The Threat Hunting Route to Predictive Cyber Security

Abstract

Within an increasingly malicious cyber threat landscape, our defense mechanisms must mature from being reactive to proactive and finally, predictive. For the modern security operations center (SOC), cyber threat hunting is the next step in the evolution. With enterprises spending more than half a million US dollars to recover from a breach,1 it's time to invest in capabilities that can detect unknown threats before alarms are raised. This will not only fortify systems but further improve security controls.

In this paper, we highlight the different elements required for developing cyber threat hunting capabilities and recommend a structured approach for enterprises across industries.

Unlike conventional IT security methods, cyber threat hunting is more proactive and iterative when it comes to searching networks and datasets to detect breaches that would otherwise elude existing automated tools.

This human-led methodology leverages analytics or a machine learning platform and a combination of techniques to counter threats. Once a new or possible security risk has been identified, these are categorized and added to an automated security information and event management (SIEM) platform.

The maturity of cyber threat hunting practices depends on an enterprise's present state of IT security, and it's willingness to invest in technology, people, and processes to further its capabilities.

Building Blocks for Threat Hunting

The success of threat hunting depends largely on the data available to the security analyst team along with an inventory of tools and platforms that can assist in visualizing, analyzing, and applying insights. This will allow the team to look for new threats which can be behavior or trend based.

In order to build such a framework, enterprises must take note of:

- **Data visibility**—wherein there are comprehensive security logs/events that include network traffic and application usage information along with relevant threat intelligence reports
- **Tools**—such as SIEM, data and user behavior analytics, firewalls, and end point solutions
- **Security intelligence**—which includes updated exploit information, attack vectors, indicators of compromise (IOC), relevant risk trends, and situational awareness
- **Skills**—with respect to forensic analysis, ability to think like a hacker, and openness to continuous learning

Broadly speaking, the cyber threat hunting process has four key stages:

- **Hypothesis** – created by a human analyst on the basis of trends, recent security events, threat intelligence reports, and insights gained through visualized data
- **Investigation** – using tools and techniques associated with linked data analysis, visualizations, statistical analysis or machine learning

- **Uncovering** – incident patterns and lateral movements within the network
- **Performing analytics** – to automate the detection process for similar incidents in the future

Cyber threat hunters can leverage Kill Chain, Diamond, or Hopper models which can aid in identifying threats and intrusion. These models provide not only a structured approach for understanding the capabilities of cyber criminals but also extract relevant information from the threat intelligence feeds. It's important to note that these models on their own may not be foolproof. Equifax's recent breach is a great example of how even the Kill Chain model on its own proved to be ineffective.2 Most security teams already have too much on their plates and may at times be unsure about what needs to be prioritized.

Perhaps, a more cohesive approach would be to combine these models' strengths. In fact, the Diamond and Kill Chain analysis are highly complementary. Kill Chain allows the security analyst to target and engage an adversary and 'create the desired effects' – identifying the right set of data along with high risk indicators. Diamond model applies scientific principles to intrusion analysis and provides a comprehensive roadmap on how the threat can be mitigated.

Future-Proofing Cyber Security Apparatus

As the first step, enterprises must build a cohesive approach to enhance and mature their threat hunting capabilities. This must be supported by a proactive threat monitoring methodology leveraging a robust analytics platform. While this process mostly relies on correlated alerts, through dedicated threat hunting enterprises can preemptively identify possible breaches within the IT environment. Newly identified threats can be categorized and added to the security management platform (like SIEM) currently in use. This will help automatically identify such threats in the future, thereby strengthening the overall enterprise security posture. This will also help to detect and address flaws in the current security framework, and build on existing capabilities rather than start from scratch each time there's a data breach.

Enterprises need to understand their IT infrastructure—hardware, software, and network resources—along with existing security controls, people, and processes before building such an approach. As highlighted in Figure 1, the next steps will include:

- Introducing and equipping the data analytics platform with machine learning and visualization features capable of onboarding huge volumes of out-of-the-box data.
- Supplying the platform with the right data sets—events logs, network traffic, end point and application information—for visualizing and analyzing purposes.
- Enriching the platform by providing indicators, evidence-based knowledge for tracking advance threats.
- Visualizing data in terms of assets and users behavior, along with network trends to identify exact breach patterns and create hypothetical scenarios.
- Creating a dedicated and specialized group of experts to address security issues—based on these hypothetical scenarios—missed by existing SOC teams. Once suspicious behavior is detected, the threat hunter will investigate, add threat artifacts to better uncover and mitigate possibilities of future breaches.
- Evaluating the extent of threat penetration and data exfiltration within a compromised IT environment.
- Integrating the platform with the automation engine to automate the detection process.

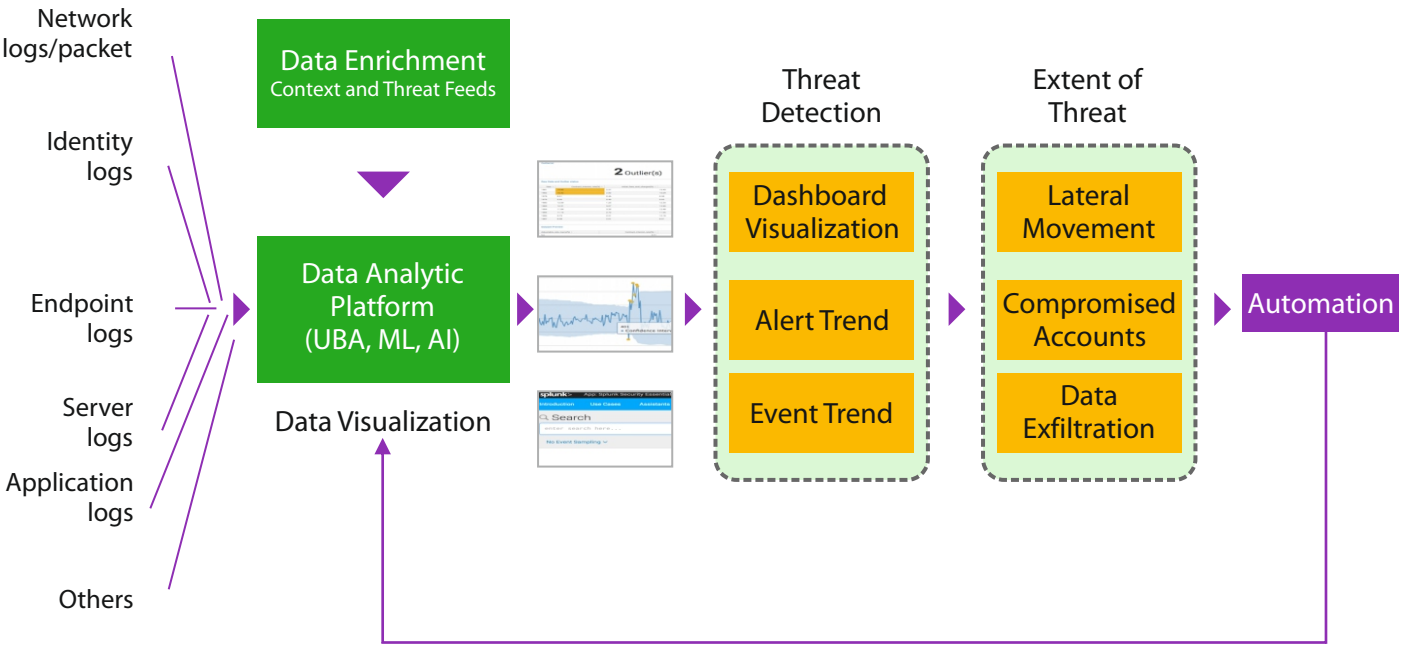

Figure 1: An end-to-end cyber threat hunting approach

Consider an example where high DNS traffic triggered a data exfiltration alert. Using the Kill Chain model, an enterprise can work backwards to hunt for the root cause. Figure 2 highlights an ideal scenario to detect data exfiltration.

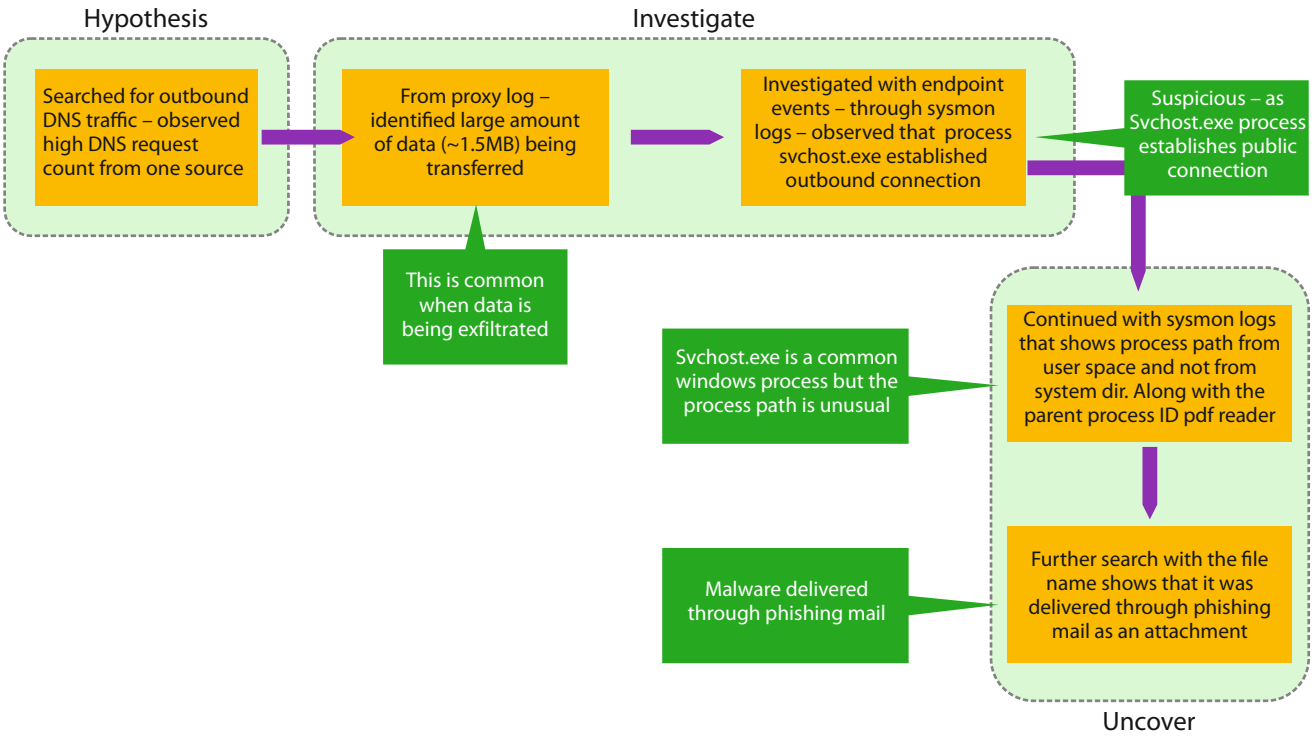

Figure 2: Detecting Data Exfiltration

However, we also need to keep in mind the lessons learnt from Equifax's massive data breach. Most Internet applications (at risk from external attackers) are usually placed in a demilitarized zone (DMZ). Communications between these apps and the enterprise's internal systems are more predictable, wherein security teams can note the frequency of access, credentials used, volume, and so on to build an adaptive behavioral profile. Malicious activities that usually go unnoticed can be tracked using user and entity behavioral analytics (UEBA).

Moreover, enterprises must use containers for applications, which provide more protection than physical servers and virtual machines. Using a Dockerfile, these containers create application images, which can be scanned easily before deployment to discover known vulnerabilities. A vulnerable application can then be swapped out seamlessly once an update patch is available. But these alone will not be able to prevent attackers from exploiting the Kill Chain.

Herein, a breach and attack simulation platform can help security teams gain a thorough understanding of these threat

actors. Across the Kill Chain, analysts can note the different ways an attacker can infiltrate, move laterally to a deeper part of the network, and exfiltrate data – buying time for security teams to figure out the best way to break the Kill Chain. One can start with segmentation to stop the lateral movement, or simply focus on stopping data exfiltration with data leakage prevention (DLP) solutions.

A set of deep packet inspection (DPI)-enabled pattern match signatures can prevent attacks similar to Equifax's. Generally, the attack vectors utilize predictable parameters. Generally, malicious HTTP requests have a shell command embedded in an XML object or a malformed header. Security teams can develop signatures based on these attack patterns, while DPI can help limit false alarms.

Fortifying the Way Forward

It's time for enterprises to adopt a continuous process of proactively evaluating threats that may infiltrate their networks and systems, rather than investigate when the need arises. This will require establishing dedicated teams and implementing platforms to uncover unknown threats, and not be limited to predefined alerts usually configured in SIEM. As the enterprise security posture matures, it will be easier to define and follow a foolproof threat hunting roadmap—leveraging artificial intelligence (AI) and machine learning to detect breaches and automate the remediation process.

References

1. Kaspersky lab, Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series, accessed on January 10, 2018, https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf
2. Federal Trade Commission, Consumer Information, The Equifax Data Breach: What to Do, September 8, 2017, accessed on January 30, 2018, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

About The Author

Prikshit Goel

Prikshit Goel heads the Managed Security Services as part of TCS' Cyber Security Practice. He focuses on providing security and IT infrastructure solutions to the customers by leveraging relationships with strategic partners and developing new offerings in the security space. He is also responsible for developing training framework, accelerators and an effective competency plan for both solution design and delivery. He has over 17 years of experience in the IT space with a focus on Information Security and Networks. He also holds many industry certifications such as PMP, Cisco CCNP and CCNA, ITIL, BAC, CEH, Splunk, Avaya, ITIL, Six Sigma Green Belt and ACS and is trained in security products such as RSA, Symantec, Palo Alto, and Cisco across various layers.

Contact

Visit Cyber Security page on www.tcs.com

Email: cyber.security@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services | M | 02 | 18