SECUINFRA
Cyber Defense. Made in Germany.

Specialist Article

Threat Hunting: Proactively search for attackers

Tracking down cyber attacks with hypotheses

They bypass detection and monitoring systems, nest throughout the network with lateral movements, and systematically siphon off data and information: Targeted, complex and often effective Advanced Persistent Threat (APT) attacks have high damage potential. Threat Hunting provides a proactive way to detect attackers in the system even without initial triggers and reduce the time to detection. By gaining knowledge, Threat Hunting allows a continuous improvement of cyber security.

Vulnerability Management, Security Information and Event Management (SIEM) or Advanced Persistent Threat Scanner: Companies monitor their IT infrastructure with various tools and focuses. Threat hunting is a useful addition to this: the proactive search for attacker activity in the system without the knowledge that there is actually an intruder in the network. In other words, it usually takes place without an initial trigger. IT security specialist Steve Anson compares threat hunting to police patrols: Police don't just wait for incidents to be reported and responded to, but actively patrol their area of responsibility. Those tasked with cyber defense should therefore also not just wait for an alarm, but actively and continuously look for traces of attacks.

Advanced Persistent Threat (APT) attackers are particularly keen to remain undetected for as long as possible. They bypass defense mechanisms, infiltrate the network and seize knowledge and data undetected. With lateral movement, they succeed in gaining more and more access to systems. Especially in the case of elaborate attacks, attackers are often so-called nation state actors, intelligence agencies or state actors. Their goal is not extorting money via ransomware, but industrial espionage: at one company in Scandinavia, for example, an APT group searched the network for connections to the US Department of Defense. These types of attacks can be detected with Threat Hunting and their gateways closed.

The requirements for Threat Hunting

People and their expertise play the key role in Threat Hunting: hunters need a wealth of experience. They must be able to put themselves in the shoes of potential attackers and know or understand their attack vectors and tactics. It is also important to know about current threat situations, including industry-specific ones, i.e. who is specifically attacking and how to go about it. It is also helpful to examine procedures and tactics from past attacks and their originators and apply them to the current situation.

At the same time, threat hunters must be familiar with the system, network and infrastructure: Threat hunting is carried out on the basis of a SIEM system, where messages and log files from the systems are bundled and evaluated - it enables a holistic view of cyber security.

Therefore, a corresponding data basis must have been created in the company through SIEM and log management: If not all information is connected, not all tactics can be used in threat hunting. A mature architecture is therefore required - this is usually the case in companies above a certain size that have laid the foundations for cyber security: Incident response processes, for example, have already been established and are lived.

Threat hunting is located in the Security Operation Center (SOC). If there are no alerts or detections in the system and no attacks need to be actively investigated, threat hunting can be carried out during idle times. The use of full-time cyber security personnel is just as conceivable as that of service providers: the trend is toward purchasing the service as a managed service, and large corporations in particular are resorting to this.

The Threat Hunting Process

In the process of threat hunting defined by Steve Anson, a hypothesis is first formulated and then it is defined what evidence there would have to be if it is correct. Thus, the hunters do not have a specific use case, but generally start freely. Based on the existing data, they search for tactics, techniques and procedures (TTP) of the potential attackers.

Tools such as UEBA (user and entity behavior analytics) or the MITRE ATT&CK matrix help threat hunters keep track of the possible variants; known attacker groups are given proper names and categorized by institutions; companies and service providers, such as developers of antivirus software, make the knowledge publicly available worldwide. For example, the MITRE ATT&CK matrix can be used to narrow hypotheses to different tactics for different phases of the attack.

One hypothesis might be that a malicious program disguises itself as a legitimate Windows system file, svchost.exe. Evidence could be that the file is located in unusual folders. Another suspicion may suggest anomalies in a network area - for example, that a client has recently been logging on at unusual times or that login attempts are being made from atypical regions. Threat hunters are not looking for Indicators of Compromise (IOC), but Indicators of Attacks (IOA).

Once the hypothesis is established, the expected evidence is subsequently searched for and the hypothesis is either validated, re-sharpened and further developed or disproved. Vulnerabilities in the security infrastructure are uncovered, log gaps or tech gaps are identified, and it is determined whether the detection mechanisms are good enough or where the limits of endpoint protection lie. The results can be reflected back and cyber security can be improved with the new knowledge - increasing the maturity of systems such as log collection. In a further step, the results of Threat Hunting can be incorporated into the automation of further detection and prevention, so that attackers are detected automatically and a time-consuming manual search is no longer necessary. In this way, Threat Hunting enables prevention to be optimized and the level of automation to be increased. If accesses are detected or malicious files are identified in the system, it also triggers the incident response process.

Overall, threat hunting reduces the time attackers spend in the system, i.e. the time between intrusion and detection. Especially in the initial phase, an attack is usually difficult to detect - it can be detected with Threat Hunting.

The three approaches in Threat Hunting

There are three threat hunting approaches: Analytics-Driven, Situational-Awareness Driven and Intelligence-Driven. In the first case, tools such as machine learning and UEBA are used to sift through the data at hand and identify anomalies. On their results, the hunters build their hypotheses. In the Situational Awareness Driven approach, one starts from the crown jewels of the infrastructure: One defines which assets and data are particularly interesting to attackers and thus worth protecting, what exactly they provide, and derives attack paths from this. The intelligence-driven approach is not only based on the available threat intelligence. The knowledge of Indicators of Compromise (IOC), Tactics, Techniques and Procedures (TTP) as well as the knowledge of which attacks are currently being carried out and which groups are being targeted also play an important role. These hunt triggers are, for example, reports from the Threat Intelligence Report or a cyber letter from the Federal Office for the Protection of the Constitution on attack campaigns against German companies. An active search with a corresponding hypothesis can build on this: The same attacker groups often resort to similar approaches.

Conclusion

Threat hunting is a productive method for companies to increase cybersecurity and complements detection and monitoring systems such as Compromise Assessment or Vulnerability Management. It can detect attacks at an early stage and reveal security vulnerabilities in the system. Based on the insights gained, it is possible to optimize and automate cyber security.

Authors: Leon Hormel, Cyber Defense Consultant

SECUINFRA Falcon Team

Maximilian Zahn, Cyber Defense Analyst

SECUINFRA Falcon Team

Further information: https://www.secuinfra.com/en/services/co-managed-siem/

Press Contact: SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Mobile: +49 160 921 633 44

marketing@secuinfra.com