CounterACT to enforce IoT Best Practices

Dr. Götz Güttich

ForeScout CounterACT is a security solution for business networks that identifies and evaluates components as soon as they connect to the network. This product is therefore not only suitable for securing "classical" environments, but also for protecting communication with "Internet of Things" devices. In our testing laboratory, we took a close look at CounterACT's abilities in this context.

Deployment of IoT devices in organizations is a fact of live. Today, IoT devices are getting more exposed and more commonly used as gateways to get unauthorized network access.

To secure their network, while deploying IoT devices, companies need visibility, segmentation, classification and detection of all endpoints in their networks. Visibility on what is connected to the network – no matter if corporate managed devices, personal devices and IoT devices.

Through dynamic network segmentation companies are able to limit the impact and/or to remediate security breaches. Classification allows the identification malicious behavior of any endpoint. Suspicious behavior originating from unmanaged IoT devices is also detected.

IAIT tested three common IoT Security Threat scenario's. In all three cases ForeScout's CounterACT successfully identified and blocked the attack. ForeScout's CounterACT is not only well suited for protecting corporate networks against threats posed by hijacked PCs and servers, but also to an excellent tool to defend against attacks that run via IoT components.

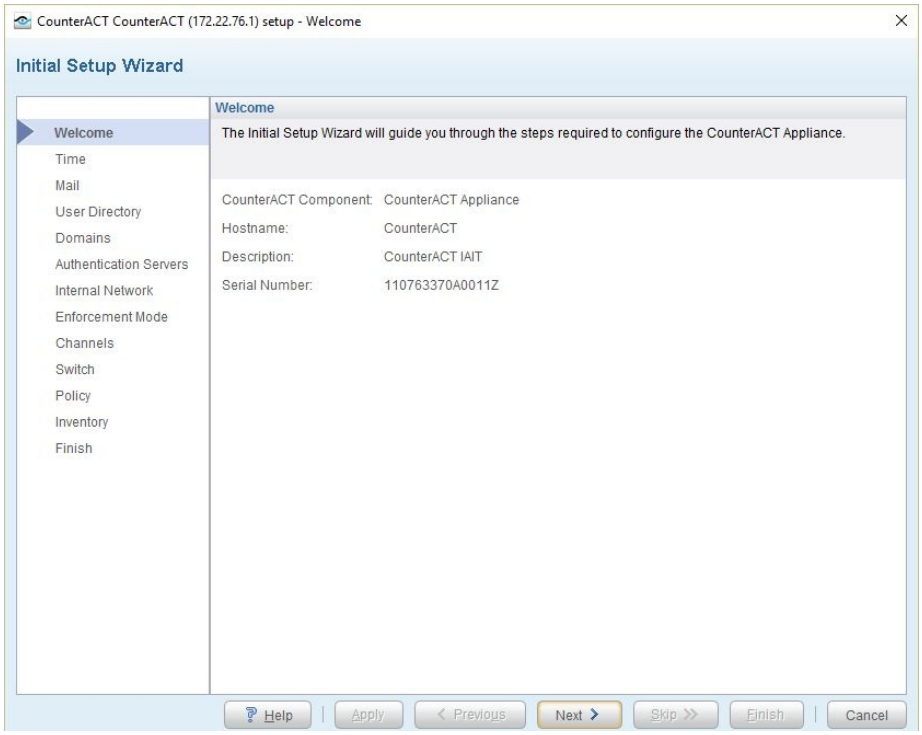
Architecture

For a large percentage of its functionality, ForeScout CounterACT works without agents on the administrated devices. That's why it can secure communications not only with known components, but also with unknown devices. Furthermore, it doesn't matter whether the products that need protection are administrated or not, nor does it matter whether the systems are stationary, mobile, physical, virtual or embedded.

In ongoing operation, CounterACT determines diverse key data for the newly added devices. These data include, for example, users, operating system, device configuration, existing software, patch status, running services, and the status of the security software. Afterwards, based on the acquired data and predefined policies, CounterACT classifies the various devices and, if necessary, takes measures to protect the network. For example, if desired, the administrators can configure the solution so that only components with up-to-date virus-scanner signatures are permitted to enter the network.

CounterACT also monitors all systems currently in operation. Rogue components that were active without the knowledge of the IT department are now a thing of the past, as are so-called "blind spots," which were formerly opaque to the company's IT staff. The majority of the work runs automatically, so this product saves time by enabling administrators to secure their networks

much more quickly. To protect the company's IT resources from endpoints that are deemed risky, ForeScout's solution also offers a quarantine in which a client can, for example, update its antivirus pattern or import necessary patches before granting them access to the LAN. Furthermore, CounterACT is also able to influence the configuration of switches and, for example, close ports through which suspicious activities occur.



The Initial Setup Wizard starts on the CounterACT appliance after the first login.

CounterACT is available as both a virtual solution and in the form of an appliance. The appliances come in several different hardware versions and can protect networks with up to a million endpoints. The product works with a variety of switches, routers, VPNs, WLAN components, firewalls, patch management systems, antivirus solutions, directories, and trouble-ticket systems. When implementing CounterACT in an existing network, the administrators only need to ensure that the security solution is given access to the network's traffic; no changes in the infrastructure are necessary.

Thanks to the abovementioned functionalities, CounterACT secures the company's network against devices of customers, visitors and employees (BYOD) that are not administrated by the company's IT department, and also protects against malware, botnets and Internet-of-Things (IOT) devices. As such, CounterACT helps ensure compliance and protect networks against both external attacks and threats from within the company.

Mode of functioning

In operation, ForeScout's solution works out of band in the network. For example, it can connect to a mirror port, where it analyses the data communication. In this context, CounterACT immediately detects new devices as they enter the network and can even identify components without IP addresses because CounterACT also scrutinizes traffic that's handled only via MAC addresses. Afterwards, CounterACT collects the abovementioned data and applies predefined rules which specify how to proceed with the individual devices.

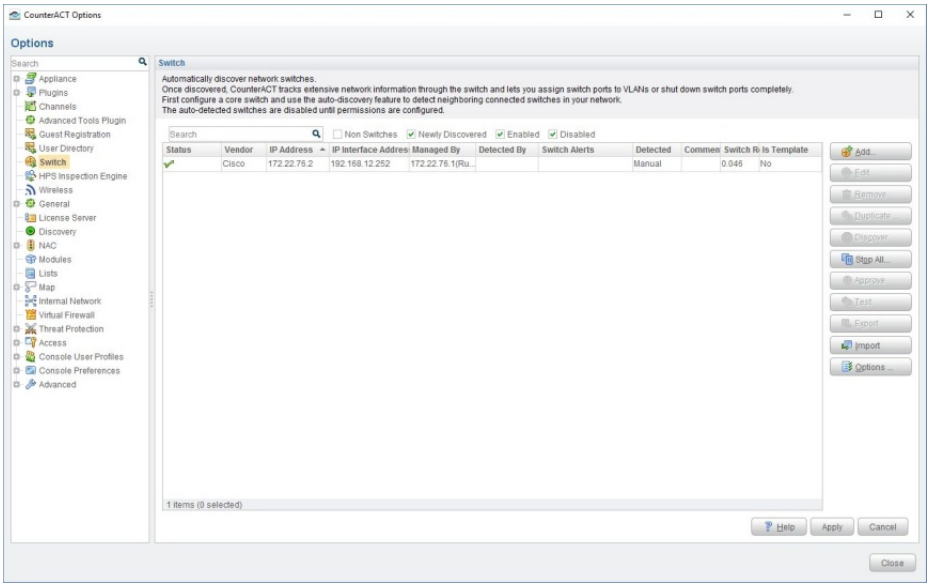
For example, relying on predefined credentials, the product will attempt to log in to a Windows computer. If it succeeds, it classifies the computer as a device that's administrated by the IT department and assigns it more comprehensive access rights than would be granted to the notebook of a guest who cannot log in and who is therefore only permitted access to the Internet. If active measures are necessary (for example, because a component is deemed risky), then CounterACT is able to send data via a so-called "response port" into the network in order to sever connection between the potentially risky device and LAN devices (by blocking a switch port or relocating an attacker into quarantined VLAN). Warnings can also be transmitted into the network in this same way.

IoT as a threat

IoT devices are becoming increasingly commonplace and are therefore causing security problems which should not be underestimated. After an IoT device (an IP telephone or a camera, for example) has connected to the network, the device is not merely able to transmit data into the network and receive data from the network: it can also become a gateway for hackers. Hacked devices are operable via the network; their IP stacks are seldom hardened and their potential se-

curity vulnerabilities can be exploited in the same way as classical IT components can be misused. Insufficient encryption and weak authentification schemata also play roles in this context.

Similar to the situation with various mobile devices, there is an even greater threat potential for IoT components than for "normal" computers because there is absolutely no assurance that the manufacturers of the IoT devices have identified potential security problems in their products or intend to speedily remedy those vulnerabilities. IoT devices are therefore a latent threat which should always be taken into consideration because hackers can use them to access data in the network.



CounterACT after successful configuration of access to our Cisco switch.

The test

In our test, we implemented CounterACT in our network environment and configured the product so that it classified our components, secured them, and monitored their ongoing operation. Afterwards, we generated various policies that we used to secure our network against typical attack scenarios via IoT devices. Finally, we checked the effectiveness of these rules.

Putting into operation

To put the CounterACT appliance into operation, we began by connecting the solution to a monitor and a keyboard, which we then booted up. After the system startup, the product asked us about the keyboard layout and offered us three configuration options. The first option called itself "Standard": this is the configuration as a stand-alone appliance and it is the one that we used in our test.

Alternatively, in a highly accessible environment, the solution can also be set up as a "Primary" or "Secondary Node." In the next step, the administrators can choose between implementing CounterACT as an appliance or as an enterprise manager. In the enterprise-manager mode, the product is also able to coordinate other CounterACT appliances in larger environments. But this mode played no role in our test because we had only one appliance at our disposal.

Now our tasks were to specify the administrator's password, the host's name, and the network interface for management accesses. Our appliance was equipped with four network interfaces. We defined the first of them as the access for the administrators. In the final step, we also specified network configuration for the management interface with IP address, gateway, network mask and similar items; afterwards, the setup was accepted and the appliance became accessible via the network.

As soon as the initial configuration was completed, we connected the appliance's fourth port (which would be assigned the task of functioning as the monitoring port during operation) to a mirror port of our Cisco LAN switch so it would be able to view the traffic in our network. We then connected the third port (which would work as the response port) via a normal network connection on the same switch.

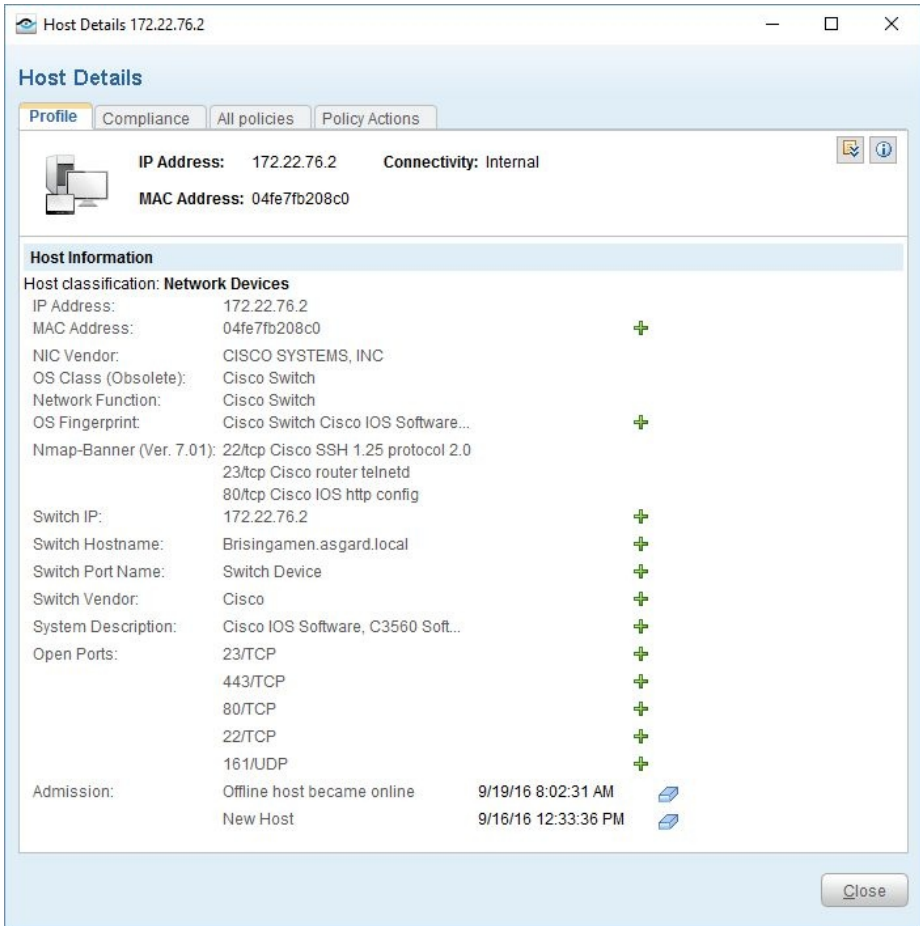
This completed the hardware configuration and we could afterwards begin finishing the installation of the CounterACT system. In operation, the solution is configured via the "CounterACT Console", which is available as management workstations under Linux and Windows. We installed it on a computer with Windows 10 Version 1607 in the 64-bit variant. This system was equipped with a Quad-Core processor, eight gigabyte RAM and 200 gigabyte available hard disc space.

As is usual under Windows, Wizard coordinates the installation of the console. The administrator will not encounter any difficulties. After the first login with the

console on the appliance, we started the “Initial Setup” assistant. This begins by showing a welcome screen and then wants to know the time zone, the time of day, and which NTP server should be used (if there is one). Afterwards, the responsible employees can specify the administrator email with mail relay, the directory that should be used for user authentification (Microsoft Active Directory, LDAP, Novell eDirectory, Sun Directory Server or IBM Lotus Notes), and the domain credentials that the appliance uses in operation in order to log in at the host and to perform a deep inspection on the host.

The next configuration dialogue focuses on the authentification servers. We had already specified our active directory controller, so this was already in the list; but, if necessary, the administrators now have the opportunity to enter additional data.

Afterwards, the Wizard asked about the IP areas that the appliance should regard as the internal network. The Wizard also wanted to know the enforcement mode. The options here are: “Full Enforcement” with NAT detection; “Auto Discovery”, in which the product continually monitors to determine if new components have come into the network; and “Partial Enforcement” without threat protection, HTTP actions and virtual firewall. With the virtual firewall, the solution is able to use a kind of “man in the middle” attack to prohibit data transfers and thus remove endpoints from the traffic.



In operation, ForeScout’s solution collects many details about the network’s components.

Under “Channels”, the responsible employees specify which ports should be used for which tasks (monitoring, response, etc.). The “Switch” area specifies access data for Alcatel, Cisco, Brocade, Huawei, Palo Alto Networks, and many other switches through which the appliance can then alter the switch configurations (if necessary), for example, to reconfigure ports.

In the “Policy” point, the responsible individuals specify the rules which will be implemented to classify network components, ensure their security (for example, by monitoring the update status of the antivirus pattern), and monitor the components in their ongoing operation. In our test, we postponed the policy definition for a later date and initially specified an empty set of rules.

Finally, the “Inventory” area offers the responsible employees a non-host-related network overview. This overview can show, for example, open ports in the network or Windows services that are running in the network. With this final item, the configuration Wizard closes itself and, after a restart, the appliance begins its work.

Configuration in ongoing operation

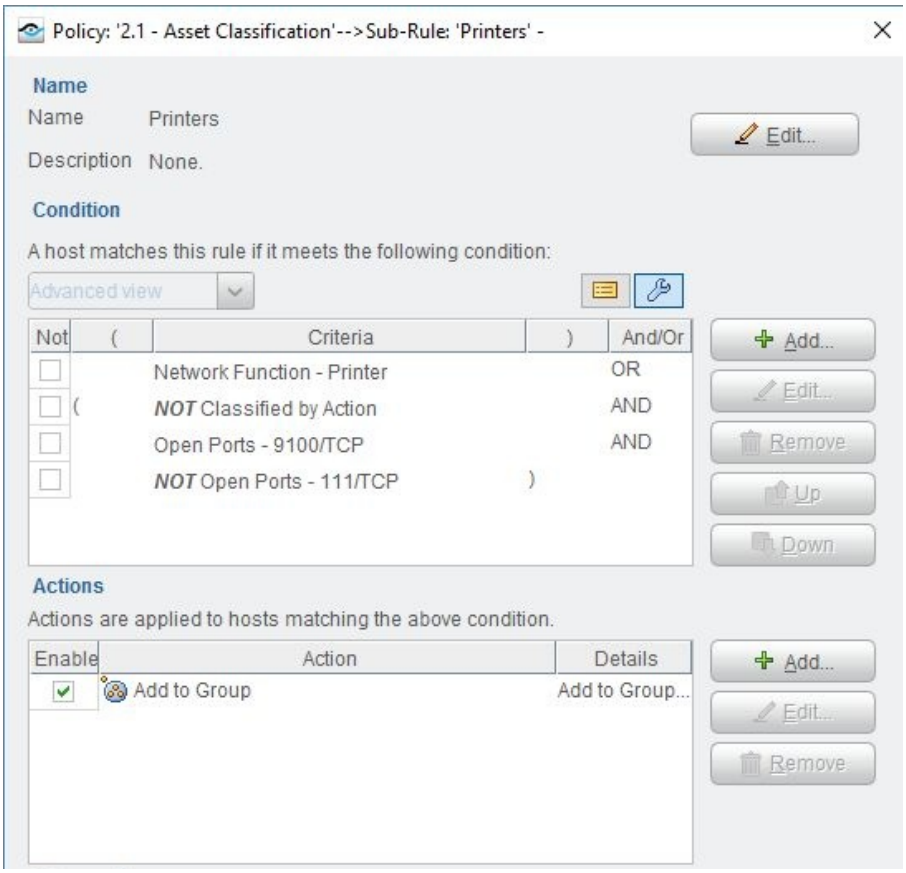
Now let’s look at a few practical examples to show how CounterACT can be used to secure company networks against threats posed by IoT devices. The first example takes effect in the aforementioned scenarios in which IoT components are hacked and then misused as gateways into the network to steal data. The second example shows how admi-

nistrators can secure specific classes of devices against misuse; printers are used as an example in this instance. The third example explores how the appliance detects port scans in the network and defends against them. Attackers usually conduct port scans after they have gained a foothold on a device. Such scans enable attackers to determine which services are available.

Example number 1: detecting and securing hacked IoT devices

If an attacker takes over a device (for example, a smart TV in a conference room or a webcam), they can change the MAC address of this device so that it will pretend to be another product. Many companies work with security solutions that are based on access control lists (ACLs). These lists classify the devices in the network: for example, they specify that the computer with the MAC address FC:FC:48:23:b0:c4 is a Windows client and that the device with the MAC address D8:1F:CC:28:d1:00 is a smart TV.

Based on this classification, many corporate security solutions now permit access to specific components, so it be sensible to grant the access rights for certain file servers to Mac OS or Windows computers and simultaneously to ensure that IP cameras and smart TVs are not granted access to these servers. In many instances, it accordingly suffices merely to change the MAC address of a hacked IoT device to thwart the security products and to gain access to the data. Conversely, in many environments, it can try to disguise itself as another operating system: for example, if a Linux-based webcam pretends to be a Windows system, this alone may often suffice to receive higher-level rights.



If necessary, in the context of classification, administrators can precisely specify which ports on a system are allowed or not allowed to remain open. Based on these data, they are then assigned to their appropriate groups.

To ensure security in such a scenario, administrators must first generate a CounterACT rule that assigns the existing devices to particular groups, for example,network devices (routers and switches), Linux servers, Windows PCs, Mac OS systems, printers, VoIP solutions, etc. As described above, this functions automatically in the context of the network scan based on the data acquired during the scan. For example, if an administrator wants to assign all of his company's IP cameras to the group of "IP cameras" and if all existing cameras are either Axis, D-Link or Mobotix, then the responsible employee can use the CounterACT console to specify a policy that reassigns into the "IP cameras" group all devices that have MAC addresses which belong to the aforementioned manufacturers.

But this does not yet make it clear where the camera comes from: it could also be a rogue device which accidentally (or intentionally) comes from one of the aforementioned manufacturers, just like one of the company's ordinary cameras. That's why it makes sense to expand the group of "IP cameras" to include two subgroups. The first subgroup, which is named "Corporate IP Cameras", should contain all of the company's cameras. The second subgroup is logically named "Non-Corporate Devices" and includes all cameras which the

appliance doesn't already know. This distinction can be made via a MAC address list: if the responsible employees enter all IP addresses of IP cameras throughout their company into the policy definition, then CounterACT can securely distinguish between foreign cameras and cameras which belong to the company.

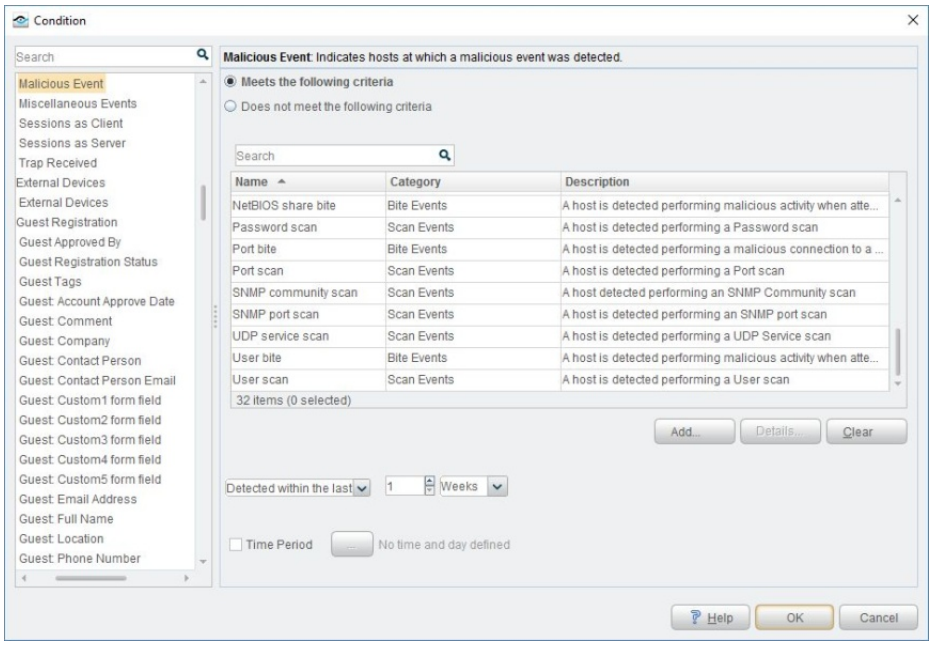
During the scan, CounterACT not only determines the MAC addresses of the devices in the network, but also (as discussed) discovers other parameters such as IP addresses, open ports or the operating system. This security solution is accordingly able to recognize a device, even if a parameter (for example, MAC address or the operating system used) has been altered.

If a webcam is hacked and the attacker uses MAC address spoofing to disguise the webcam under the MAC address of a known Windows client and thus thwart the ACLs, then CounterACT detects the fact that the device is now active in the network under an altered MAC address. This address is not in the list of known MAC addresses of IP cameras, so, in the next step, the suspicious device is assigned to the group of "Non-Corporate Devices".

The attacker has thus been identified, but now it must be made harmless. This is why the people responsible for IT augment the policy with an action which assures that no data theft ensues. Several different options are available here. For example, all devices in the group of "Non-Corporate Devices" can be placed in a quarantined VLAN where they can cause no harm.

Alternatively, CounterACT can also be set up to automatically block the switch port on which the affected device depends. The security solution accesses the switch configuration for this option. Simultaneously, the product can send alarms to the administrators and can also initiate many other actions. In this way, it becomes relatively simple for a company to prevent data theft through IoT devices via MAC address spoofing. In our test, we used a Linux client under Fedora 24 to simulate MAC spoofing: CounterACT immediately detected our manipulation.

Incidentally: if an attacker disguises itself as another operating system (in our example, as a Windows client), then another set of rules comes into play. This is because in our scenario, we began by classifying the Windows devices. The distinction between "Windows" or "not Windows" was made prior to its assignment to the group of "IP cameras". The hacked device, which disguised itself as a Windows solution, was consequently not assigned to the group of IP cameras, but among the Windows systems. Various security rules can be specified for these: in our test, all Windows systems that CounterACT couldn't log into (that is, also our test computer with false operating-system identification) were quarantined so they could do no harm.

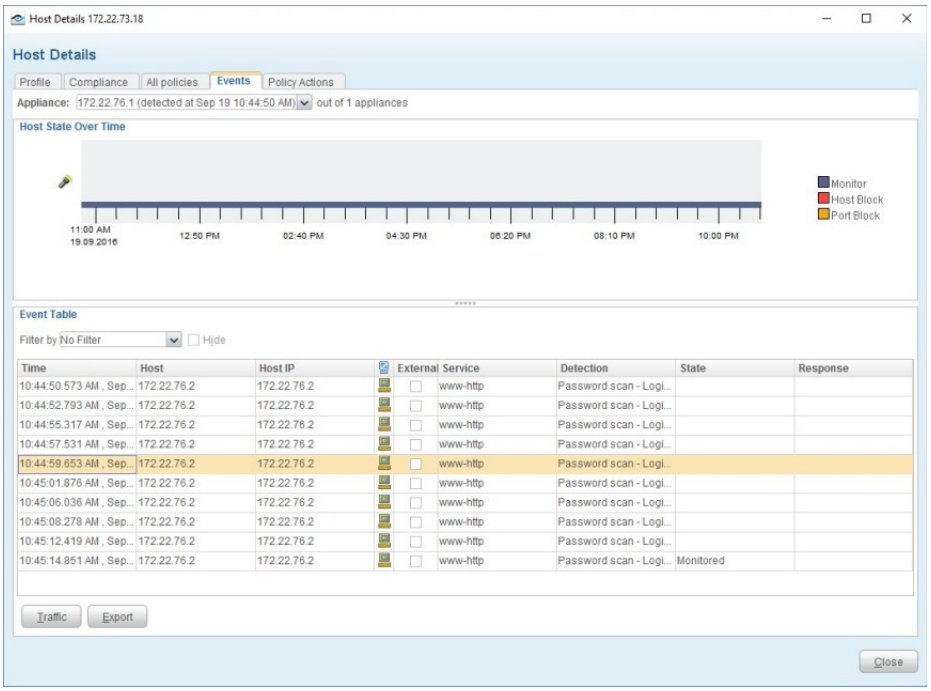


CounterACT detects a large number of different attack scenarios.

Example number 2: printer P2P clarification

Our second scenario assumes that an attacker has taken control of a printer and afterwards attempts via P2P to use this printer to move data off the company's premises. CounterACT likewise thwarts this attempt. The affected policy initially assigns the components in the network to specific groups. In our example, printers can be recognized because port 9100 for print orders is open and port 80 for the configuration interface is likewise open. If all of the printers in a company are made by the same manufacturer (for example, Xerox), then the NIC manufacturer can again be used for classification. If ne-

cessary, it is even possible to instruct CounterACT to call up the printer's web interface and check if it exports specific contents such as the identity of the contact person within the company. If all of the aforementioned factors are determined to apply, then the printer lands in the group of "Corporate Printers."

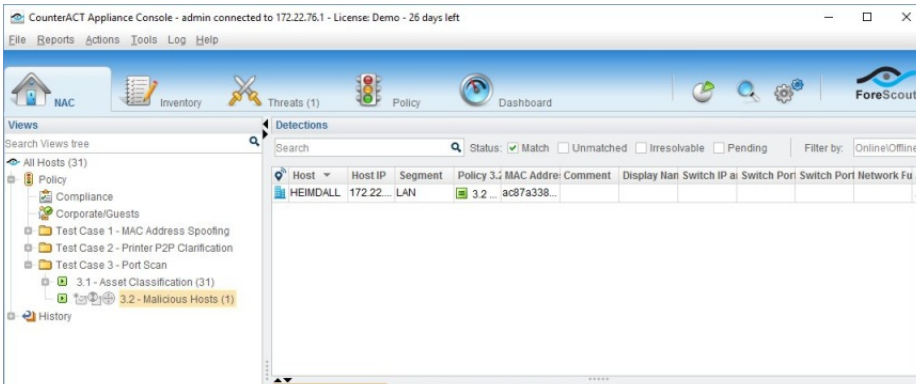


Detailed information about a previously run password scan.

If a hacker now sets up a P2P service on the computer, this usually causes additional ports to open. CounterACT detects these additional openings in ongoing operation and accordingly reassigns the printer to the group of "Non-Corporate Devices." Various actions can be defined here; the security appliance then undertakes these actions to prevent data theft.

Example number 3: defense against port scans

Our third example involves port scans. If a hacker penetrates into an unknown network, then his next step after he has taken over the first device will most likely be to run a port scan in the network. This will enable him to find out which services are offered by which machines. That's why it is important to speedily detect and isolate computers or other systems in the network that run port scans which haven't been authorized by the IT department – before these computers or other systems can be misused to attack network services. CounterACT can be used here too. To do so, the responsible individuals simply need to specify their security appliance to check whether any existing systems in the network are running port scans. Various other malicious events can also be detected, for example, hostname scans, NetBIOS name scans, password scans, SNMP community scans, and similar events. As soon as ForeScout's solution has noticed an activity of this kind, it can perform an action such as blocking the affected switch port or putting the affected system into quarantine. This isolates the attacker and protects the network from any further actions which the attacker might undertake. In our test, we conducted port scans under Windows systems and under Kali-Linux: CounterACT immediately detected our actions.



CounterACT identifies a system under Kali-Linux which has performed a port scan.

Summary

A security appliance such as ForeScout CounterACT is not only excellently well suited for protecting corporate networks against threats posed by hijacked PCs and servers, but can also defend against attacks that run via IoT components. CounterACT's range of functions is impressive, but configuring individual policies is comparatively uncomplicated because this product's manufacturer has conceived its configuration and management interface in a very comprehensible way. In our test, the rules for our three attack scenarios were speedily as well as easily implemented and caused no negative surprises in operation.