o entext

Table of Contents

Introduction

Every day a plethora of threats target your company

but the volume of data has grown, allowing attackers to hide in the noise. While artificial intelligence and machine learning can help by highlighting anomalous activity, such automation does not know whether the anomalous behavior is good or bad. It lacks situational context.

Blending the two approaches and letting them work together to get faster, actionable insights, with context, helps with the real problem: Reducing the time a company is exposed to threats. A system that puts together different data sets can improve the chance of detecting—and prioritizing—the signs of an attack. This layered approach to security analytics results in better coverage of a company's attack surface and earlier detection of threats—before they can do extensive damage.

Layered analytics—which brings together correlation, behavioral analytics and threat hunting—helps companies minimize the impact of an attack. For vigilant companies with

- The big data analysis and search capabilities of ArcSight Recon by OpenText™ supports extensive threat hunting and incident response activities.

Combining layered analytics, and not relying on a single approach, gives additional context to

Correlating the behavior of various entities—whether processes, devices or users—allows security operations to see through these attempts at obfuscation and gives organizations a better chance to detect and stop unknown threats. While the link included in the initial e-mail used in an Emotet campaign, for example, may fool any blacklist, a rule that correlates an e-mail message from an unknown sender with a link to an previously unknown domain could help identify a wide variety of phishing attempts.

Pre-Emptive Threat Detection

Companies are inundated with security events, often causing alert fatigue for security analysts.

Often, indicators of compromise found by other organizations can be the starting point for analysts to hunt for threats in their own network Mining analysis of high-pro le incidents, such as the compromise of SolarWinds' software, can also be a good starting point to look for attackers in your own network.

Only a quarter of companies were able to stop ransomware before data is encrypted, and those who paid a ransom had roughly double the costs—$1.4 million—compared to those who refused to pay a ransom[6].

Conclusion

The key to catching complex threats early is to uncover signs of attack from as many parts of the chain as possible. By not relying on a single source of information, layered analytics can correlate subtle evidence of an attack into a single decision based on context. Real-time correlation allows organizations to use known threat details to automate threat detection. User and entity behavior analytics (UEBA) can determine what activity is normal in your organization and what should be considered an anomaly. And, threat hunting gives security teams the tools to use current indicators of compromise to take a second look at historical data.

Layered analytics supports the entire threat-intelligence lifecycle. ArcSight ESM operationalizes any intelligence on known threats by integrating it with the real-time correlation engine. ArcSight Intelligence allows user and device behavior to be analyzed for unknown or emerging threats by uncovering abnormal activities. And ArcSight Recon gives analysts a tool for proactively looking into evidence of threats.

No matter where you start in the analytical cycle, adding additional capabilities and analytical layers is simple. ArcSight's ESM, ArcSight Intelligence, and ArcSight Recon are tightly integrated to allow each product and its analyses to be used as context451 Tm (l5ty teams the tools to use current indicatorsc9lys7ET EM

oper e