

JOINT
SOLUTION
BRIEF

Recorded Future for Cisco SecureX

As the largest enterprise cybersecurity company in the world, Cisco Secure is on a mission to radically simplify security for our customers. We lead the way in SASE, XDR and zero trust through applied intelligence that anticipates the needs of your business and provides the protection you need everywhere so you can work anywhere. Integrating it all is Cisco SecureX, our security platform that provides simplicity, visibility and efficiency across your security infrastructure. Learn more at www.cisco.com/go/secure.

The Recorded Future Intelligence Platform produces accurate and actionable intelligence at scale, delivered in real time. It combines automated analytics with human expertise to unite an unrivaled variety of open source, dark web, technical sources, and original research. By dynamically categorizing, linking, and analyzing intelligence in real time, the platform delivers easy-to-consume insights for proactive and persistent risk mitigation, via role-based modules that are tailored to your needs.

Challenges Overcome through Integration

This integration with Cisco SecureX enables a user in SecureX to determine the maliciousness of verdicts for an observable, based on combined evidence. The user can then pivot to Recorded Future for broader searching.

This integration provides value for both SecureX and Recorded Future. A platform approach confidently tackles the most pressing security operation challenges. This Recorded Future integration for Cisco SecureX provides:

- **Simplicity:** Integrate technology together with true turnkey interoperability
- **Visibility:** Accelerate time to detect and investigate threats and maintain contextual awareness

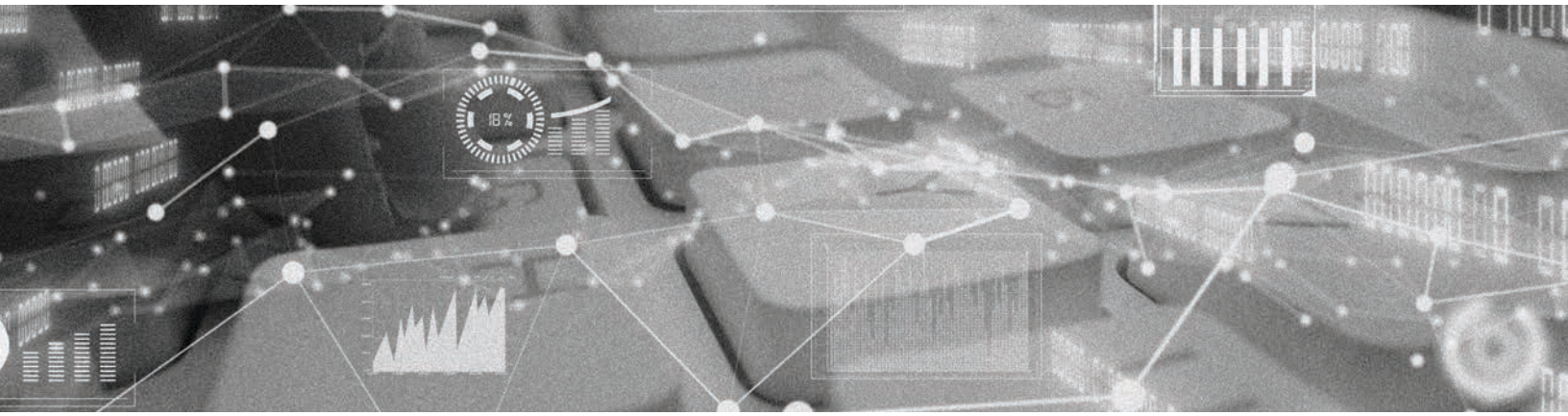


BENEFITS

- Enables analysts to instantly enrich IOCs in the case record
- Tasks to quickly reference the available data and support condition-based subsequent actions
- Provide one-off tasks within the case record to avoid the time lost working multiple windows, systems, or sites

USE CASES

- From SecureX (UI or Ribbon), query Recorded Future for observables (IP, IPV6, Domain, URL, MD5, SHA1, SHA256) and return verdicts to SecureX threat response, based on the Risk Score
- From an Observable, within SecureX threat response (UI or browser ribbon), allow the user to pivot into Recorded Future for additional TI or investigative function.



Cisco Umbrella

Threat Score 100

SHA256 **d2c0135e66b71454d1ab8c5bfbaefa5565a68335e8f833dc7ce603ebf6782048**

SHA1 **b91daa9b78720acb2f008048f5844d8f1649a5c4**

MD5 **decbc720b7cf89646b0c6d2dde595f4e**

Magic Type PE32 executable (GUI) Intel 80386, for MS Windows

Size 364032 bytes

First Seen May 16, 2016, 15:09

- AV Results**
 - Win.Trojan.Agent (ClamAV)
- Behavioral Indicators**
- Network Connections**
- Associated Samples (max of 20 shown), powered by Cisco Amp Threat Grid**

For Additional Information [Hash View](#)

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

ABOUT CISCO SYSTEMS

CISCO SYSTEMS INC. is the worldwide leader in networking for the Internet. The company was founded in 1984 by two computer scientists from Stanford University seeking an easier way to connect different types of computer systems. Cisco Secure is now the largest B2B Cybersecurity company by revenue.