Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

The Cyber Security Remediation Bottleneck

By: Mark Cummings, Ph.D.

Cyber crime is one of the largest industries on the planet. We are getting better at detecting breaches. Fixing things, not so much. The bottleneck is remediation – stopping the attack and closing the hole the attacker came through. This is because remediation is a manual process. The only way to make things better is to automate remediation. In doing so, it is helpful to use the human immune system as a model for what is needed.

The improvement in detection has come through behavioral analysis. Behavioral analysis is an automated process. It observes system behavior and detects changes in behavior that indicate an attack. But, once a cyber intrusion/compromise has been detected, incident response falls back to manual processes. Problems with speed, reliability, and available skill sets make reliance on manual response problematic. What is needed is the automated ability to respond quickly. Quick and comprehensive — any part of an organization's combination of computers and communications systems under attack. Modeling this overlay combination of automated detection and remediation on the human immune system produces a cost-effective increase in cyber security.

Innovative software technologies have the capability to create such a cyber immune system. This system would need to combine centralized and distributed components, protecting all layers of technology. It would need to move with functions as they migrate from physical, to local virtual, to hybrid Clouds. It also would need to be able to deal with the dramatic increase in data volumes. Because of its importance, it needs to have high availability. For example, it cannot be shut down for maintenance every time a vendor updates one of the profusion of system components that exists in a large organization.

Cyber Crime Today

Losses in direct cash as well as brand value are large and increasing.

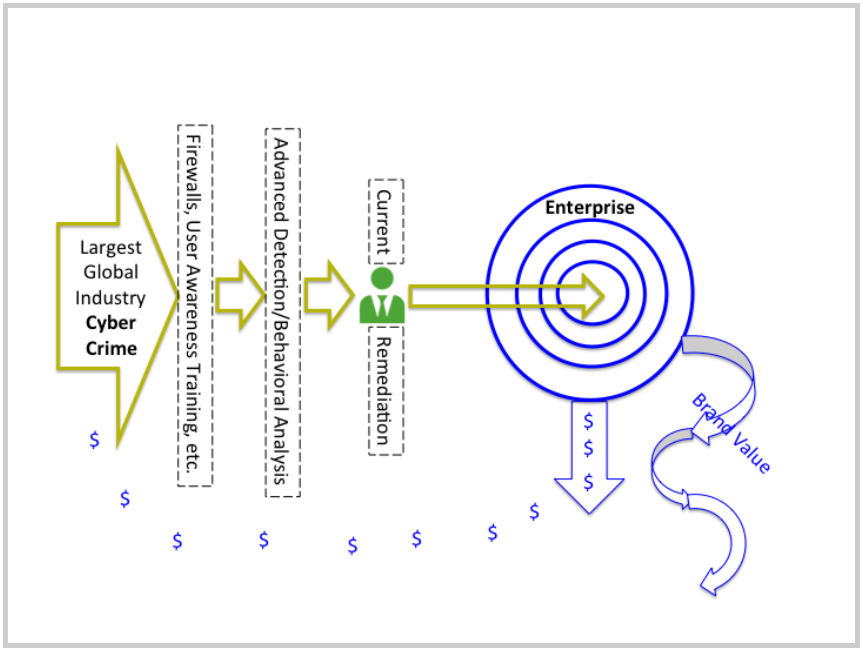

Figure. 1 - The current impact of cyber crime.

Firewalls, virus checkers, and user awareness training have put up an external barrier (a cyber outer skin) that stops 95 percent of the attacks. Unfortunately, there are too many attacks. IDT reports that a typical large enterprise experiences hundreds of cyber attacks per day. The 5 percent of attacks that get through that cyber outer skin cause tremendous losses. The direct cash losses are huge. The FBI estimated that in 2016 direct losses from cyber crime in the United States amounted to $9 billion. But, the brand value losses may be greater. Dyn Corp. lost one-third of its annual revenue within 10 days of its attack. Yahoo suffered more than a $1.2 billion loss in acquisition value as a result of its attack. Equifax, so far has lost one-third of its market capitalization value as a result of its attack.

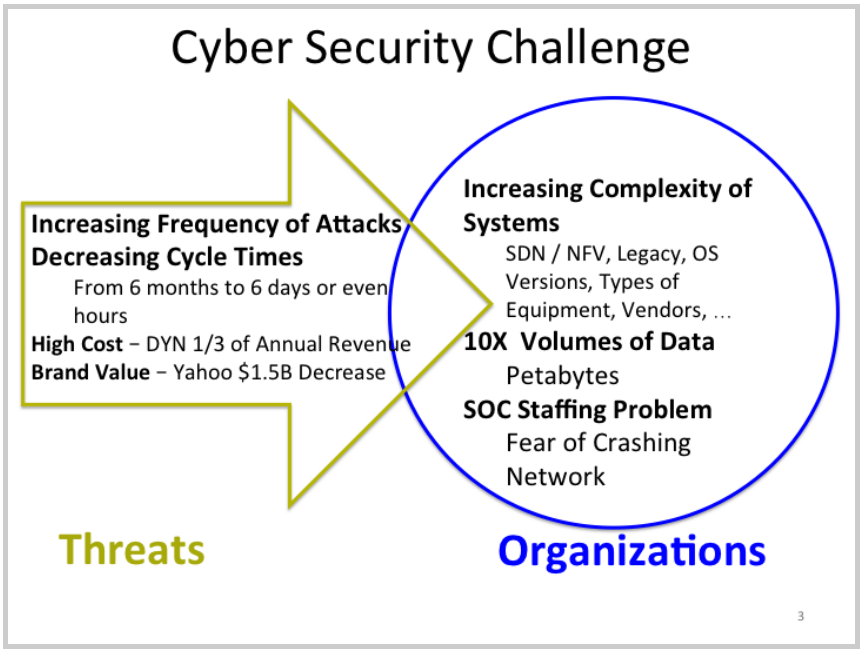

Figure 2 - The Cyber Security Challenge

Cyber crime is getting more and more difficult to deal with because of system complexity, volumes of data, and reduced cycle times — and all while more and more lives depend on data. As digitization proceeds, the volume of data that behavioral analysis systems have to deal with is growing dramatically. Some are experiencing petabyte data loads and worry that the load will accelerate.

Cycle time refers to the time it takes for attackers to come to the conclusion that their attack has been compromised, and therefore have changed it. This is particularly important for behavioral analysis systems because the change in attack results in a new behavior pattern to look for. If remediation doesn't happen fast enough, an organization may have a compounding set of rogue software and unauthorized intrusions simultaneously. This compounding makes further detection and remediation very difficult. It also hampers the ability of an organization to warn those impacted by the attack. This leads to further losses as seen in the Yahoo and Equifax cases.

All this is happening against a background of increasing system complexity, driven by layers of technologies, organizational units, vendor proprietary products, and other variables.

Lives depend more and more on digital systems. Large-scale examples include air traffic control, electric utility operations, and health care systems. Consider that there is an average of three to six connected devices on hospital patients at any given moment. Then, there is also the case of autonomous vehicles.

Remediation Today

Manual remediation today has serious difficulty keeping up. It is often too slow to prevent damage and sometimes, out of fear of crashing the system, not performed at all.

Remediation is generally performed by an SOC (Security Operations Center) that functions 24/7. Large organizations maintain an internal SOC, contract with an external entity, or a combination thereof. External companies, generally called an MSSP (Managed Security Service Provider), are often provided by telcos' Enterprise and Government Business Units. To do this, a telco either develops an internal capability and white labels an external MSSP, or openly subcontracts to an external MSSP.

Once an attack has been detected, it is up to the SOC to remediate. Typical remediation includes activities such as: changing firewall settings; disabling IP addresses; quarantining a system component; installing a patch; initiating a system restore function; rebooting a component; reloading software from a known good source; reconfiguring a system component; threat hunting; and so on.

These remediation functions today are provided manually from the SOC. In a piece in *Forbes* entitled "*Take Human Error, Inertia Out Of Security*," Larry Ellison of Oracle is quoted as saying, "Why is it that the worst data thefts have occurred after a software patch was available to prevent the system vulnerability that the hackers ultimately exploited? It's often because the target organization never applied the patch."

The problem is that to perform these functions manually it is best to have a staff person who is fully knowledgeable about the underlying technology. It ranges from very expensive to impossible to have a complete contingent of staff with expertise in all the technologies available all the time. This is because of the complexity and volatility of today's systems and the many layers of legacy and emerging technologies. It is generally referred to as the SOC Staffing Problem.

One common approach to the Staffing Problem is to use "playbooks". That is a step-by-step handbook for each type of technology and each type of threat. Unfortunately, manual implementation of playbooks can lead to serious problems. A competent staff member can encounter difficulties that cannot be dealt with using a playbook on a technology with which they are not familiar. For example, such a staff person using a playbook on a portion of the S3 Corp.'s system, inadvertently hit a wrong key. In the S3 case, the staff person did not understand the underlying technology. As a result, that person could not recover from the keystroke error, and could only watch as a series of cascading system failures brought down the entire network. It took most of a business day to bring the network back up. Since S3's business is the provision of service through its network, this meant that the company was out of business for a day with serious direct financial and brand value damage. This incorrect key problem is often called the "fat finger" problem.

In the words of Jon Oltsik, senior principal analyst, Enterprise Strategy Group, "Today's security operations teams are experiencing pain — too many manual processes, too many disconnected point tools, and a real shortage of the right skills. Manual remediation is time-intensive and can be prone to human errors."

The result is that manual remediation is often slow to respond (days, weeks, sometimes even months). Worse, sometimes not even attempted, out of fear crashing the whole complex of systems. This can also lead to attempts to cover up the breach. Recently, there have been a number of such breach cover-ups that have received a lot of negative attention. It is reasonable to assume that there are at least an equal number of breach cover-ups that have not yet been exposed.

Automated Remediation – A Network Immune System

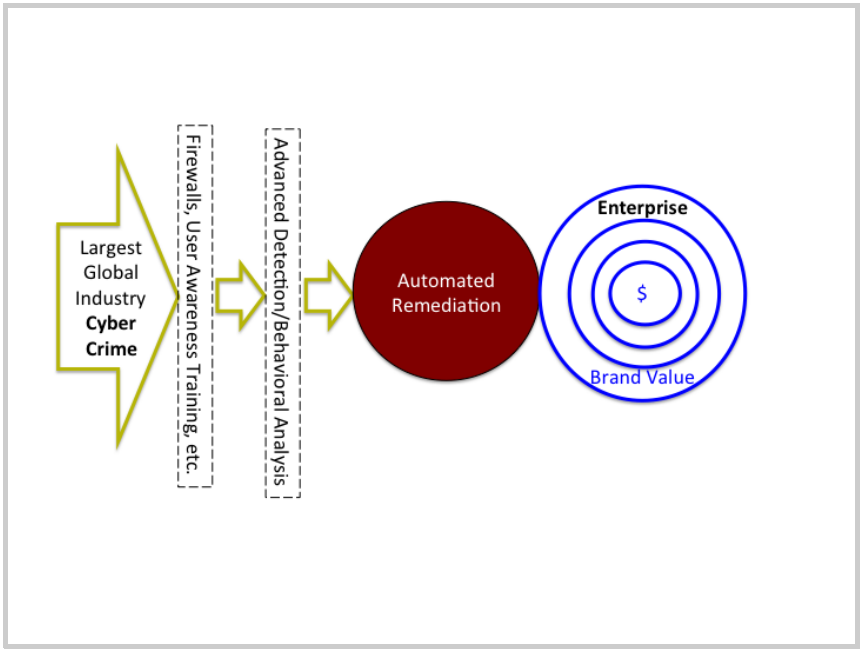

Figure 3 - Automated Remediation to combat cyber crime.

The concept of a network immune system is that large cyber systems can be thought of as similar to the human body with a skin (firewalls, etc.) keeping out most of the bad things, and an internal system that takes care of the ones that get through the skin. Stephanie Forrest proposed the concept of a network immune system 20 years ago. Now, the need for such a system has become clear and automated remediation makes it possible.

Automated remediation should be similar in concept to the human immune system. To achieve that objective in today's cyber systems, it must have the following characteristics:

- Combination of Central/Distributed - work with system components throughout the network (central site, edge, in between, etc.);
- Connect to all - layers of technology, administrative units, vendor products – even as they change;
- Move with functions as they move - from physical to local virtual, to private cloud, public cloud, hybrid cloud, etc.;
- Deal with today's scale – respond in second(s) to attacks on critical resources;
- Combine manual input where and when appropriate; and
- Deliver five nines performance (Telco-grade reliability).

This automated remediation capability should, much like the human immune system, be an overlay. Its objective is to be able to respond very quickly to an identified attack — in fractions of a second — several seconds at the most. To do this, it must have elements connected and physically very close to all system components. Attacks today target components at the edge, in the central site, and in between. So the automated functionality has to be able to have functionality that can function in all of these areas. Furthermore, in today's systems, functionality can move from: physical device, to local virtual implementation, to the cloud. Once in a cloud, it can move back and forth between private and public cloud. So, the automated remediation capability must be able to move with it.

This implies that the cyber immune system, like the human immune system, must have components distributed throughout the cyber system it is protecting. That these components must be able to move around in the cyber system without being reprogrammed; interact with each other very quickly and reliably; and interact with all the interfaces/data models of the cyber system components they are protecting.

Because of its critical nature, the automated remediation capability must be functioning reliably all the time. This means that it can not be shut down for system maintenance or because of the addition or change of components in the cyber system being protected. It has to be able perform in spite of the dramatically growing data volumes and cyber system scales. Finally, no man-made

system can be perfect, but the automated remediation capability should be able to meet the typical Telco performance standard of five nines. That is, an up time of 99.999 percent of the time.

There is an ongoing need for manual participation in some remediation activities. But in those cases, the manual activity also needs to be supported by automated tools to be effective. As Bill Yeack, an international security expert says, “Cyber assets can be categorized by value into five levels (level one: large numbers of low value assets – to level five: small number of very high value assets). For levels one and five, you want immediate incident response with no human interaction that might cause delays. For level two through four, you may want to have a human operator review proposed responses before they are implemented.”

Innovative software technology can today deliver these capabilities. The challenge today is for market participants to correctly understand what is needed and support those sources of innovation that are seeking to provide it.