IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Black Hat 2018 — To the Edge and Beyond

August 22, 2018

By: Robert Ayoub, Frank Dickson, Christopher Kissel, Sean Pike, Robert Westervelt

IDC's Quick Take

The annual Black Hat conference took place August 4–9, 2018, in Las Vegas. The show is considered the top technical information security conference and includes hands-on trainings, briefings, and a business expo over the course of the conference. This year's conference continued the tradition of advanced technology sessions around hacking endpoints but also added content around human issues such as diversity and PTSD, as well as an increasing number of sessions looking at cloud and IoT. From a vendor perspective, IDC felt that many significant platform updates were announced as well as solidification of partnerships and integration of acquisitions announced earlier in the year.

Event Highlights

Black Hat traditionally falls about six months after RSA and provides an excellent opportunity to rate progress on RSA announcements. This year, RSA was late, and therefore, Black Hat was only four months after RSA. This left little time for many major changes to the vendors since RSA; however, as mentioned previously, several acquisitions did occur just prior to the Black Hat show. That being said, several key themes were present during the show.

IDC's Point of View

Several key themes that were presented during the show are discusses in the sections that follow.

The Move to the Edge Is Real

Previous Black Hat shows focused on the seeming novelty of hacking a wide variety of endpoint devices (anyone remember the car wash hack?). But as IoT devices are more pervasive on enterprise networks and their security is more regularly being included under the auspices of the CISO, the need for better insight around securing these edge devices seems to have moved past the novelty phase.

Many vendors talked about the integration of IoT-specific capabilities into their platforms. Encryption was another hot topic as organizations look to protect data as it transits the cloud. In addition, there was an increasing number of discussions around detection of malware in encrypted data streams. Mobile security had an increased emphasis this year as well from the vendor community with numerous vendors demonstrating mobile security capabilities.

The final and perhaps most significant indication that a shift has occurred in architecture is the sudden inclusion of identity protection as a core security component. While vendors struggled to find a voice in the security conversation in years past, this year, it seemed vendors were the belles of the ball. At one point, I'm positive I saw the Duo team walking in slow motion through a crowd of people like the primary protagonist in the house party scene of a college party flick (this is probably over the top but true). Let us not forget that SecureAuth and Core Security were merged recently with the idea of addressing the "intelligent intersection of security and identity." The trend is very real and was prognosticated in March 2017 by IDC in *Identity and Access Management: The 3rd Platform Foundation*

of Cybersecurity. As more and more enterprises focus on transforming their architecture and moving workloads to the edge, ensuring (and continually ensuring) the identity of both humans and devices before they access corporate resources becomes critical.

It's All About the Platform

The discussion around the move to a platform has been ongoing for over a year now. With organizations transitioning from on-premise to both private and public cloud and the continued information security workforce challenges, security vendors are being forced to innovate their management consoles and toolsets to operate more efficiently across all platforms and to combine tangential functions into those platforms to help address console fatigue.

Many of our discussions centered on integration of acquisitions into a platform approach or how a vendor's platform offers operational and management efficiencies over pure-play competitors. In particular, the platform approach was clearly articulated by numerous vendors. Palo Alto Networks shared insight around its XDR platform concept. Fortinet's recent acquisition of Bradford Networks continues to augment its security fabric. Qualys announced its Passive Network Sensor (PNS), a new member of the Qualys sensor family that natively integrates network analysis functions into the Qualys Cloud Platform. Splunk shared that it has completed integration of Phantom Cyber into its platform.

Just before Black Hat, Spirent announced the integration of Data Breach Emulation onto its CyberFlood platform. Emulation is different than attack simulation: Spirent emulates 10,000+ applications, 3,000+ attacks, and 19,000+ malware scenarios in a test environment. With 18 patents in hyperrealism and another 2 pending, Spirent is able to recognize a DoublePulsar attack or an adversary running an exchange exploit.

Both the discussion of the expanding edge and the continued expansion of platforms and capabilities were encouraging. Given last year's almost exclusive focus (from the vendors) around ML and AI and RSA's extensive promotion of partnerships, Black Hat provided validation that some of the more lofty notions in security (e.g., that ML and AI will solve all our problems) are giving way to more practical use cases such as validated proofs of partnerships and fully integrated acquisitions.

Security Researchers Target IoT Devices, Industrial Control Systems

Security researchers are showing renewed vigor identifying weaknesses in the infrastructure that supports industrial control system environments and, in particular, environments that control critical functions in dams, traffic management systems, tunnels, and other infrastructure. Researchers warn that attackers have easy access to penetration testing tools from valid security vendors and electronic testing instruments and even security gateway firmware on eBay and other websites at relatively low cost. During one demonstration, a penetration tester and security consultant showed how he could identify and exploit many vulnerabilities in widely deployed industrial control gateways and showed how a real-world attack could lead to catastrophic failure.

The manufacturers of these solutions have been largely cooperative but should heed all the attention their products are gaining at Black Hat as a sign to invest in ways to strengthen internal patch management and secure software development processes. Chief information security officers and those tasked with managing security in industrial control systems environments should balance vulnerability-based and threat-based approaches to risk management.

Let's be clear. Vulnerabilities have been widely known in industrial control system environments for years. Practitioners should identify and address weaknesses and configuration issues but also consider the attack activity, determine who the likely threat actors are, and address the critical assets most at risk. The goal of any security professional these days is to succeed even in the face of many software bugs.

RSA Jr? Maybe Not

Having attended Black Hat for many years, the IDC analysts could not help but wonder if Black Hat was evolving into something without a unique purpose. Attendance has clearly increased as the event has taken an increasingly commercial appeal. The expo floor clearly had an RSA Security Conference–type feel. However, the increased commercial "RSA lite" feel seems to come at the expense of technical depth. Black Hat did not have significant commercial announcements like the RSA Security Conference. Black Hat also did not have the same level of technical announcements, such as the famous "Jeep hack" of years ago. Only time will tell if Black Hat becomes "just another show."

Subscriptions Covered:
Internet of Things: Security Practices, Security Products