IntSights Cyber Intelligence Releases Industry's First All-in-One Enterprise Threat Intelligence & Mitigation Platform

Leading Threat Intelligence Firm Helps Enterprises Turn the Tables on Threat Actors; Unique Cyber Reconnaissance Capabilities Power Automated Risk Remediation

https://www.prnewswire.com/news-releases/intsights-cyber-intelligence-releases-industrys-first-all-in-one-enterprise-threat-intelligence--mitigation-platform-679402833.html

INTSIGHTS

SANS Report: Why Organizations Need Tailored Cyber Threat Intelligence

By Nathan Teplow, May 3, 2018 8:00:00 AM

SANS

Tailoring Intelligence for Automated Response

A SANS Review of IntSights' Enterprise Threat Intelligence and Mitigation Platform

As cyber attacks continue to grow in size, scope and complexity, organizations across the world are forced to find new ways to protect themselves and mitigate these cyber threats. This has given rise to many Cyber Threat Intelligence (CTI) solutions and services, which all serve the purpose of helping organizations identify and mitigate new cyber threats. However, each solution has its unique benefits and challenges that organizations need to consider before they begin using.

Read more »

Are Your Devops Servers Exposing Sensitive Information?

By Ariel Ainhoren, May 1, 2018 8:00:00 AM

In recent years, DevOps, the culture and practice of automating and monitoring the development life cycle, has enabled delivering software increasingly faster and shortening the time to market. Many companies have transitioned to working in a CI/CD cycle, continuously releasing software on a daily, weekly, or bi-weekly basis to respond to customer needs more quickly and keep up with changing trends.

But this practice of DevOps has brought a multitude of security issues. New tools emerge frequently, each with their own security level and configuration, causing DevOps engineers to struggle keeping up with the different configuration and security guidelines coming down from management. This struggle eventually leads to security holes.

Read more »

How to Build an Effective Threat Intelligence RFP

By Nathan Teplow, May 10, 2018 10:15:00 AM

WHITEPAPER

RFP DEVELOPMENT FRAMEWORK

THREAT INTELLIGENCE SOLUTION REQUIREMENTS AND VENDOR CAPABILITIES

INTSIGHTS
Threat Intelligence Realized.

With the cybersecurity threat landscape growing and evolving rapidly, many enterprises and other large organizations are seeking more effective ways to protect themselves and their employees from these threats. Threat intelligence platforms can help you take a more proactive approach to managing cybersecurity. By translating early warnings and imminent threats into specific security actions, you can significantly reduce your risks and preemptively mitigate attacks. To meet these goals, you need a platform that combines external data collection, cyber intelligence algorithms and live human analysis into an integrated, scalable, and manageable package. There are a range of quality threat intelligence platforms to choose from. The challenge you face is determining which solution is best for your unique needs and business requirements.

Read more »

Are Your Employees Exposing Login Credentials Through Collaboration Tools?

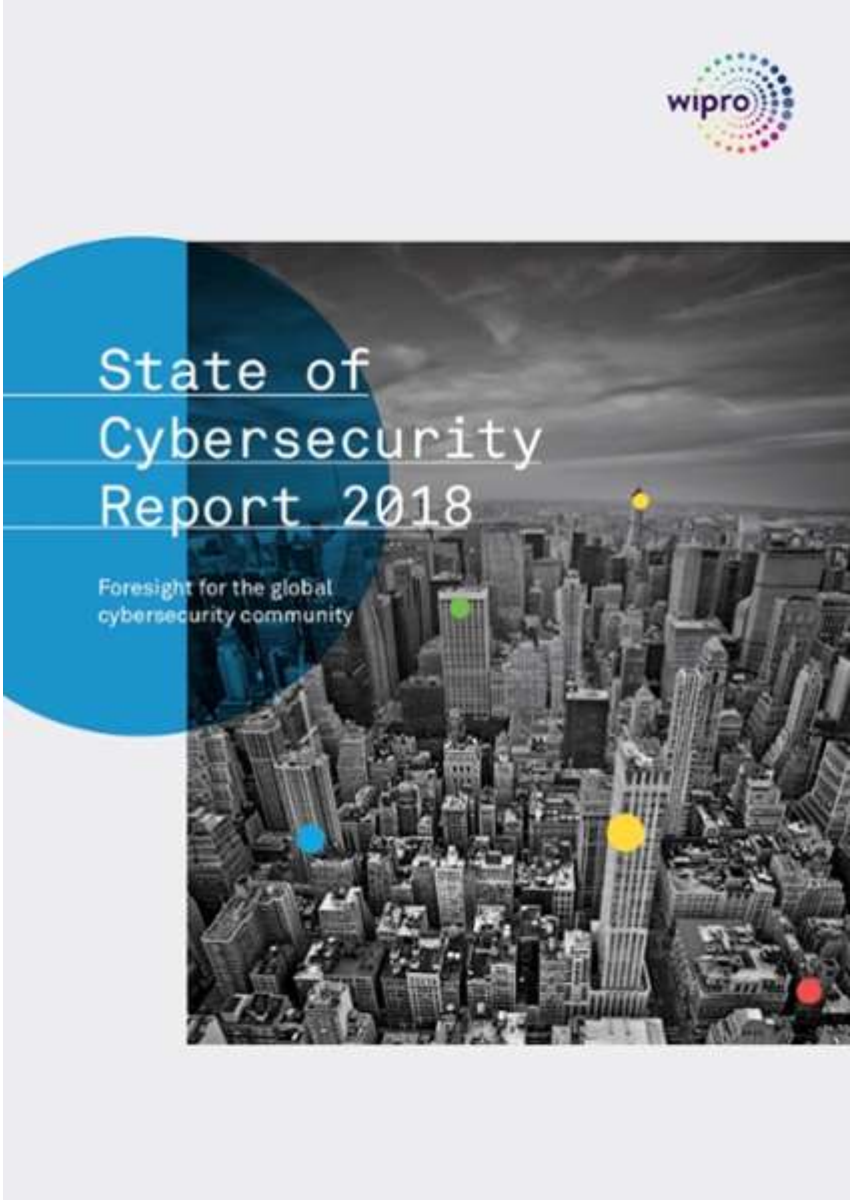
By Alon Arvatz, May 9, 2018 9:48:22 AM

Last week, Brian Krebs, who runs the popular security blog KrebsOnSecurity, published some interesting research about how employees are posting corporate login credentials within tools that are exposed to web searches. In particular, he looked at Trello.com, a popular collaboration and project management tool, and found numerous instances of exposed login credentials on publically available Trello boards.

On a similar note, the IntSights Threat Research team published new research last week about organizations unknowingly exposing DevOps servers to the web. When servers and 3rd party tools are accessible online via simple search techniques, it becomes incredibly easy for hackers to discover sensitive information that was intended to only be accessed internally.

Read more »

New Wipro Report: State of Cybersecurity 2018



By Nathan Teplow,
May 21, 2018
9:00:00 AM

2017 was a historic year for cybersecurity. The estimated number of records stolen through 2017 doubled from 2016 (from 1.38 billion to 2.7 billion). In addition, the world was hit with unprecedented ransomware attacks, like WannaCry (which we just celebrated the 1 year anniversary of). This has caused organizations to re-think how they approach cybersecurity and allocate their budgets. It's also caused cybercriminals to shift their tactics and tools when planning and launching cyber attacks.

Wipro recently published their State of Cybersecurity 2018 Report, which provides an overview of the existing cybersecurity landscape and how organizations are currently protecting themselves. IntSights is proud to be one of the key contributors to this year's report.

Read more »

Watch: Dark Web Tour with CSO Online

By Nathan Teplow, May 17, 2018 9:00:00 AM

You've likely heard of the Dark Web, but do you really know what it is and how it's used? There’s a lot of hype and confusion surrounding the Dark Web these days, but it can actually be an asset in protecting your organization from cyber crime. IntSights' Chief Product Officer, Alon Arvatz, recently sat down with Steve Ragan from CSO Online, to provide a brief tour of the Dark Web and dispel some of its common misconceptions. Alon also shares a few best practices for navigating the Dark Web and how organizations can use it as a source of threat intelligence to anticipate and defend against cyber attacks.

Watch Alon's tour of the Dark Web and find out how you can leverage it to protect your organization.

Read more »

WannaCry Outbreak Anniversary: What We Really Learned Over the Past Year

By Itay Kozuch, May 16, 2018 9:00:00 AM

On May 12, 2017, WannaCry ransomware surprised the world and began spreading across hundreds of thousands of computers around the globe. To build the attack, WannaCry's creators exploited an EternalBlue vulnerability, which was stolen by the Shadow Brokers from the NSA (National Security Agency). They also leveraged additional tools and exploits, enabling the ransomware to spread quickly and encrypt vulnerable computers on its way.

The WannaCry attack made international headlines and changed the way we think about malware attacks. Here's what we've learned in the past year since the initial WannaCry outbreak.

Read more »