THE STATE OF SECURITY (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/)

News. Trends. Insights.

HOME (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY) » FEATURED ARTICLES (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/FEATURED/) » Threat Intelligence Fundamentals

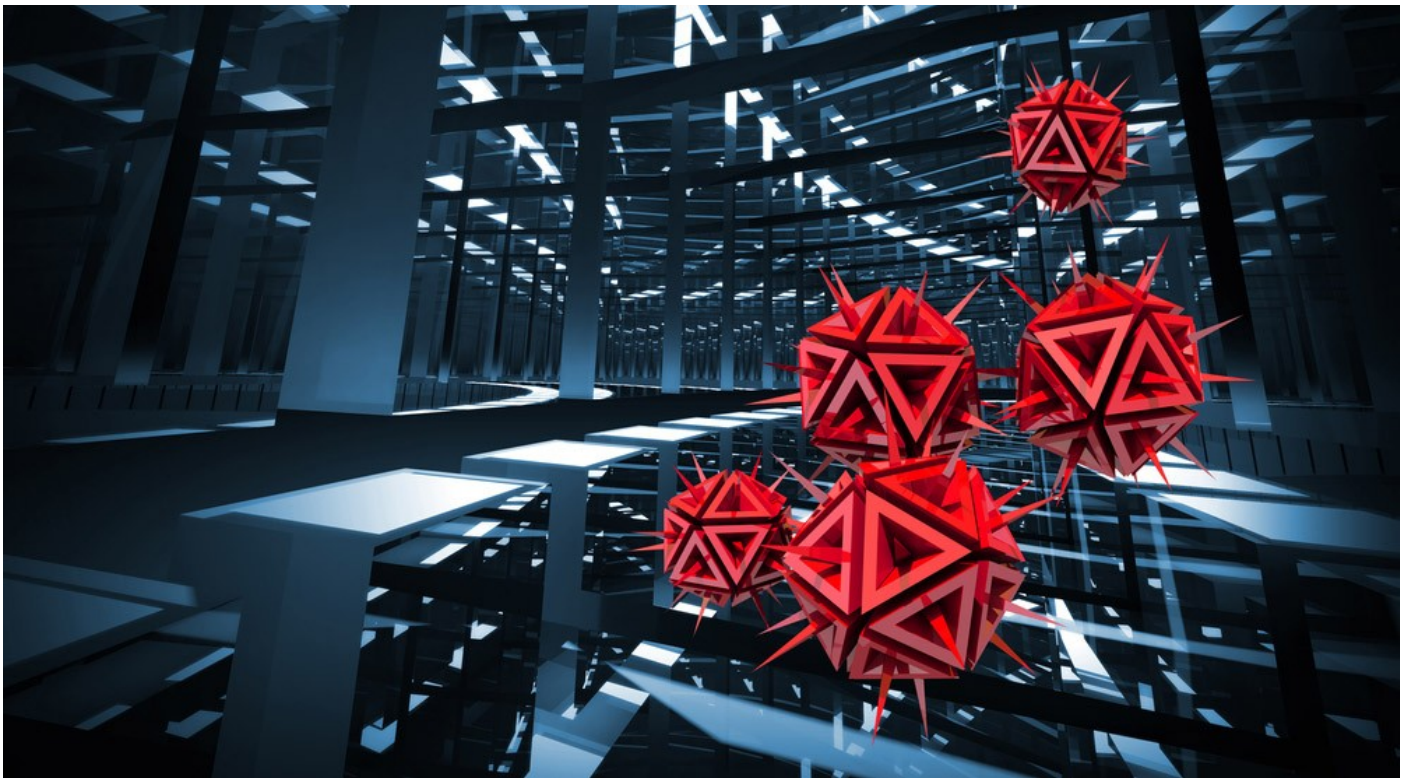
Threat Intelligence Fundamentals

(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/PAUL-NORRIS/)

PAUL NORRIS (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/PAUL-NORRIS/)

DEC 1, 2015 |

OFF TOPIC (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/OFF-TOPIC/)



(http://www.tripwire.com/state-of-security/off-topic/threat-intelligence-fundamentals/)

7 123 15

With so many disparate offerings and so much pressure to be ‘conducting’ threat intelligence, companies today risk investing a lot of time and money with little positive effect on security.

Threat intelligence (http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/what-is-the-best-way-for-a-company-to-consume-threat-intelligence/) is the process of moving topics from ‘unknown’ to ‘known unknowns’ by discovering the existence of threats within your environment and moving them to the ‘known knowns’ where the threat is well understood and mitigated.

For example, an ‘unknown’ could be that zero-day attack waiting to be dropped in to your environment and you nor the industry has any intelligence on it. A ‘known unknown’ could be a piece of malware that has been written and is out in the wild, but you have no idea when, where or who will use it to exploit your systems, whereas a ‘known known’ is where the threat or malware is well known, documented and plenty of mitigating controls are in place.

Threat intelligence is a vital part of your security arsenal, making it possible for you to consume and analyse multiple sources of threat data and ultimately improve threat detection and response. But where do you start? And how do you wade through seemingly infinite amounts of threat data to determine what is actionable for your organisation and functional with your existing security tools?

The Tripwire Technology Alliance Program (http://www.tripwire.com/company/partners/technology-alliance-partner-tap-program/#threat-intelligence) supports a rich ecosystem of Security Technology partners to provide customers with complete solutions for advanced cyber threat protection.

An example here would be how our customers can utilise Tripwire Enterprise to detect new files on systems being monitored which can then be also screened by a third party to determine if they are malicious and, therefore, pose a threat to the organisation.

Tripwire is hosting a webcast as part of their 'Threat Intelligence University (http://info.tripwire.com/register-threat-intelligence-university-emea/?source=socialmedia)' on the 9th December 2015 between 8 am and 11.30 am GMT.

In this half-day virtual event, you will learn:

- How to make threat intelligence information actionable
- How to evaluate the wide range of threat intelligence technology options available to help bolster detection and remediation capabilities
- How to improve security efficiency by combining business context with vulnerability intelligence through the use of golden builds
- Why threat modeling matters and how to prevent the most common mistakes
- How to leverage the different technologies in your arsenal to improve your overall threat intelligence and reduce risk
- Predictions for the future of threat intelligence 2016 and beyond…

By attending, you can earn up to **3 CPE credits**.

AGENDA

Time	Session	Speaker
8:00 am	Introduction/How to Make Threat Intelligence Really Work	Paul Edon
8:30 am	Internet Security Threat Landscape Countermeasures	Lloyd Webb
9:00 am	Forget the Needle, Focus on the Haystack	Dean Ferrando
9:30 am	These Aren't the 'Threats' You're Looking For…	Paul Norris
10:00 am	Threat Modeling: Lessons from Star Wars	Adam Shostack
11:00 am	Closing/Today's Top 5 Takeaways & Future Predictions	Paul Edon

Join industry thought leaders including Adam Shostack, author of *Threat Modeling* and Tripwire's security experts for the latest installment of Tripwire's ***Threat Intelligence University***.

Click here to find out more. (http://info.tripwire.com/register-threat-intelligence-university-emea/?source=socialmedia)

7 123 15

CATEGORIES Featured Articles (http://www.tripwire.com/state-of-security/topics/featured/), Off Topic (http://www.tripwire.com/state-of-security/topics/off-topic/)

TAGS threat intelligence (http://www.tripwire.com/state-of-security/tag/threat-intelligence/), tripwire (http://www.tripwire.com/state-of-security/tag/tripwire/), webcast (http://www.tripwire.com/state-of-security/tag/webcast/), zero-day (http://www.tripwire.com/state-of-security/tag/zero-day/)

0 Comments The State of Security 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON **THE STATE OF SECURITY** WHAT'S THIS?

Android Malware Uses Social Engineering to Enable Automatic App Installation

1 comment • 13 days ago

Avat Nigel Tolley — Is there even a strong warning about giving up control over what is effectively root? I'll not give that permission to …

Beware the Cyber Blind Spots

1 comment • a month ago

Avat Dan Sveaver — Have you heard the term 'cyber analytics'? I'm supposed to write a paper about it for my Information Assurance …

What Happens to Hacked Social Media Accounts

2 comments • a month ago

Avat Christina — Many of my accounts have been hacked and information grossly altered or deleted. From what I understand it is a a …

Study: US IT Pros Less Confident in Board's Cybersecurity Literacy Than UK …

1 comment • a month ago

Avat duniajilbab — Thanks for sharing, hope that it can be a goodness for us all. be a modest muslimah , Keep istiqomah. ^^

Subscribe Add Disqus to your site Privacy DISQUS

About Paul Norris

(http://www.tripwire.com/state-of-security/contributors/paul-norris/)

Paul Norris (http://www.tripwire.com/state-of-security/contributors/paul-norris/) has contributed 1 post to The State of Security.

View all posts by Paul Norris (http://www.tripwire.com/state-of-security/contributors/paul-norris/) >

Follow @pjnorris

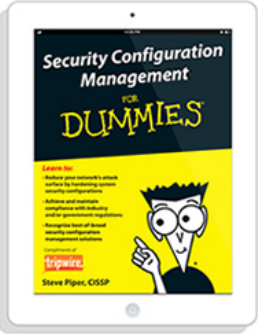
The State of Security Newsletter

Receive the latest security stories, trends and insights directly in your inbox each week.

Enter your email address here...

Sign Up

FREE EBOOK



Latest Security News (/state-of-security/topics/latest-security-news/)

New ‘Pro’ Point-of-Sale Malware Found For Sale in Underground Forums DEC 2, 2015

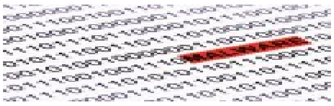
China Blamed for Hack into Australia’s Bureau of Meteorology DEC 2, 2015

Scope of FBI’s National Security Letters Revealed by Lifted Gag Order DEC 1, 2015

Europol Takes Down 1,000 Websites Selling Counterfeit Goods NOV 30, 2015

ISPs Cannot Be Forced to Block Customers’ Access to The Pirate Bay, Finds Swedish Court NOV 30, 2015

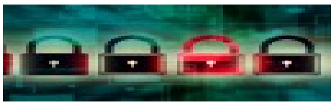
POPULAR FEATURED RECENT



(http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/dyreza-trojan-can-now-hook-into-microsoft-edge-enlist-windows-10-users-into-botnet/)

Dyreza Trojan Can Now Hook into Microsoft Edge, Enlist Windows 10 Users into Botnet (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/dyreza-trojan-can-now-hook-into-microsoft-edge-enlist-windows-10-users-into-botnet/)

NOVEMBER 29, 2015



(http://www.tripwire.com/state-of-security/security-awareness/the-three-principles-of-a-secure-system/)

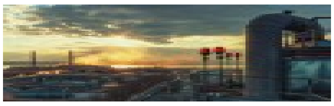
The Three Principles of a Secure System (http://www.tripwire.com/state-of-security/security-awareness/the-three-principles-of-a-secure-system/)

NOVEMBER 30, 2015

(http://www.tripwire.com/state-of-security/latest-security-news/magspoof-device-can-wirelessly-emulate-magnetic-stripe-credit-card/)

MagSpoof Device Can Wirelessly Emulate Magnetic Stripes, Credit Cards (http://www.tripwire.com/state-of-security/latest-security-news/magspoof-device-can-wirelessly-emulate-magnetic-stripe-credit-card/)

NOVEMBER 26, 2015



(http://www.tripwire.com/state-of-security/featured/the-industrial-internet-of-things-fueling-a-new-industrial-revolution/)

The Industrial Internet of Things: Fueling a New Industrial Revolution (http://www.tripwire.com/state-of-security/featured/the-industrial-internet-of-things-fueling-a-new-industrial-revolution/)

NOVEMBER 29, 2015

(http://www.tripwire.com/state-of-security/latest-security-news/open-source-router-updates-its-own-security-analyzes-web-traffic/)

Open Source Router Updates Its Own Security, Analyzes Network Traffic (http://www.tripwire.com/state-of-security/latest-security-news/open-source-router-updates-its-own-security-analyzes-web-traffic/)

NOVEMBER 27, 2015

(http://bit.ly/1Kb6rne)

Tweets Follow

Tripwire, Inc. @TripwireInc 20m
Threat Intelligence Fundamentals bit.ly/1Toxm5X via @pjnorris #infosec #security
Show Summary

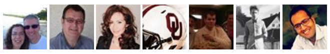
Tripwire, Inc. @TripwireInc 2h
5 Key Challenges for the Industrial Internet of Things (IIoT) tripwire.me/21uGlbk via @DMBisson w/ @PatrickCMiller @garymintchell #IIoT
Show Summary

Tripwire, Inc. @TripwireInc 6h
China Blamed for Hack into Australia’s Bureau of Meteorology tripwire.me/1TuqzrF via @DMBisson #security #infosec
Show Summary

Tripwire, Inc. @TripwireInc 7h
Highlight Endpoint Changes to Thwart Emerging Breaches

Tweet to @TripwireInc

Be the first of your friends to like this



Topics (/state-of-security/topics/)

- Government ›
- ICS Security ›
- Incident Detection ›
- IT Security and Data Protection ›
- Latest Security News ›
- Off Topic ›
- Regulatory Compliance ›
- Risk-Based Security for Executives ›
- Security Awareness ›
- Security Slice ›
- This Week in Security ›
- Tripwire News ›
- Vulnerability Management ›

FOLLOW US