Industry Leaders Collaborate at OASIS to Define Cybersecurity Course-of-Action Playbooks with CACAO

Accenture, Cisco, Cyware, EclecticIQ, FireEye, Fornetix, IBM, New Context, Syncurity, ThreatQuotient, U.S. NIST, and Others Will Develop Machine Readable Cyber Response Playbooks

24 September 2019 Members of the OASIS nonprofit consortium are working together to create an international standard that implements the course-of-action playbook model for cybersecurity operations. The work of the new OASIS Collaborative Automated Course of Action Operations (CACAO) for Cybersecurity Technical Committee [1] will describe and document the steps needed to prevent, mitigate, and monitor responses to attacks.

"The best way organizations can defend against threats is to document their prevention, mitigation, and remediation steps into course-of-action playbooks," said Allan Thomson of LookingGlass Cyber Solutions, co-chair of the OASIS CACAO Technical Committee. "Unfortunately, most playbooks are one-off's at this point. CACAO represents a significant opportunity to define a standard mechanism for playbooks, so they can be executed and shared across organizational boundaries and technology solutions."

Bret Jordan of Symantec, co-chair of the OASIS CACAO Technical Committee, added, "The need for automated and shareable cyber security playbooks is critical to improving operational cyber security. CACAO will not only define how playbooks are created, the standard will also describe how playbooks are distributed across networks, business units, organizations, and systems."

Each CACAO playbook will consist of a sequence of cyber defense actions that can be executed by various technological solutions. CACAO playbooks will be referenceable by other cyber threat intelligence that provides support for related data such as threat actors, campaigns, intrusion sets, malware, attack patterns, and other adversarial techniques, tactics, and procedures.

Participation in the CACAO Technical Committee is open to all through membership in OASIS. Security Vendors, Incident Responders, Security Operation Centers (SOCs), Security Orchestration, Automation and Response (SOAR) solution, CSIRTS, Cyber Defense Centers, Threat Intelligence Analysts, Large Enterprises, Governments, MSSPs, and others are invited to join the group.

Support for CACAO

Accenture Managing Director, Anup Ghosh, said, "The lack of standardized playbooks for interoperability between vendor products has advantaged cybercriminals. The efforts of the CACAO Technical Committee to standardize and share their operations playbooks can now tilt the balance in favor of defenders. We are excited to contribute to the CACAO technical committee to address this issue and to enable the development of
standardized playbooks for security operation centers."

**Cisco Systems** Senior Technical Leader, Security Business Group, Jyoti Verma, said, "The deliverables of the new OASIS CACAO TC are of paramount importance in the fight against advanced threat actors; by defining cyber defense actions that can be executed in the form of machine-readable playbooks. These playbooks could be used to capture security processes around detection, investigation and response of cyber security threats. Having a standard way to represent these playbooks would enable organizations to share and leverage known techniques for SOC operational efficiency."

**Cyware Labs** VP of Research and Innovation, Avkash Kathiriya, said, "We are proud to join forces with the CACAO initiative as they mature the threat intelligence domain. By empowering security teams to go beyond the simple sharing of information, this initiative will ensure organizations can take action and yield results that will improve their ability to proactively block threats. The initiative will also work towards the standardization of COA Playbooks so customers can speak the common language of preventing, defending and remediating threats."

**EclecticIQ** Director, Intelligence Collaboration, Chris O’Brien, said, "It is critical to continuously improve the ways that we collaborate on threat intelligence within the cyber security community. The work that OASIS has put into these efforts cannot be valued highly enough. With the launch of the CACAO TC, we take the next important step to develop a protocol that will further streamline collaboration on remediation in the form of standardized playbook languages for courses of action."

**FireEye** Chief Engineering Architect & Distinguished Engineer, Paul Patrick, said, "The ability for an organization to create a playbook that can be shared and utilized by other organizations creates a true force multiplier across the security industry. Threat actors are constantly changing their tactics and implementing new targeting techniques. By creating a standardized response framework that works across technologies already in place, security teams will be able to thwart and respond to future attempts without prior knowledge of the attack."

**Fornetix** CTO, Charles White, said, "In regards to Collaborative Automated Course of Action Operations, the Fornetix Team is proud to support this new technical committee. Orchestration for Courses of Action is critical for building Cyber Resiliency in the enterprise. We look forward to contributing to the CACAO specification."

**IBM Security** Chief Architect of Threat Management, Jason Keirstead, said, "The ability to efficiently collaborate across vendors on incident response actions and playbooks, will fill a critical gap in the cybersecurity operations ecosystem, and enable better outcomes for our clients. IBM Security is proud to support the formation of this TC."

**New Context** CEO and Founder, Daniel Riedel, said, "Rapid response time is vital for protecting society from cyberattacks. Today, the Internet is integrated into every aspect of our world. It is imperative that the knowledge on how to react to those threats is an open standard that can be shared between public and private sectors. CACAO will enable common threat remediations to be shared between organizations regardless of their technology footprint. In the end, CACAO will advance innovation and improve technologies that will enhance our ability to respond to cyber threats rapidly and keep the connected world safe. Which is why New Context is honored to be part of the Committee."
Syncurity Founder & CSO, JP Bourget, said, "Syncurity is excited to join the CACAO Technical Committee for Cyber Security. Agile playbooks will enable Blue Teams to share TTPs [Tactics, Techniques & Procedures] and produce a unified response across the organization. A standardized framework will vastly improve content-sharing beyond the enterprise and will rapidly improve our collective defenses. Syncurity is committed to the development of open, interoperable standards that will defend enterprises against attackers."

ThreatQuotient CTO and Co-Founder, Ryan Trost, said, "The opportunity for industry peers to collaborate in a meaningful way, as led by the CACAO Technical Committee, will play an important role in standardizing the documentation and sharing of security operations playbooks. With a shared mission of providing organizations with more clarity and efficiency in their cybersecurity operations, ThreatQuotient supports the efforts of CACAO to further the capabilities of today?s defenders."

More information
https://www.oasis-open.org/committees/cacao

About OASIS
One of the most respected, member-driven standards bodies in the world, OASIS offers projects?including open source projects?a path to standardization and de jure approval for reference in international policy and procurement. OASIS has a broad technical agenda encompassing cybersecurity, privacy, cryptography, cloud computing, IoT, augmented reality, and other areas. Each project operates independently under industry-approved process and IPR policies. OASIS members can be found in 100+ countries on virtually every continent. Major multinational companies, SMEs, government agencies, universities, research institutions, consulting groups, and individuals are represented. http://www.oasis-open.org Media inquiries: communications@oasis-open.org; +1.941.284.0403

Links:
[1] https://www.oasis-open.org/committees/cacao