The evolution of network monitoring and forensics

LogRhythm
The Security Intelligence Company

Network monitoring and forensics must keep pace with attacks regularly breaching perimeter defences. As threats evolve so must security technology.

The cyber threats facing organisations today are growing in both complexity and the impact they have. A glance through news headlines in 2017 shows this to be the case.

The UK NHS was one of the highest profile casualties of the global WannaCry ransomware attack in May. And what was initially thought to be a new variant of the Petya ransomware – dubbed NotPetya – surfaced in June hitting container shipping giant Maersk and the TNT division of FedEx, among others.

Meanwhile, credit monitoring agency Equifax is still to realise the full extent of the fallout from the hack in May that exposed personal data of 143 million US customers. Particularly as the breach was only discovered in July. At the time of writing a number of senior executives had resigned as a result.

As well as the damage to brand and reputation, the financial costs of these breaches are huge. Cybercrime costs organisations an average of $11.7m per year, according to the 2017 Cost of Cybercrime study by Accenture and Ponemon[1].

And there is the likelihood of additional hidden costs further down the line through operational disruption or the loss of proprietary information and other strategic assets.

Organisations cannot afford to take modern cyber threats lightly. And as attacks evolve they need to move away from traditional network monitoring and forensics. If you stand still, you run the risk of becoming the next big cyber breach news story.

Cybercrime costs organisations an average of $11.7m per year

[1] 2017 Accenture and Ponemon Cost of Cybercrime Study https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Compromises should be expected

Threat actors are penetrating corporate networks using methods such as spear phishing and whaling, to compromise credentials. Once in they move laterally to consolidate their position and compromise other more privileged accounts.

Additionally, the number of routes into networks have increased, with cloud computing, mobile devices and the Internet of Things all providing potential entry points for attackers. This helps explain why 79 per cent of surveyed organisations said they were breached in 2016[2].

The 'new normal' is that the criminals are going to get into your corporate network. Committing too much resource on defensive perimeter protection – the 'gates, guards and guns' – and not focussing enough on what happens inside your network is no longer realistic.

Modern threats typically take their time to surface. The average time for an organisation to realise it had been breached in 2016 was 99 days[3]. Although this is an improvement on the 146 days seen in 2015, it's still plenty of time for damage to be done.

Organisations must identify a threat before they are impacted and as early as possible in the cyber attack lifecycle. This could be the difference between a compromise that causes minor headaches and one that develops into a full breach in which the loss of the corporate 'crown jewels' makes the organisation headline news.

Organisations must identify a threat before they are impacted and as early as possible in the cyber attack lifecycle

Stopping threats earlier in the kill chain

VPNs and firewalls remain important for the 'north-south' movement of data in and out of a network. But increasingly, it is essential to effectively monitor data as it travels 'east-west' across a network.

It's crucial that the attack is stopped as early as possible in the cyber attack lifecycle, also known as the 'kill chain', to minimise the damage to a network. There are six recognised stages in the kill chain: reconnaissance, initial compromise, command and control, lateral movement, target attainment, and finally exfiltration, corruption and disruption.

[2] 2017 Cyberthreat Defense Report' http://www.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Webroot_Q3_2017_CyberEdge_Cyberthreat_Defense_Report.pdf
[3] Mandiant M-Trends 2017 https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

LogRhythm
The Security Intelligence Company

The further along the lifecycle an attack travels, the greater the likely damage to the organisation. If a malware incident is caught at the lateral movement stage, it will prevent it moving across the network and reaching the data it's aiming to damage or obtain. If, however, exfiltration of data is already taking place, the damage, to a greater or lesser extent, has been done.

As a result, effective monitoring and forensics are absolutely crucial for flagging activity within the network that suggests an attack in the early stage of the kill chain is in progress.

How monitoring and forensics needs to evolve

Before any threat can be detected you must be able to see evidence of the attack within the IT environment.

The activities that suggest a cyber attack is in progress – such as a typical user behaviour - generate digital fingerprints, audit trails and log data at the entry point to the network and within the network itself. Monitoring and forensics technology needs to identify these digital fingerprints and alert the security operations centre as quickly as possible, before the next stage of the kill chain is triggered.

Monitoring and forensics needs to move beyond looking for an indicator of compromise (IoC), such as the signature of a malware file, and focus on the tools, techniques and procedures (TTPs) used by cyber criminals.

If they hunt for the signature of a malware file, they will have to keep up with each IoC that arises, making it harder to detect new threats. It is far more effective to focus monitoring technologies on TTPs. For example, this approach will flag up unusual user behaviour or whether files are being encrypted en masse - a sure sign that something is wrong.

LogRhythm's Threat Lifecycle Management platform can help organisations gain the deep and broad visibility they require to avoid a compromise turning into a damaging data breach. Arm your security staff with the visibility that they need today by contacting LogRhythm.

About LogRhythm

LogRhythm is the pioneer in Threat Lifecycle Management™ (TLM) technology, empowering organisations on six continents to rapidly detect, respond to and neutralise damaging cyberthreats. LogRhythm's TLM platform unifies leading-edge data lake technology, artificial intelligence, security analytics and security automation and orchestration in a single end-to-end solution. LogRhythm serves as the foundation for the AI-enabled security operations centre, helping customers secure their cloud, physical and virtual infrastructures for both IT and OT environments. Among other accolades, LogRhythm is positioned as a Leader in Gartner's SIEM Magic Quadrant.

www.logrhythm.com