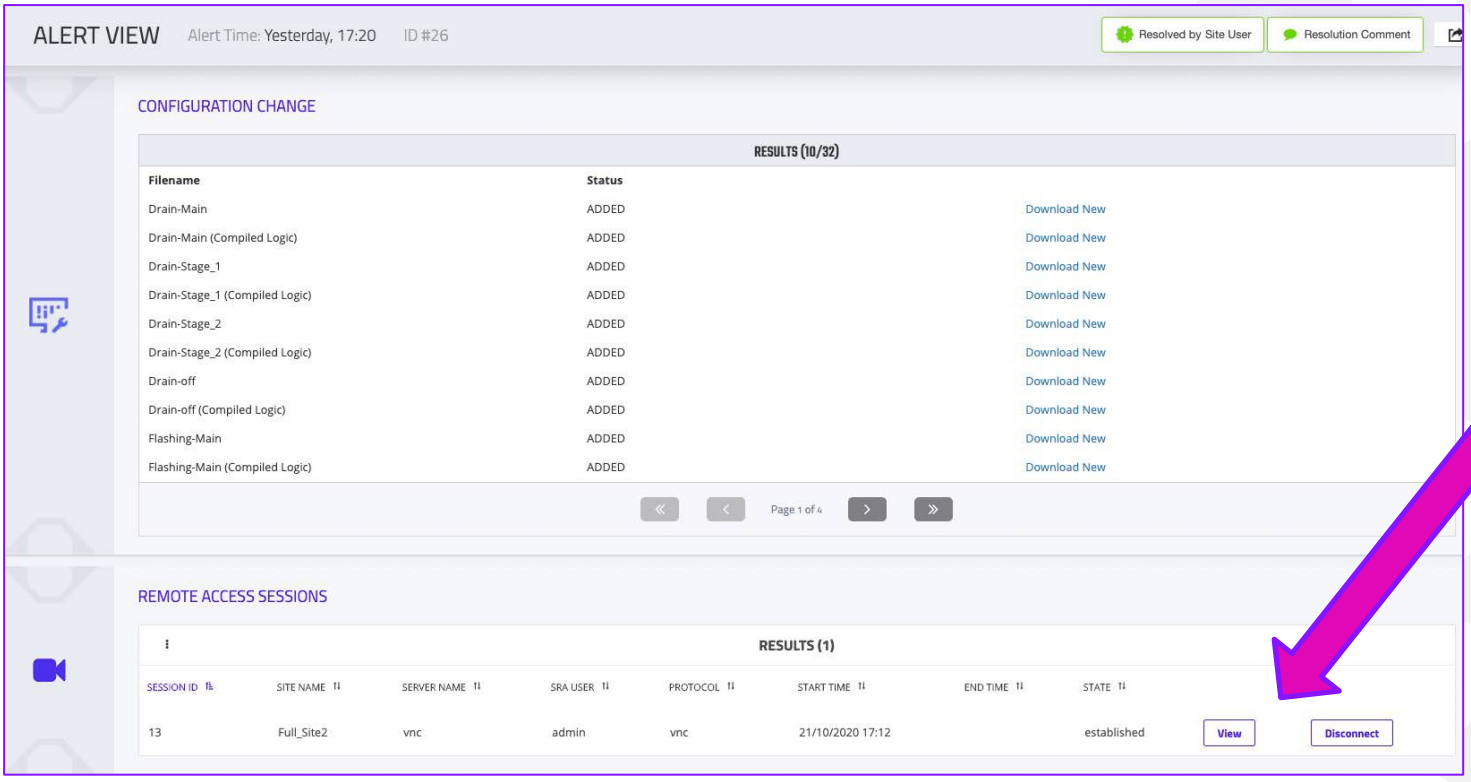

Image 3: All alerts related to an SRA session link to that session. All sessions can be monitored over-the-shoulder in real-time and are recorded in full for future audits and investigations. SRA administrators can also disconnect live SRA sessions when necessary.

Part 3

An IT SOC analyst quickly sees the alert within CTD. The alert includes the original MoC ticket, the specific SRA session and user, and the unauthorized operation that triggered it. Upon reviewing this information, the IT SOC analyst chooses to escalate the alert to the IT SOC manager who then opts to monitor the OT engineer's live SRA session directly from CTD and immediately decides to disconnect the session and view the recording to investigate the event that triggered the alert.

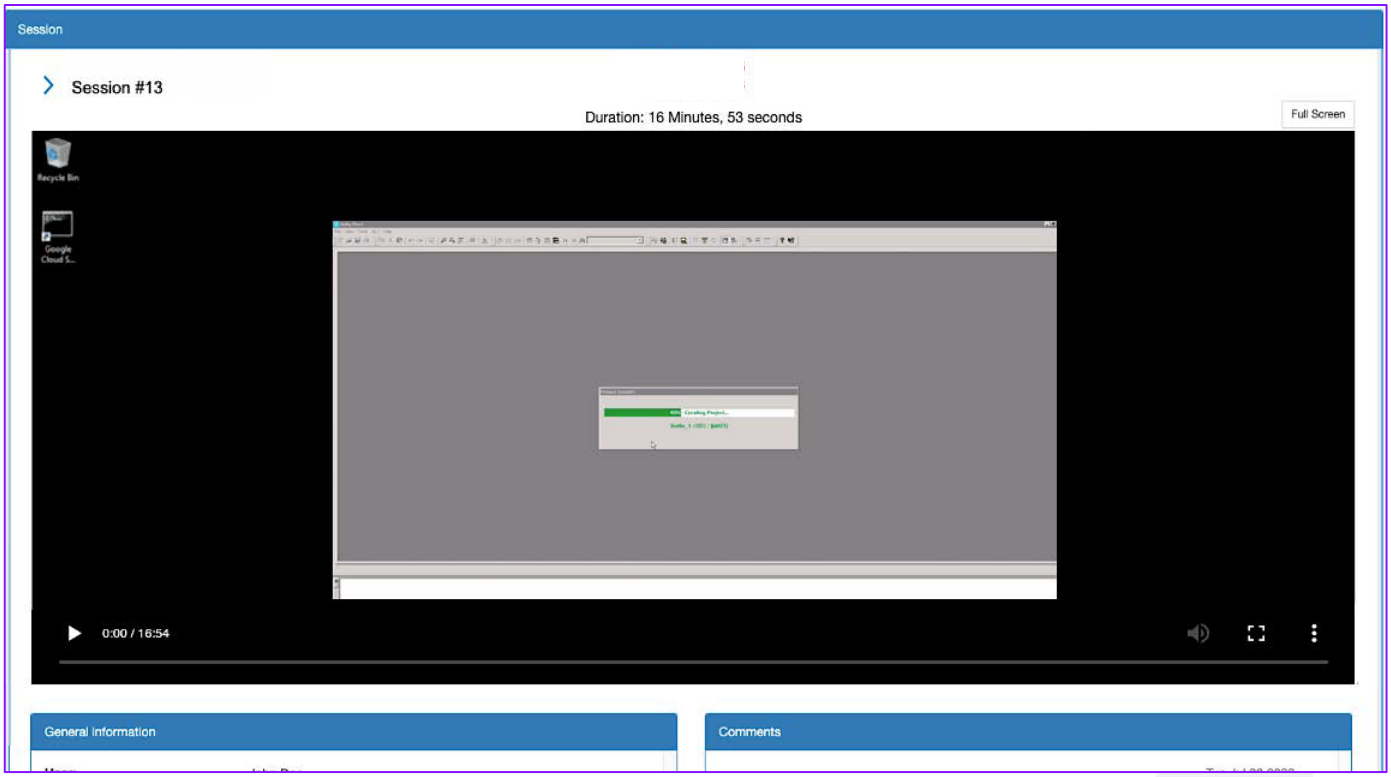

Image 4: This image shows the IT SOC Manager's over-the-shoulder monitoring view of the OT engineer's live SRA session.

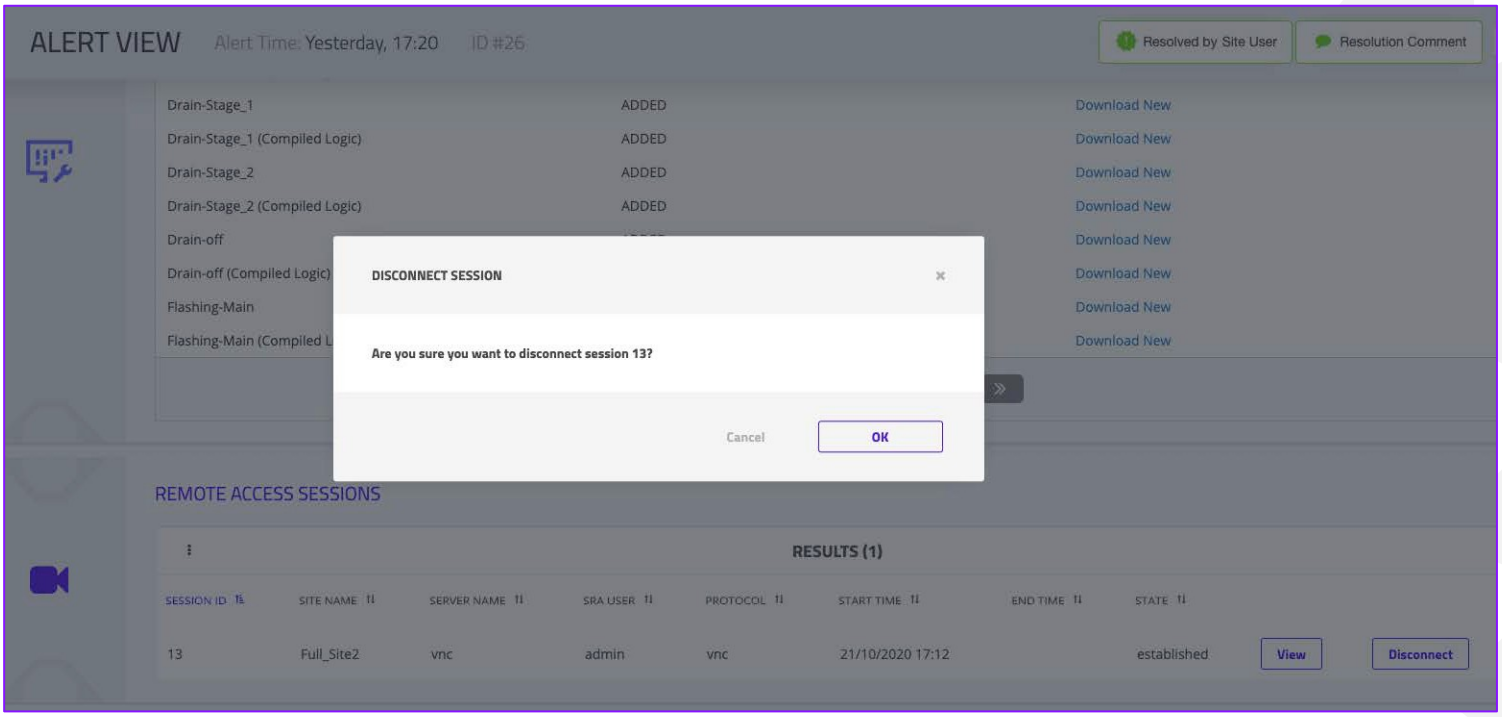

Image 5: This image depicts the "Disconnect Session" option from the perspective of the IT SOC manager who chose to disconnect the OT engineer's in-progress SRA session after viewing it directly from the related alert in CTD.

Recognizing the abrupt termination of their SRA session, the OT engineer tries to reconnect to the engineering workstation but is unsuccessful. The initial authorization granted for their session is no longer valid, so in order to reconnect to the workstation, the OT engineer must request authorization for a new session.

Part 4

After determining that the OT engineer's download of a new configuration to a PLC during an SRA session was an unintentional error, the IT SOC manager notifies the OT manager, who then chooses to authorize the OT engineer's request to restart their original session – but only after further restricting their access controls accordingly.

The OT manager also opts to monitor this session in real-time to ensure it remains error- and risk-free.

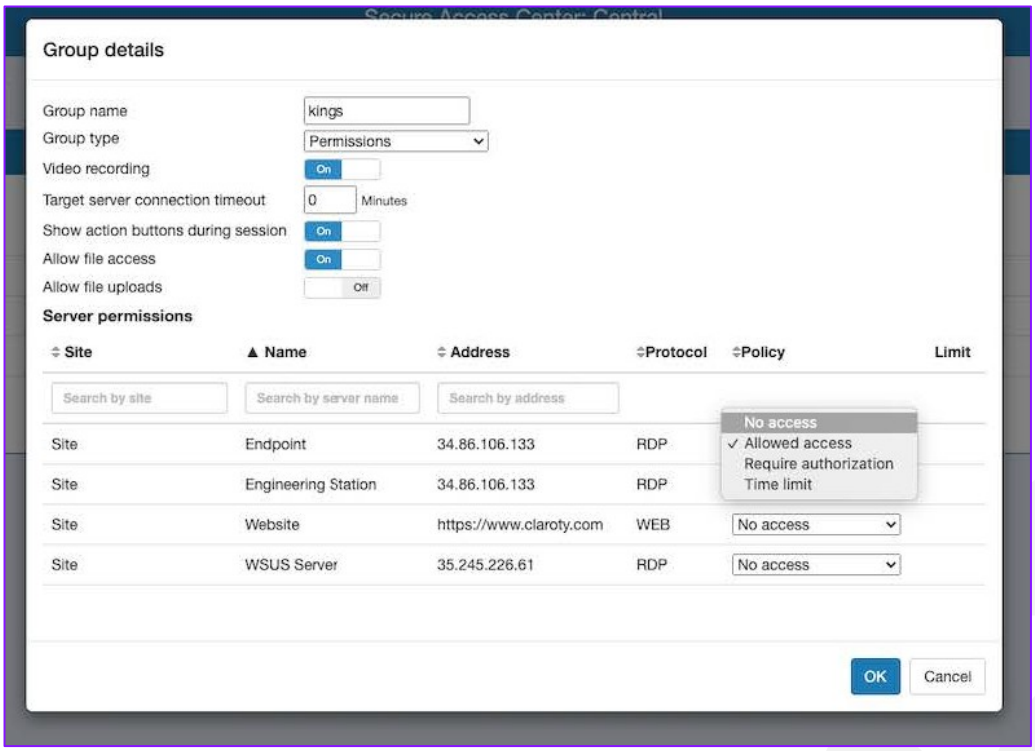

Image 6: SRA's granular and highly customizable access controls can be easily adjusted as necessary by administrators based on the principles of Zero Trust and Least Privilege. This image depicts the OT manager's perspective from the SAC.

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team.

The company is headquartered in New York City and has a presence in Europe, Asia- Pacific, and Latin America, and deployments on all seven continents.

CLAROTY

CONTACT US

contact@claroty.com