Kevin Richards
Managing Director, North America and Strategy & Risk Lead

(Full transcript)
June 2017

(FULL VIDEO)

Building Resilient Healthcare Systems
iDefense® Vulnerability Management

Kevin Richards
At iDefense®, part of Accenture Security, we understand that today's security executives and practitioners require a new way to consume dynamic intelligence so they can investigate threats and take action. In order to fulfill this requirement, Accenture Security has developed the iDefense® IntelGraph, an innovative new tool to capture and link all facets of the cyber threat landscape together.

This data-driven security intelligence application allows practitioners to quickly understand the diverse threats they are facing, investigate additional risks to their organization, allocate resources effectively and determine the proper courses of action to take.

This use case focuses on vulnerability threat exposure. You'll see how iDefense® IntelGraph helps users quickly determine proper risk mitigation approaches and patch prioritization. We'll ask questions likIs this vulnerability being exploited? If so, then by what malware family? Are there indicators of compromise associated with the malware family that can be used for detection or mitigation if a patch cannot be immediately rolled out? Do the vulnerabilities associated with the malware family provide links to other exploits and further remediation actions? Are any threat actors or toolkit developers attributed to or associated with the malware family? If yes, then who? And finally, are there countermeasures or signatures that can be used?

Let's say you need to investigate a particular vulnerability in Adobe Flash. Here you can add the CVE number into the search field and right away find a number of contextual relationships to this vulnerability. The nodal graph to the right shows these relationships. Some of the obvious relationships are, associated vulnerability technologies and packages from a variety of Linux distributions. You'll also see detection signatures that you can add to your IDS.

Click on the Malware Families fundamental, and right away you'll find that many exploit kits are associated with this vulnerability. Let's focus on the RIG exploit kit. Here, you can see the threat actor who developed the exploit kit. You will also find IOCs to leverage for mitigation and detection activities, which will help to reduce your threat exposure in case you can't patch right away. Upon further investigation, we learn that the Magnitude exploit kit also exploits this vulnerability. You'll now need to add this CVE to the top of your patch prioritization queue, since it's being exploited by two significant malware families.

With iDefense® IntelGraph, you can find IOCs and signatures to leverage for detection and mitigation activities, uncover potential previously unknown security risks, and prioritize your security resources more effectively.

To learn more, go to Accenture.com/iDefense.

END