Combating Cybercrimes with Defense in depth approach - SAFE method

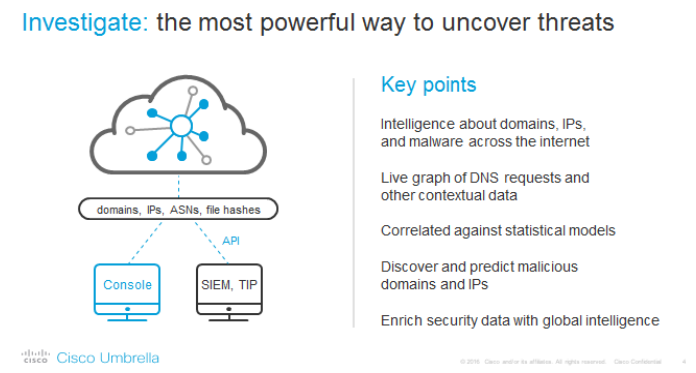
Ransomware worms and creative phishing attacks are taking news headlines by storm. Organized Cybercrimes are increasing in its sophistication but there is no 'silver bullet' to protect data, people and infrastructure. Traditional point products confining to network perimeters are not sufficient in protecting today's digital business models from evolving threat vectors. A modular and layered security defense method with an integrated architecture is key in combating cybercrimes and to protect business networks. SAFE method provides a framework and best practice guidelines to defend against threats using simple concepts.

http://cs.co/90028cJvK

Table 1 *The SAFE Method*

Category/Phase	Example Icon	Description	Function
Key		Organizational Model	The Key documents threats, risks, and policies throughout an organization.
Threat		Unauthorized Packets This threat is blocked by firewalls.	The top security threats of an organization are catalogued.
Capability		Firewall	Capabilities are used to describe security functions.
Architecture		Firewall Capability on a Logical Router	Architectures are used to logically arrange the security capabilities.
Design	G0: G1: 4451-x	4451x with Firewall	Designs are used to provide specific products and services.

Cisco Umbrella Investigate



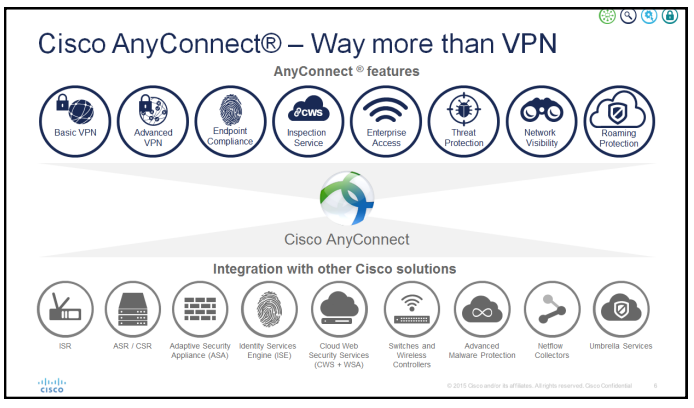
Gaining the most complete view of threat has direct implication on how efficient and faster your incident response triage activities are. But it's not easy when the observables and pieces of information are spread across IPs, domains, URLs, hashes, etc. Cisco Umbrella Investigate gives the most complete view of the relationships and evolution of internet domains, IPs, and malware helping to pinpoint attackers' infrastructures and predict future threats. Many cyber criminals reuse tactics and techniques that produce the same observables and therefore create a pattern that can be used to detect and prevent future attacks by threat actors.

http://cs.co/90098cJN5

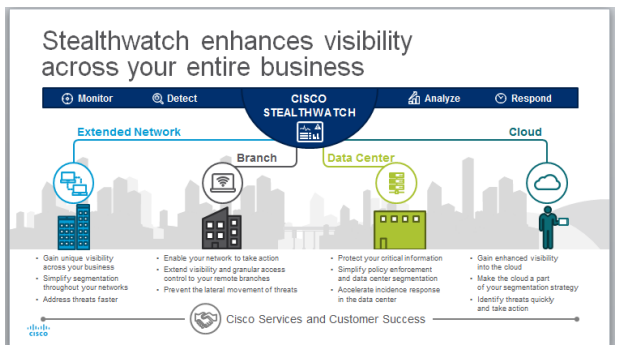
AnyConnect Network Visibility Module

One of challenges in IT administration is getting endpoint context data especially in the event of security incident. One other challenge IT admins face could be identifying user devices running legacy Operating Systems. Cisco's premier secure mobility client, AnyConnect is expanding its endpoint security capabilities with Network Visibility Module (NVM). NVM collects context-enriched flows from an endpoint whether it is on or off premise. This rich flow context includes user, device, location, application and destination. NVM coupled with a Cisco solution such as Stealthwatch or a 3rd party solution such as Splunk allows customers to gain critical visibility into network connected devices and user behaviors .

http://cs.co/90008cKOI



Cisco Stealthwatch



How to do you contain a malware infection that lands and expands its footprint in the East West direction in your network? Recent WannaCry Ransomware is a good example of a Malware which behaved this way looking to infect other hosts within the same subnet over SMB 445/TCP and also use the Tor network to communicate. Cisco Stealthwatch's NetFlow based visibility and intelligence analysis into east-to-west traffic will allow the solution to prevent widespread infection in an organization laterally.

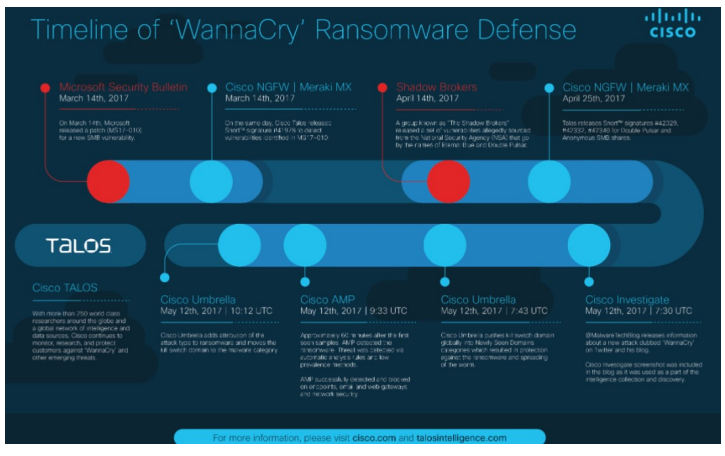
http://cs.co/90048cKWE

Threat Spotlight: Cisco Coverage for Adylkuzz, Uiwix, and EternalRocks

When the WannaCry attack was launched, it was one of the first large scale attacks leveraging the data that was leaked by the Shadow Brokers. Over the past couple of weeks, Talos has observed other malware variants that are using the ETERNALBLUE and DOUBLEPULSAR exploits from the Shadow Brokers release as part of their campaigns. Among them were Adylkuzz, Uiwix, and EternalRocks.
When mitigating risks, it is important to remember that the best way to prevent attacks exploiting CVE-2017-0143 to CVE-2017-148 as described in the Microsoft Security Bulletin MS17-010 is to apply the security update as soon as it is possible for your organization. These attacks are exploiting vulnerabilities that have been known for at least two months and, depending on the exploit, have been covered by NGIPS and NGFW technologies dating back to mid-March 2017.
Snort Rule: 42329-42332, 42340, 41978, 422

http://cs.co/90048czJe

Join Webinar— May 31: Anatomy of the attacks– WannaCry Ransomware & Google OAuth phishing- Register Now



http://cs.co/90028czky

For more information on Cisco Security solutions and products, please contact your **Cisco Account Manager**

Suggestions/comments on this newsletter contact Joby James at joby@cisco.com