Progress® | Flowmon

Adaptive Security Model: **A Network Approach**

Gartner's Adaptive Security Model helps organizations all over the world to assess maturity of their protection mechanisms. The concept employs several tools complementing each other to build a constantly evolving security architecture. Why does a deep insight into network traffic, combined with analytical capabilities, play a crucial role in this "security circle"?

The Gartner security model reminds us that blocking and prevention techniques are not enough today. Organisations must approach security as a well-constructed process to keep up with the growing volumes of clever and automated threats. But let us face the truth, 100% protection is an illusion. Usually it is not a question if you get compromised, but when. Once it happens you should then be ready to resolve the situation and optimize the entire security circle to strengthen your environment against the next strike. And this idea of a constant-learning approach is also the basis for the Flowmon security model which reflects Adaptive Security Model from a network perspective. It explains why a deep understanding of network behavior is crucial and how it contributes to optimizing the risk and security management processes of an organisation.

In the following text we will explain its added value on a real example of a ransomware attack against a Flowmon customer. The target organization was a European hospital with over 1500 employees and around the same number of beds. Naturally, the hospital devoted much energy to the protection of its systems and data. Since it was a modernthinking organization, it had already invested in a next-generation firewall, different email and web filters, an end-point data-loss prevention system and antivirus software, network access control and Active Directory for authentication.

We will look at what investments were made by this customer in cyber security and what the Return-of-Investment (ROI) was for the particular security incident.

PREVENTION

While the NetOps team will appreciate Flowmon's data on network structure during sizing, capacity planning or performance management, SecOps teams will use the same data to identify non-approved service traffic

FORENSICS

Flowmon stores full traffic statistics for weeks or even months, and auto-triggers the recording of detected anomalies to provide full packet trace of the event. This provides a wealth of insight about the communication and enables post-compromise analysis of the incident.

DETECTION

Perimeter and endpoint security can only protect against threats of known signature. The rest require a layered security model that can monitor the gap between perimeter and endpoint and pick up early indicators of compromise on the network level.

RECOVERY

Flowmon helps to assess the attack scope and impact to draft a robust recovery plan. This includes identifying parts of the network which were compromised, assets and users affected, and what needs to be re-installed or recovered.

RESPONSE

When it comes to response, the SecOps team assesses the risk and decides how to mitigate, but it's the NetOps who carries it out on the network level. Flowmon helps with coordination between the teams and agreement on the remedial action, which is essential for faster time to respond.

Prevention

A malicious email was received by an employee bypassing all preventive tools. Using social-engineering the email convinced the user to install Ransomware. This Ransomware spread around the network, including stations that had access to a visual documentation storage system. Among others, this "warehouse" kept all CT and X-ray scans of thousands of their patients. The Ransomware was able to encrypt almost half of the data, preventing doctors to access such a crucial source of information. Doctors could not intervene on patients whose lives depended on the precise estimation of their condition that could only be achieved by body scans. No important decisions on surgeries or treatments could have been taken without a clear understanding of the client's health status. Retaking a scan, costing around 2.000 EUR per patient, was not an option as any new scan would have been encrypted immediately after saving.

The consequential reputation loss, customer loss, operational costs, prosecution or charges the hospital might have faced for the inability to provide services were nothing compared to the fact that people's lives were in danger. The latest reports show the total potential financial impact of such attacks on hospitals could grow to hundreds of thousands of euros.

~170.000 EUR

Total amount spent on Preventive Security (CAPEX)
ROI: N/A (prevention did not stop the intrusion)

Detection

The customer‘s detection capabilities focused only on perimeter and end-points, thus creating a vacuum space of no protection in between. Additionally, they utilized only traditional approaches with signatures - ineffective against this new type of Ransomware. Flowmon filled the blank spaces by operating on the network between the perimeter and end-points so it was capable of seeing malicious activity inside the monitored network.

It does not specifically say: “I’ve discovered Ransomware called D4t4L0ck3r1.3.” The power of an anomaly detection system lies in the fact it does not rely on signatures, and therefore it can discover currently unknown attacks. So instead, it will tell you: “This station is acting in an unusual way. It is sending too much data, communicating to different systems, contacting outside IPs, etc.” Which is how our customer detected the attack. Thanks to Flowmon’s capabilities to identify an unknown attack based on heuristics and advanced anomaly detection mechanisms, the customer could react in a matter of minutes. This early-warning, near real-time system saved time for their engineers to detect the root-cause of the problem. Which, without Flowmon, would have taken anywhere from an hour to a whole day.

~38.000 EUR

Total amount spent on Flowmon to detect the attack (CAPEX)
ROI: single attack

Response

This is where even companies utilizing advanced detection capabilities experience major financial losses. In such situations, where every minute counts, automated incident response comes in handy. Flowmon can be easily integrated with a variety of systems that might not look like they fall under the incident response category in the first place. Leveraging equipment, which is already in the network, can be a very flexible and timeefficient solution, especially when automated. Flowmon can orchestrate systems such as Network Access Control (NAC), authentication services, Firewalls, etc. to block or disconnect infected stations from the network. In our case, the customer manually disconnected the malicious station performing the encryption from the network using NAC to prevent further data “loss”. However, without the previous step they would have still been blind to see which station was responsible at that point.

0 EUR

Total amount spent on Flowmon to orchestrate a response to the attack (CAPEX)
These capabilities are an essential component of the detection system.
ROI: N/A, single attack

Response

This is where even companies utilizing advanced detection capabilities experience major financial losses. In such situations, where every minute counts, automated incident response comes in handy. Flowmon can be easily integrated with a variety of systems that might not look like they fall under the incident response category in the first place. Leveraging equipment, which is already in the network, can be a very flexible and timeefficient solution, especially when automated.

Flowmon can orchestrate systems such as Network Access Control (NAC), authentication services, Firewalls, etc. to block or disconnect infected stations from the network. In our case, the customer manually disconnected the malicious station performing the encryption from the network using NAC to prevent further data "loss". However, without the previous step they would have still been blind to see which station was responsible at that point.

0 EUR

Total amount spent on Flowmon to orchestrate a response to the attack (CAPEX)
These capabilities are an essential component of the detection system.
ROI: N/A, single attack

Recovery

Disaster recovery responses may vary depending on the nature and magnitude of the attack. In the worst case scenario it would involve retaking all the possible and important scans again from scratch. Fortunately for our customer the Ransomware was stopped in its tracks in a timely manner and it could not impact other critical services. A full restoration of the impacted data took around 20 minutes. This is no time compared to the amount of resources needed to restore or rebuild multiple critical applications or large-scale data repositories.

Flowmon provides hard data disaster recovery decision making. In our case it helped the administrator to determine what other stations were potentially infected and would have sooner or later represented a threat. Not only could those stations have encrypted other important files, they could have tried to infiltrate sensitive data outside their network. A full software refresh was performed on those stations as the locally installed AV could not identify and remove the malicious code.

0 EUR

Total amount spent on Flowmon to enable a prompt recovery (CAPEX)
These capabilities are an essential component of the detection system.
ROI: N/A, single attack

Forensics

To be honest with ourselves, Prevention is still very important and if we could create an ideal Prevention strategy, we would never need to design multi-layer Security models with Detection, Response. Only after performing a full recovery, administrators have time to focus on building up better prevention systems which is impossible without evidence for analysis and forensics. Flowmon helps to thoroughly understand the characteristics of an intrusion throughout the whole process and across all IT departments. Flowmon provides both aggregated statistical data and even full packet traces - triggered manually or automatically. So get the most out of your investments to Prevention by adjusting it on the fly with the ultimately scalable, easy to deploy and work with, and all-in-one solution. Based on this investigation our customer introduced even more restrictive access rights to the storage, and applied rules that would specifically report on this type of incident and preventively block the source of encryption as a fully automated action.

0 EUR

Total amount spent on Flowmon to orchestrate a response to the attack (CAPEX)
These capabilities are an essential component of the detection system.
ROI: N/A, single attack

Wrap up

A dysfunctional computer network inherently equals loss of company productivity. Networks are just like your own body. Taking vitamins cannot guarantee you never get sick. And when you do, you can visit the doctor who can prescribe medicine that cures you in a few days - which means you are incapable of working and will be unproductive during that period. Continuous monitoring, observation and automated detection of bad symptoms can save you a trip to the GP and all those wasted days on sick leave.

Final Bill

Total potential business impact w/o appropriate technologies in place: ~300.000 EUR
Total cost of Detection, Response, Recovery, Forensics toolset: ~38.000 EUR
Total cost of Detection, Response, Recovery, Forensics operations (people): ~500 000 EUR
Total ROI: single attack

Computer networks have become a nervous system of every organisation. Paying attention to this part of business IT really pays off. Modern network monitoring and security tools allow a way not only to **detect threats** bypassing firewalls and signature-based protection. They also significantly **simplify response** to new and persistent threats, **accelerate recovery** process and provide important **information for forensics** that empowers **better prevention**. Thus they play a key role in strengthening the entire security circle of an organisation.

Be proactive, think about what happens if prevention fails. It is not as expensive as you would think and you do not need to deploy ten different tools from ten different vendors to cover the majority of the fundamental parts of the Adaptive Security