

IBM Announces Cloud-Based Community Platform for Cyber Security Applications

CAMBRIDGE, Mass., Oct. 15, 2018 /[PRNewswire](#)/ -- IBM (NYSE: [IBM](#)) today announced a new cloud-based community platform for cyber security applications. [IBM Security Connect](#) is the first security cloud platform built on open federated technologies, with AI at its core, to analyze security data across previously unconnected tools and environments.

An IBM analysis of clients' environments found that on average, cybersecurity teams are using over 80 different security products from 40 different vendors. Our research also indicates less than 20 percent of the features in these on-premise tools are used and may not provide the outcomes clients expect due to integration and complexity challenges.

By integrating security data from IBM Security products with an ecosystem of security vendors, clients, and business partners, IBM Security Connect is designed to help improve efficiency and collaboration as teams defend against cybercrime. IBM Security Connect will enable users to apply machine learning and AI, including Watson for Cyber Security, for analysis to help them identify threats or risks and improve the efficacy and efficiency of threat detection and response. Users can design and deploy new customized and comprehensive solutions to address security outcomes, such as SOC Operations workflows or Digital Trust.

IBM Security Connect will extend the rich set of capabilities from IBM's security products, via robust integration capabilities to connect data, applications and tools from an ecosystem of vendors, made possible by the cloud.

"The growth of cybersecurity technology and data combined with a growing skills shortage is creating an unexpected level of complexity for security teams," said Marc van Zadelhoff, General Manager, IBM Security. "Leveraging the power of the cloud, we can now bring together tools, data and people without expensive customization and integration projects. Data federation through IBM Security Connect helps give security professionals increased security visibility and efficiency without the hassle of migrating data or overly complicated product integrations."

A New, Open Approach to Cloud Security

IBM Security Connect will help tackle some of the biggest security challenges today via open standards, which can help pave the way toward collaborative innovation. As it is built on open standards, it can help companies build unique microservices, develop new security applications, integrate existing security solutions, and leverage data from open shared services.

Key services include: Open security data integration services for sharing and normalizing threat intelligence, federated data searching across on-premise and cloud data repositories and security solutions, and real-time sharing of security alerts/events and insights that can be leveraged by any app or solution integrated with the platform.

IBM Security Connect will become the home of IBM's current Security App Exchange and all IBM Security applications built on a platform powered by IBM Cloud, but fully compatible with other cloud providers. IBM Security will also champion the creation of new open standards in burgeoning areas such as the sharing of response playbooks and analytics patterns and will actively invest in developing new open source projects that align with these efforts.

IBM Security's commitment to openness also means that many existing open security and protocol standards are leveraged throughout the platform, such as STIX™ (Structured Threat Information eXpression) and TAXII™ (Trusted Automated eXchange of Indicator Information). The IBM Security project [STIX-Shifter](#), which is publicly available on GitHub, consists of an open source library which allows software to connect to products that house data repositories using STIX Patterning, and return results as STIX Observations. Using these open standards for connecting to any data source combined with IBM Security's already powerful security analytics and incident response capabilities helps clients to gain broader visibility and detect threats and risks that were otherwise missed due to disconnected data across complex hybrid environments.

IBM Security Connect's initial set of applications and services will allow users to quickly connect to multiple security products or data repositories to automatically federate data for the purpose of prioritizing and responding to threats. This revolutionary approach of federating data enables clients to leave their data where it is, as opposed to building costly data lakes, which can complicate or outright prevent security data analysis.

IBM Security Connect will also be an integral part of IBM Security Services offerings both as a consumer and a contributor of new innovation; including advancements in voice-enabled AI, machine learning for security threat scoring, global threat analytics, orchestration playbooks and mobile-enabled MSS applications. IBM Security Services will leverage the open power of IBM Security Connect to develop deep and valuable integrations across its partner ecosystem to deliver greater value for its global customers.

Addressing Complexity in Cybersecurity Operations

Designed to deliver "community-driven" security strategies, IBM Security Connect will operate as an open platform with an open development community. As part of today's announcement, a significant number of technology partners and global system integrators including Cisco, Capgemini, Carbon Black, Check Point, CrowdStrike, EY, ForeScout, Forcepoint, Fortinet, McAfee, Qualys, Smarttech, Symantec, Tenable, Trend Micro, and VMware have committed to integrating with IBM Security Connect in order to help provide

improved data sharing across security vendors for our joint clients. Many of these vendors will also contribute to building integrated applications on IBM Security Connect. IBM already has hundreds of pre-built apps built by IBM and partners available via the IBM Security App Exchange for integrating at the product level. Once available, these additional integrations will be built into IBM Security Connect within months of launch, widening the reach of the platform to help manage compliance and address threats.

For example, one of the first solutions being tested by clients will focus on Threat Operations Workflow. This solution is designed to empower security analysts to proactively identify, investigate, and respond to their most critical threats from a single, cloud-based solution. Threat Operations Workflow integrates seamlessly through open connectors to QRadar (both on-premise or cloud), as well as other SIEMs and endpoint solutions. By leveraging open SDKs, other security data ponds or lakes such as Hadoop, and point security products can be supported to provide a federated view and workflow for security analysts across previously unintegrated and siloed products.

Built in Expertise and Skills

With the well-documented skills challenge the security industry is facing, IBM Security Connect will also feature digitized expertise from IBM's 4,000+ global security practitioners to provide best practices and guidance on how to implement security and risk management strategies. The pre-integrated apps allow users to create easy-to-use common workflows across multiple applications, so teams can focus on solving security issues instead of struggling to integrate dozens of security products. In addition, IBM Security has dedicated 50 developers toward development of the community, where security practitioners can collaborate and share integrations.

IBM Security Connect is designed to make accessing IBM X-Force Security Services expertise even easier for clients at all levels; including offerings and expertise in X-Force Red Security Testing, Managed Security Services and Incident Response Services.

IBM Security Connect is anticipated to be available in 1Q 2019.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 60 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security, follow IBMSecurity on Twitter or visit the [IBM Security Intelligence blog](#).

CONTACT:

Dillon Townsel

dillon.townsel@ibm.com

512-571-3455

SOURCE IBM
