Application: 5726

Cognitive Operations for Security Incident Detection and Response

Page: General Information

Provide information about the company to be considered for the award. If you will be nominating an individual, specify the nominee’s employer.

Name of Organization/Company

Cisco Systems, Inc.

[redacted]

Additional Contacts

I would also like to have others receive emails about the disposition of our entries.

Page: Entry Information

Entry Title

Cognitive Operations for Security Incident Detection and Response

Category

Q06f. New Service of the Year- Information Technology - Managed Services

New Service Submission Format

Written Answers

a. Briefly describe the organization that developed the nominated new service: its history and past performance (up to 200 words). Required

Cisco Systems, Inc. is a global leader in networking for the Internet, providing hardware, software, and services that enable seamless access to information worldwide.

Founded in 1984 by Stanford University computer scientists, Cisco has consistently led in the innovation of Internet Protocol (IP)-based networking technologies. Cisco specializes in routing and switching, while also advancing technologies in areas like home networking, IP telephony, optical networking, security, storage area networking, and wireless technology.

Cisco not only offers cutting-edge products but also a wide range of services, including technical support and advanced services. The Customer Experience (CX) organization within Cisco focuses on delivering personalized, proactive, and predictive digital experiences for support and lifecycle management, enhancing customer engagement and satisfaction.

Through its continuous innovation and comprehensive service offerings, Cisco facilitates easy access to information for individuals, companies, and nations, reinforcing its position as a pioneer in the networking industry.

Within Cisco, this innovation was developed within Cisco's Customer Experience (CX) service, for use by Cisco Managed Services (CMS) which remotely operate customer's network and security operations centers.

b. Specify the date on which this nominated service was introduced to the marketplace. Outline the nominated service's features, functions, benefits and novelty (up to 250 words). Required

IT Security teams struggle to defend their organization, since they are bombarded with alerts from too many disparate tools with no way to effectively prioritize, investigate, and rapidly remediate threats. Extended detection and response (XDR) is the essential answer to this challenge, with security incident detection and automated response capabilities for security operations teams.

Since July 2023, the approach has been to use programmatic (static rule-based) workflow automation in Cisco XDR Automate to respond to security threats. The challenge with this approach is that each automation workflow needs to be identified, developed, and maintained.

With Cognitive Operations, we present a new approach using Generative AI to fully automate security incident response without writing rule-based response. This innovation introduces generative AI at the heart of the security investigation, analysis, response, and remediation. As a result, generative AI analyzes and responds to security threats for scenarios that don’t have a match for any specific detection & response workflow and even handles security threats that their organization has never seen before.

c. Explain why the nominated service is unique or significant. If possible compare the service to competitors' offerings and/or to the organization's other or past products (up to 250 words). Required

With a rule-based approach to security incident and response, it requires a complete management discipline to the automation portfolio, including:

• Identification of security incident scenarios that need automation

• Prioritization of scenarios into the most important ones

• Development of a rule-based workflow

• Maintenance, testing, and releasing of changes to workflows, as business processes or best practices evolve.

In contrast, with this innovation to integrate Cognitive Operations, security personnel no longer have to write and maintain scenario-specific workflows, allowing for a ‘one-fits-most‘ type of approach to automated response. A cognitive approach to analysis and response allows for security investigation and response to be faster, more consistent, and less expensive:

• Handles incident response at the speed of operation, reduce investigation and response times from hours to less than 5 minutes.

• Reduces operating expense of security operations center, by reducing the time or number of incidents that human analysts need to work

• Reduces the amount of escalations and transfers between teams, by harnessing the cross-domain intelligence of large language models.

• Policy and technical knowledge can be continually updated to improve efficacy and specificity of knowledge over time, through an easily managed interface.

• Improves quality of response and record keeping, through the benefit of automation, allowing for reduction in human inconsistencies across analysts or human error.

• Provides ability for human approval and reinforcement to continually improve the intelligence through time.

d. Reference any attachments of supporting materials throughout this nomination and how they provide evidence of the claims you have made in this nomination (up to 250 words). Optional

This capability has been integrated into Cisco’s Managed Detection and Response (MDR) services since August 2024 for 33 customers, demonstrating correct action for over 70% of the incidents. This also helps to more effectively manage false positives in SOC incident response, which we currently observe at 40% of the overall volume.

An integration in another technology domain (managed services for network operations) using the same approach is also currently in development to start testing in Summer 2025.

The capability is fully functional and has been open sourced on Github. We have also been teaching customers for the last year on how to build these integrations at Cisco Live US 2024 and Cisco Live Amsterdam 2025.

This framework takes what used to be days of development to write new rule-based specific response workflows, and instead be able to introduce new tools, use cases, and knowledge in the matter for a few hours, significantly improvement development velocity and time to release new automation into production.

Finally, Cisco offers services through CX that help a customer build these integrations, which will be rebranded under Cisco’s consultative AIOps service by the end of 2025.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Would you like to add an additional supporting document?

Yes

Supporting Document 2

[redacted]

Would you like to add an additional supporting document?

No

By your submission of this entry to The Stevie Awards, you verify that you have read and agreed to abide by the regulations, terms and conditions of the competition (https://www.asia.stevieawards.com/rules-and-terms-conditions-competition)

Terms and Conditions

I Agree