SOLUTION BRIEF

Remediant

INTELLIGENT SESSION CAPTURE (ISC): SENTINELONE

THE CHALLENGE

Traditional PAM vendor (CyberArk, ThycoticCentrify and BeyondTrust) session monitoring and recordings are:

- Produced as large media files, that are difficult to search and not amenable to data analysis
- Burden on auditors, compliance officers and security admins to review and analyze video screen recordings for suspicious activity
- Does not provide comprehensive visibility into all threat activity (privileged and non-privileged users) on endpoints: for example, a background download is not recorded.
- Available at an additional cost of infrastructure (storage)
- Complex to deploy, use and manage with security blind spots

THE SOLUTION

Remediant's Intelligent Session Capture (ISC) leverages your existing investment in a EDR solution to:

1. Provide context to what time a privileged session started and ended. This correlated with EDR continuous detection helps better identify, confirm and respond to a nefarious incident in near-real time

2. Give you better, more actionable session monitoring and automatic intervention of endpoint threat activity

3. Track everything that happened before, during and after the privileged session to fully understand the attack. This includes network connection, downloaded files, processes and other activities

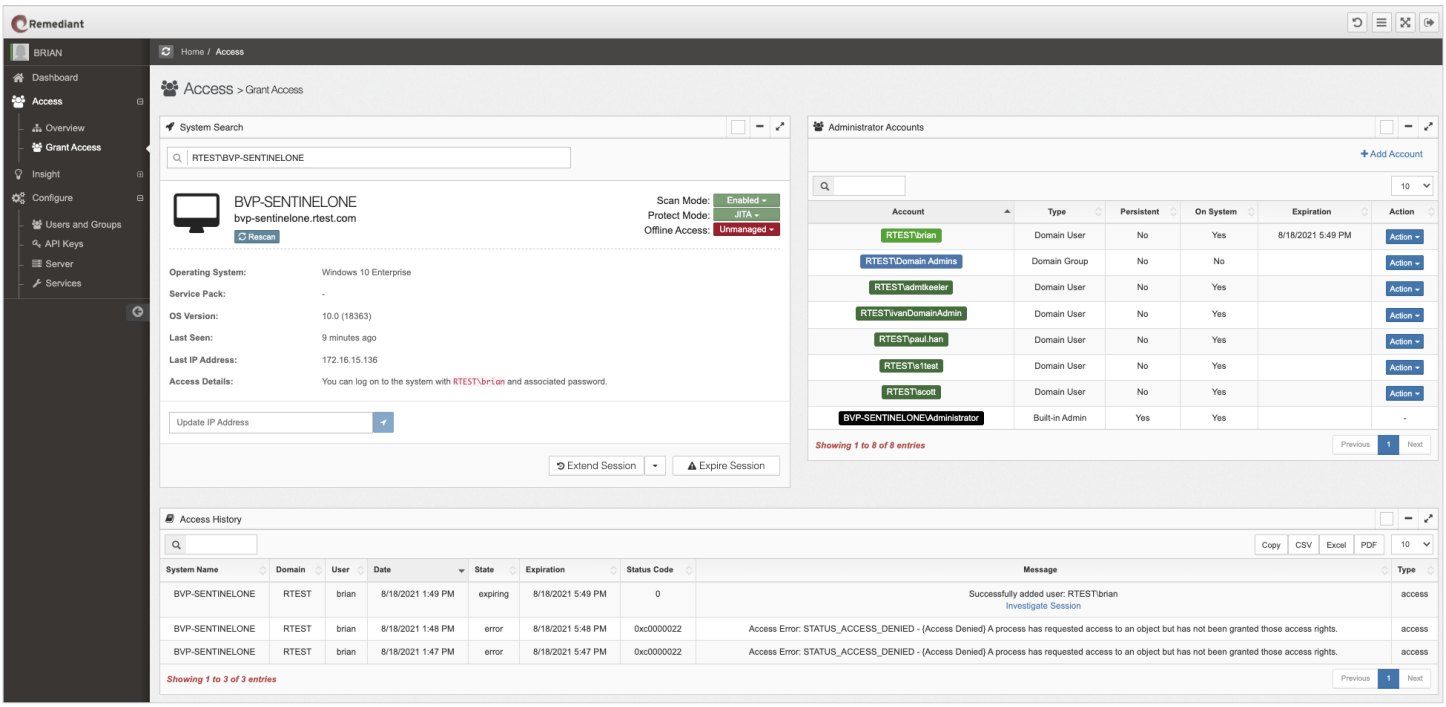

Figure 1. Remediant SecureONE Console

USE CASE

The combined solution helps Incident Response teams quickly determine root cause and stop lateral movement attacks at endpoints:

For example:

- A user signed into a Windows endpoint browses a website and accidentally downloads malware
- The IR team detects this event using an EDR solution
- To investigate, the IR team leverages Remediant's Intelligent Session Capture (ISC) to identify that during a privileged session (JIT) the malware activates on the Windows endpoint to send sensitive information to a C&C site (provides context during the privileged session)
- ISC helps the IR team pivot to the EDR console from Remediant to view all other systems the user has admin rights to during this JIT session and also easily search and find all other systems the malware has moved laterally to infect.
- At this stage, the IR team may either isolate or quarantine the malware infected endpoints using an EDR solution
- The IR team can realize the principle of least privilege by implementing JIT and enabling ZSP on all the malware infected endpoints to eliminate lateral movement

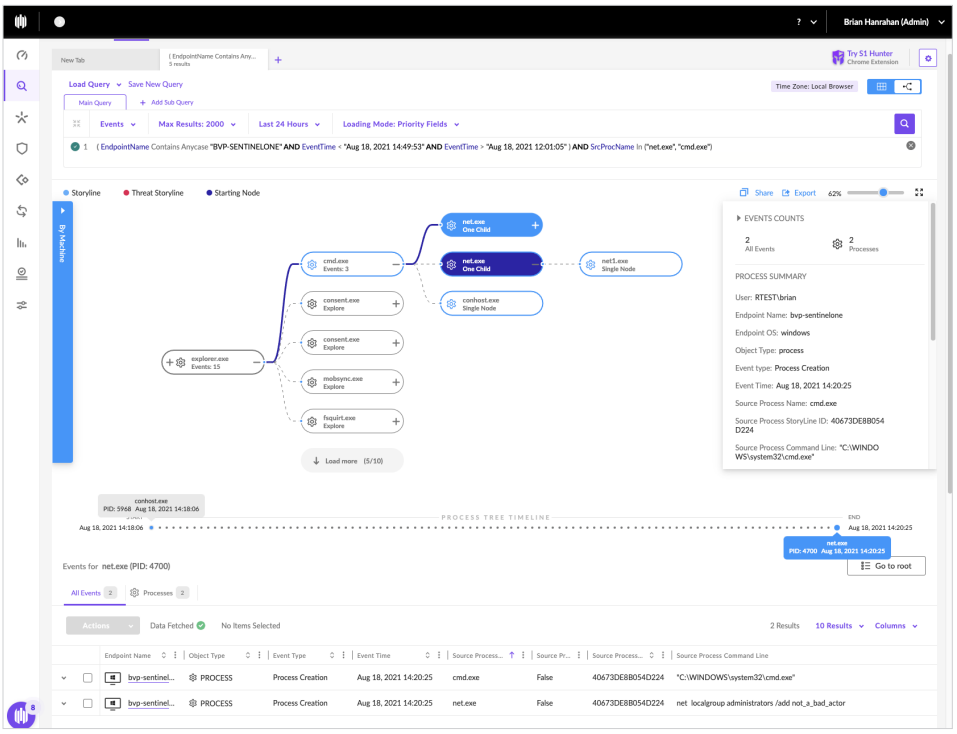

Figure 2. Intelligent Session Capture SentinelOne Investigate Console

BENEFITS OF REMEDIANT ISC + EDR

1. Obtain contextual data into privileged account activity while eliminating the need for additional infrastructure for recording and PAM agents
2. EDR data recordings are easy to access, search and analyze for auditing, forensics and compliance purposes
3. Correlate privileged account activity by accessing the recordings of all end point activity from an EDR solution to expedite incident response and remediation in real time
4. Prevent lateral movement attacks by removing excess standing privilege and replacing with JIT access

Remediant
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111
(415) 854-8771

ABOUT REMEDIANT

San Francisco-based Remediant is bringing Zero Trust to the Privileged Access Management (PAM) market by taking a focused approach to removing the biggest undiscovered security risk: (24x7/always on/persistent) administrator (rights/privileges/access). Built upon the principle of Zero Standing Privilege, Remediant's award-winning SecureONE PAM software delivers Just Enough, Just-in-Time privileged access and continuous discovery with agentless simplicity. SecureONE protects millions of endpoints worldwide and has been adopted by major enterprises across a number of industries. For more information, please visit: *https://www.remediant.com*.

082521