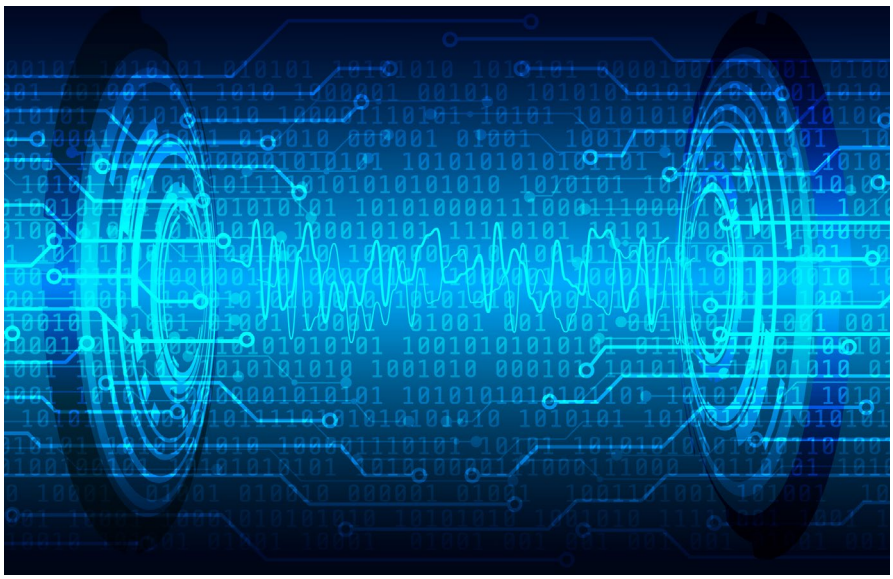
Highlights from webcast on Data Security

THE SIGNAL IN THE NOISE: MAKE SECURITY DATA WORK FOR YOU

A Digital Dialogue based on a webcast featuring a spokesperson for Ivanti Xtraction.



Everybody talks about the need for data security. But most IT and security professionals say providing it is not easy.

Here is what Ivanti, the company that unifies IT to better manage and secure the digital workplace, is hearing from its customers regarding what they are facing in terms of data security problems:

- Compliance issues
- Delays due to complexity
- Resource shortage in security teams
- Gaps and new threats impacting security
- Rising cost of oversight and compliance

Much of the complexity IT faces is the fact that 55 percent of security professionals use technology from at least six vendors, according to the Cisco 2017 Annual Cybersecurity Report. That is a lot to keep track of if you have to go from one vendor's interface to another and then remember what you were seeing in the five or more other interfaces you have to keep an eye on.

Security teams wrestle with IT systems and must cross-reference output manually, putting it all in a spreadsheet just to produce one report. That takes a lot of time and resources. To make matters worse, security teams are often shorthanded. Manual reporting may fall through the cracks.

Security Gaps and Silos

Gaps in oversight can result from silos of security tools including governance, risk management and compliance (GRC), asset management, identity management, and patch management. This leads to gaps in visibility that make it hard for IT teams to get a holistic view of overall security technology, which can leave the IT infrastructure at increased risk. With information coming at IT from various sources in varying timeframes, response to any security risk is dangerously slow while security threats continue to evolve. If IT pros are only looking at the interface from one of its tools, there is the possibility that they will be lulled into a false sense of security. On the other hand, trying to manually comb through all of the data coming from six or more tools is often too time consuming and so IT does not have a big picture of security. It's hard to tell what is just noise and what is critical data. It also makes it difficult to provide data needed for compliance audits that can come at any time and completely disrupt workflow.

"You need to consider a different approach to reporting to deliver up-to-the-minute meaningful and actionable IT security data critical to every business," a spokesperson for Ivanti Xtraction told the webcast audience.

IT needs a way to make security data visible and available with a methodology that will satisfy any audit.

There are three areas where it is important for IT security teams to focus on in reporting:

1. How is your environment performing
2. Knowing the status of patches
3. Compliance reporting

> "You need to consider a different approach to reporting to deliver up-to-the-minute meaningful and actionable IT security data." —Ivanti

Critical Security Controls

Center for Internet Security's Critical Security Controls (CSC) is a set of practical defenses for stopping cyberattacks. The CSC offers prioritized, well vetted, and supported security actions organizations can take to assess and improve their current security state. Focusing on the top five controls will help security teams cover 85 percent of cyberattack scenarios:

1. Unauthorized/Authorized Device Inventory: Security teams need to discover and manage devices to ensure authorized devices can gain access on network, but prevent unauthorized and unmanaged devices from gaining access. They need to know what devices are on their network and how to defend them.

2. Unauthorized/Authorized Software Inventory: Security teams need to discover and manage software on devices to ensure only authorized software can be installed and executed on the network. At the same time, they need to prevent unauthorized and unmanaged software from being installed or executed. This includes Application Whitelisting so users can only run applications that are explicitly approved.

3. Secure Configuration (Hardware/Software): Security teams need to define, implement, and manage configuration of all hardware and software. This includes:

- Implementation of secure configuration systems at scale (like AD Group Policy, etc…)
- Track, report on and correct issues via rigorous workflow management and change control processes
- Identity and service management to prevent attackers from exploiting vulnerable services and settings

4. Vulnerability Assessment & Remediation: Security teams need the capability to assess and remediate vulnerabilities including:

- Continuous assessment of OS and third-party application vulnerabilities
- Scan for threats based on up-to-date information associated with level of risk
- Patch Management
- Detect vulnerabilities and take informed action to mitigate
- Minimize window of opportunity for attackers

5. Controlled Use of Admin Privileges: Security teams need capabilities to track and control admin rights. Gaining access to admin rights is one of the ways hackers use to infiltrate an infrastructure. So it's important to manage who has privileges for what computers, networks and applications, while ensuring users have the necessary rights to do their jobs. This also includes privilege management to remove unnecessary system rights or permissions, and prevent abuse of power while supporting productivity.

Xtraction Brings It All Together

Ivanti provides a solution with its Xtraction product, which is self-service, real-time dashboard reporting software. Xtraction consolidates data from multiple sources and tools. It then presents it on one screen.

Xtraction provides CSC control insights including:

- **Visibility:** Exactly what you want to know and when
- **Insight:** Patches of greatest threats; how long environment was at risk
- **Admin Rights:** Who has admin rights and should they have those rights?
- **Devices and Applications:** Are there unauthorized devices or applications on the network?
- **Change Control:** Is the change control process being followed?
- **Application Access:** Is there unauthorized access based on roles?

Xtraction also provides insight IT security teams need to meet compliance standards.

Xtraction's pre-built data connectors mean no coding, no need for Business Intelligence (BI) gurus, and definitely no spreadsheets. Security teams are able to view data in context, and make smarter, faster decisions with ease.

Xtraction merges security tools and data to provide real-time insight. Xtraction helps you highlight trends, risks and financial impacts specific to your business.