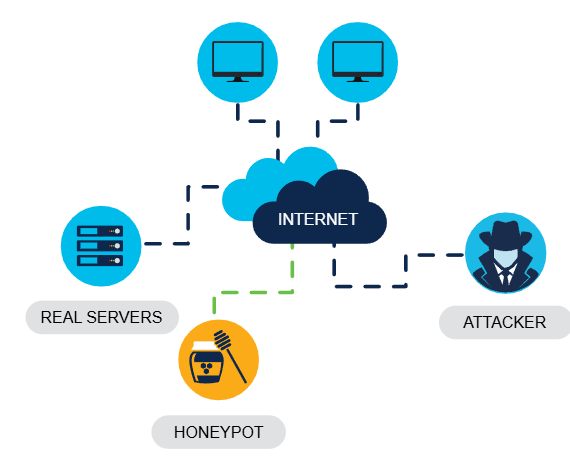
Behavior approach to cybersecurity

Behavior-based security

- it’s a form of threat detection that involves capturing and analyzing the flow of   
 communication between a user on the local network and a local or remote destination.

Any change in normal patterns of behavior are regarded as anomalies, and may indicate an   
 attack

= honeypods  
 **it’s a behavior-based detection tool that lures the attacker in by appealing to their   
 predicted pattern of malicious behavior.** Once the attacker is inside the honeypot, the network administrator can capture, log and   
 analyze their behavior so that they can build a better defence  
 

= ciscos cyber threat defense solution architecture

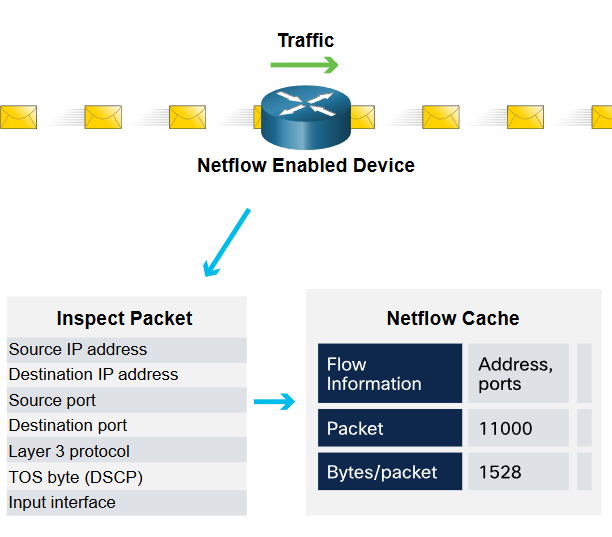
This security architecture used behavior-based detection and indicators to provide greater   
 visibility, context and control.

The aim is to know who is carrying the attack, what type if attack they are performing and   
 where, when and how the attack is taking place

NetFlow

Netflow technology **is used to gather information about data flowing through a network**, **including who and what devices are in the network, and when and how users and devices access the network**

It’s an **important component in behavior-based detection and analysis**. Switches, routers and firewalls equipped with netflow can   
 *report information about data entering, leaving and traveling through the network the information is sent to netflow collectors there they are analyzed*



Penetrating testing

Commonly known as **pen testing**

Is the **act of assessing a computer system, network or organization for security   
 vulnerabilities**

**A pen test seeks to breach systems, people, processes and code to uncover vulnerabilities which could be exploited. This info is then used to improve the systems defenses to ensure that it is better able to withstand cyber attacks in the future**

All the steps:

PLANNING

**The pen tester gathers as much information as possible about a target system or   
 network, its potential vulnerabilities and exploits to use againts it**

**This invilves conducting passive or active reconnaissance and vulnerability   
 research**

SCANNING

Pen tester carries out **active reconnaissance to probe a target system or network   
 and identify potential weaknesses which, if exploited could give an attacker access** may include:

- Port scanning to identify potential access points into a target system  
 - vulnerability scanning to identify potential exploitable vulnerabilities

- establishing an active connection to a target to identify the user account,   
 system account and admin account

GAINING ACCESS

**The pen tester will attempt to gain access to a target system and sniff network   
 traffic, using various methods to exploit the system** including:  
 - launching an exploit with a payload onto the system  
 - breaching physical barriers to assets  
 - social engineering

- exploiting website vulnerabilities

- exploiting software and hardware vulnerabilities or misconfigurations

- breaching access controls security

- cracking weak encrypted Wi-Fi

MAINTAINING ACCESS

The **pen tester will maintain access to the target to find out what data and   
 systems are vulnerable to exploitation it is important that they remain undetected**,   
 typically using backdoors, trojan horses, rootkits and other covert channels to hide   
 their presence

ANALYSIS AND REPORTING

**The pen tester will provide feedback via a report that recommends updates to   
 products, policies and training to improve an organizations security**

Impact reduction

COMMUNICATE THE ISSUE

- **Communication creates transparency, witch is critical in this type if situation**

- **Internally**, all employees should be informed and a clear call to action   
 communicated  
 - **externally** all clients should be informed through direct communication

BE SINCERE AND ACCOUNTABLE

- **respond to the breach in an honest and genuine way, taking responsibility where   
 the organization is at fault**

PROVIDE THE DETAIL

- **be open and explain why the breach took place and what information was   
 compromised**. Organizations are generally expected to take care of any client costs   
 associated with identity theft services required

FIND THE CAUSE

- **take steps to understand what caused and facilitated the breach**. This may   
 Involve hiring experts to research and find out the details

APPLY LESSONS LEARNED

- **make sure that any lessons learned from forensic investigations are applied to   
 prevent similar breaches from happening in the future**

CHECK, AND CHECK AGAIN

- **attackers will often attempt to leave a backdoor to facilitate future breaches. To   
 prevent this from happening, make sure that all systems are clean, no backdoors   
 are installed and nothing else has been compromised**

EDUCATE!

- **raise awareness , train and educate employees, partners and clients on how to   
 prevent future breaches**

What is risk management?

**Its the formal process of continuously identifying and assessing risk in an effort to reduce the impact of threats and vulnerabilities.**   
You cannot eliminate risk completely but you can determine acceptable levels by weighing up the impact of a threat with the cost of implementing controls to mitigate it. **The cost of a control should never be more than the value of the asset you are protecting**

Frame the risk

**Identify the threats that increase risk**  
 They may include processes, products, attacks, potential failure or disruption of services,   
 negative perception of an organizan. reputation, legal liability or loss of intellectual property

Assess the risk

**Determine the severity that each threat poses**  
 examle: threats potential to bring an entire organization to a standstill. While others may be   
 only minor inconveniences.  
 **It can be prioritized by assessing financial impact**

Respond to the risk

**Develop an action plan to reduce overall organization risk exposure, detailing where risk   
 can be eliminated, mitigated, transferred or accepted**

Monitor the risk

**Continuously review any risk reduced through elimination, mitigation or transfer actions**

Remember, not all risks can be eliminated so you will need to closely monitor any threats   
 that have been accepted