



The Power to Prevent:
It's the Next Generation

FIDELIS SECURITY SYSTEMS, INC. 4416 EAST WEST HIGHWAY, SUITE 310, BETHESDA, MD 20814



Fidelis XPS™ Tech Talk: Preventing Cyber Attacks with Real-Time Threat Intelligence

Fidelis Security Systems
Will Irace, Senior Solutions Architect

June 2010
Version 1.0

Contents

Introduction	3
Fidelis XPS Feed Manager.....	4
Fidelis XPS Policy: A Primer.....	5
Reputational Feeds and the Information Flow Map	5
Alerting on Malicious Traffic	6
Conclusion	8

Figures

Figure 1—New "Reputation" location fingerprint.....	4
Figure 2—Information Flow Map: A Suspicious Node.....	6
Figure 3—Reputational Details From Fidelis XPS and Cyveillance.	7
Figure 4—Decoding Path and Single-Click Payload Extraction.	8

FIDELIS SECURITY SYSTEMS, FIDELIS EXTRUSION PREVENTION SYSTEM, FIDELIS XPS, the FIDELIS SECURITY SYSTEMS logo, and/or other FIDELIS SECURITY SYSTEMS products referenced herein are trademarks of Fidelis Security Systems, Inc. Copying, use or distribution of any material contained herein is expressly prohibited. Copyright © 2010 Fidelis Security Systems, Inc. All rights reserved.

Introduction

Fidelis XPS™ is an incredible network security platform. The patented Deep Session Inspection™ engine in our solutions gives our customers unprecedented wire-speed network visibility into content and application activity, coupled with real-time control over how information is exchanged on today's complex and interconnected networks. The Fidelis XPS Information Flow Map™ feature, another Fidelis innovation, has given our customers even deeper awareness of network traffic, in the form of a real-time display that provides an intuitive, content-aware view of all activity. Fidelis XPS CommandPost™, our policy configuration and sensor management environment, enables user-friendly, customizable analysis of alerts and events, not to mention an incredibly powerful and flexible policy system that connects the power of the Deep Session Inspection platform with actual business policies, objectives and requirements. In addition to our ability to solve data leakage prevention (DLP) problems for our customers, our unique set of technologies are uniquely suited to managing the cyber security risks posed by today's most advanced, dedicated and well-resourced adversaries by working at the session, protocol and payload levels targeted by the newest threats.

But most of our customers don't have a crack team of malware researchers and threat analysts to maintain awareness of all the very latest threats, and as a matter of fact we don't either. So we've built an innovative new feed management system that can improve situational awareness by automatically importing and updating reputational data from any number of free or subscription-based sources. To demonstrate the value of this exciting new feature we have partnered with Cyveillance, an industry-leading provider of intelligence-led security solutions. Their advanced Internet monitoring platform and research organization constitute an unparalleled source of continuously updated reputational knowledge that evolves just as quickly as the threats.



Fidelis and Cyveillance are working together to bring additional value to our security-driven customers. It's an ideal partnership: Fidelis delivers network security appliances with the power to prevent content-based attacks from infecting critical networks or causing costly and embarrassing data breaches, and Cyveillance delivers the reputational intelligence required to stay on top of ever-evolving malware and phishing attacks. Taken together, the visibility and control from Fidelis XPS paired with continuously updated threat intelligence from Cyveillance delivers a degree of situational awareness and a standard of protection well beyond what traditional threat mitigation technologies can offer.

Fidelis XPS Feed Manager

Fidelis XPS network security appliances now include the Feed Manager feature, which arrives preconfigured with two of the most powerful threat intelligence feeds available anywhere: an anti-phishing feed and an anti-malware distribution feed, both powered by Cyveillance. These advanced data sources, continuously updated by Cyveillance and automatically kept up to date by Fidelis XPS, allow our customers to enforce network security policy by monitoring and controlling network access to sites known to Cyveillance to host phishing or malware threats. In addition, Fidelis XPS can be configured to use any number of additional threat intelligence feeds from sources either internal or external to enterprises. These customized feeds can be formatted as XML, CSV or as simple text files, and it's easy to adjust feed sources, refresh rates and access credentials from the CommandPost GUI. Once the right combination of free, paid and custom feeds has been configured, reputational feeds from Fidelis XPS can easily be incorporated into Fidelis XPS policy.

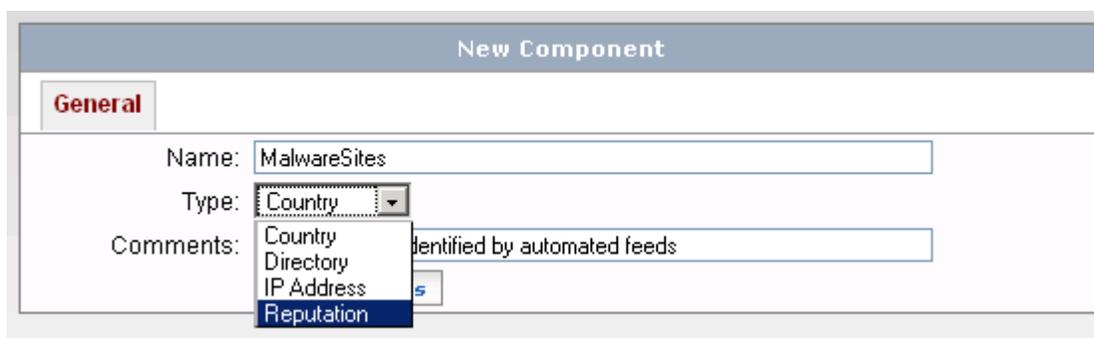


Figure 1—New "Reputation" location fingerprint.

The Fidelis XPS "location" fingerprint category has a new "Reputation" type alongside the previously available "Country," "Directory," and "IP Address" location types (see Figure 1). You can construct Reputation fingerprints that use any combination of the available feed categories ("Phishing," "Malware," and "Custom"), and then use these fingerprints in Fidelis XPS policy rules by themselves, or in combination with other fingerprints as part of more sophisticated rules.

The anti-malware distribution and anti-phishing feeds powered by Cyveillance and included with Fidelis XPS are available to all Fidelis customers for a free 90 day trial, after which they are available from Fidelis on a subscription basis.

Fidelis XPS Policy: A Primer

Fidelis XPS policy is constructed from building blocks we call “fingerprints.” These fingerprints come in three categories, focused on **content** (the message itself, after all the protocols, payloads, applications and archiving has been stripped away), **location** (the origin and destination of the message), and **channel** (any of thousands of attributes having to do with how the message has been transmitted). These fingerprints are assembled into rules as boolean expressions. A rule expression can be somewhat complex, like this:

```
C_Source AND From_Engineering_Dept AND NOT  
(To_QA_Testing AND FTP AND Normal_Business_Hours)
```

(In English: “prevent or alert on any traffic containing C source code if it’s transmitted from the engineering department, unless it’s destined for the QA lab via FTP during normal business hours.”)

Here’s a simpler favorite:

```
MS-DOS AND ImageFileNames
```

(In English: “prevent or alert on any traffic containing a DOS/Windows executable that’s been renamed to look like an image.” Remember, this rule doesn’t care if the renamed executable is buried in a dozen nested zip archives; Fidelis XPS will still spot this payload quickly enough to block the transfer, if prevention is specified.)

Dozens of different types of content, location and channel fingerprints are available, enabling the creation of a content protection and network security policy that’s as simple or as complex as business requirements dictate.

Reputational Feeds and the Information Flow Map

While it may be tempting to start by constructing a comprehensive set of Fidelis XPS rules leveraging the new threat intelligence feeds, it isn’t necessary to take this step to get immediate value from those feeds. The Fidelis XPS Information Flow Map feature will automatically display malicious hosts in red, drawing instant attention to internal nodes talking to hostile hosts and enabling a rapid, targeted threat mitigation response (see Figure 2).

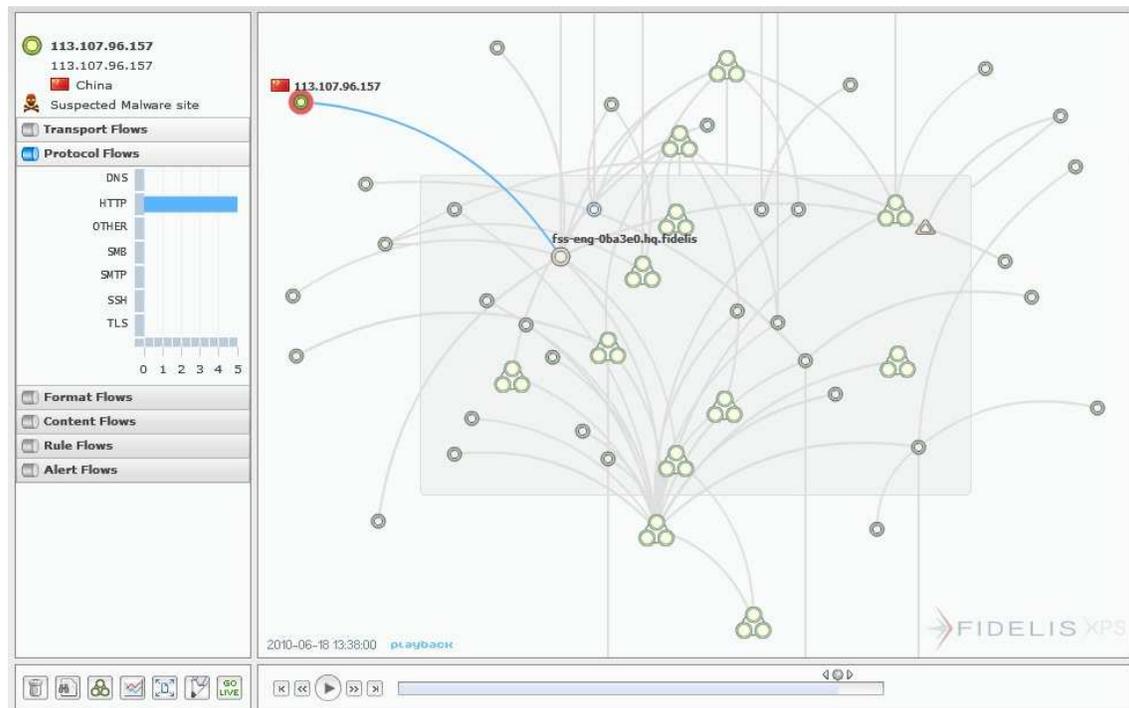


Figure 2—Fidelis XPS Information Flow Map: A Suspicious Node.

Alerting on Malicious Traffic

When threat intelligence feeds are used in Fidelis XPS rules, the resulting alerts tell the whole story of suspicious sessions. Fidelis XPS reports on exactly what was transmitted, what protocol was involved, the format and contents of the payload—and we can see at a glance why the destination host was suspicious in the first place (see Figure 3).



Learn more about using Fidelis XPS to kill content-based malware:
<http://goo.gl/AvSP>

Policy: Unauthorized Traffic (UT) < find similar
 Rule: UT, Malicious Site < find similar
 Summary: HTTP: 172.17.1.58 -> 217.16.1.24 < find similar

tum highlighting off

Matched On: **PhishingSites** highlighting on true

Type	Source	Name	Value
phishing cyveillance	url		http://mabiteetmoncouteau.com/privé/index.php
phishing cyveillance	url		http://pnc.mabiteetmoncouteau.com/
phishing cyveillance	url		http://pnc.joompad.be/
phishing cyveillance	host		mabiteetmoncouteau.com
phishing cyveillance	host		pnc.mabiteetmoncouteau.com
phishing cyveillance	host		pnc.joompad.be
phishing cyveillance	title	Welcome to Punjab National Bank Internet Banking Services	
phishing cyveillance	title	Personal Banking - PNC Bank	
phishing cyveillance	domain		mabiteetmoncouteau.com
phishing cyveillance	domain		joompad.be
phishing cyveillance	target		Punjab National Bank
phishing cyveillance	target		Other
phishing cyveillance	target		PNC
phishing cyveillance	ip_address		217.16.1.24

Figure 3—Reputational Details From Fidelis XPS and Cyveillance.

Another analysis feature our customers love is the decoding path display and our single-click payload extraction capability. Alert detail views include extensive information about all the work the Deep Session Inspection engine did to uncover each threat. If, for example, an FTP session is used to transmit a ZIP archive containing a renamed RAR archive containing a malware-infected PDF, Fidelis XPS CommandPost presents this information in the form of a decoding path (which itself can be made part of policy). Better still, each level in the decoding path includes a clickable link for downloading the payload as it existed at every step along the decoding process (see Figure 4). And as if that isn't enough, CommandPost permits network session downloading of both sides of any conversations that violate policy, enabling a detailed and comprehensive forensic response.



Figure 4—Decoding Path and Single-Click Payload Extraction.

Conclusion

The word for 2010 is “proliferation.”

Threats are proliferating: enterprises face internal accidental misuse, unknown internal threats and an increasingly sophisticated and talented set of external adversaries. Network communication modes are proliferating: it’s not always sensible to institute blanket bans against social networking sites, instant messaging or even peer-to-peer channels. Finally, threat mitigation technologies are proliferating: the days when a socket-based firewall was enough are long gone, and security vendors have saturated the market with an alphabet soup of “solutions” that add unwanted complexity. Find out what our most demanding customers already know about Fidelis XPS: the incredible Deep Session Inspection platform, blended with our Information Flow Map, flexible policy engine and intelligence-led reputational data from Cyveillance, provide unsurpassed leverage you can use to achieve and enhance situational awareness and decisively answer today’s advanced online threats.

“Fidelis gives us big bang for the buck from the pure security compliance perspective. Best tool that we can use to give us situational awareness.”

– US Energy Company

Call us today at 800.652.4020 to schedule a closer look.