White Paper

Detect and Stop Advanced Threats Faster to Reduce Security Risk

Secureworks Crowdsources Threat and Tactics Intelligence for Fast and Accurate Behavioral Threat Detection

By Christina Richmond, Principal Analyst

January 2020

This ESG White Paper was commissioned by Secureworks and is distributed under license from ESG.

Contents

Executive Summary – Market Challenges

Threat prevention is a critically important component of a cybersecurity strategy, and most organizations invest abundant resources into security controls and processes in this area. Cybersecurity professionals are responsible for threat prevention, detection, and response. Threat prevention depends upon decreasing the attack surface with proper security hygiene activities, but that isn't always enough, as adversaries can circumvent these defenses with simple changes to evade signature-based detection. This allows them to compromise IT assets and can lead to extensive damage.

This is where threat detection and response come into play. Beyond blocking known malicious behavior, organizations must collect, process, and analyze internal and external data, identify and investigate suspicious activities, and remediate problems quickly before minor issues become major data breaches. The processes, tools, and personnel used for these tasks are generally referred to as security analytics and operations and often reside in a platform architecture called a security operations and analytics platform architecture, or SOAPA (see Figure 1).

Tactics, Techniques, and Procedures

Cyber-adversaries often employ sophisticated attack tactics, techniques, and procedures (TTPs) in order to avoid detection, but they don't change the foundation of the TTPs greatly over time. Adversaries don't often create new tools or tactics. They use the same ones over and over. In fact, while there are millions of malware variants—far more than "goodware," in fact—there are only hundreds of tactics or techniques that are used routinely with subtle changes. And, in many cases, multi-stage attacks simply blend into benign IT activities. This forces organizations to constantly upgrade security analytics and operations tools, skills, and processes to stay a few steps ahead of the hackers. Unfortunately, this can be extremely difficult, as security analytics and operations are often limited by a lack of experience, resources, and skills; an assortment of disconnected point tools; and manual processes. But there is the possibility for organizations to impact the adversary where it hurts, in the wallet, by forcing them to build new tactics.

This white paper is focused on the challenges that cybersecurity professionals face with threat detection and response (TDR) and advancing solutions to these challenges using SOAPA, machine and deep learning, human analysis, automation, and behavioral playbook mapping. While automation is not yet mature enough to detect malicious activity, analyze the TTPs used, and respond on behalf of organizations with zero human involvement, Secureworks is innovating to help companies get more out of automation, software, and intelligence with its newly launched Red Cloak Threat Detection and Response platform. The platform is particularly adept at spotting advanced and unknown threats quickly by using data science to uncover known tactics or behaviors. Critical human analysis must be augmented by software-based security analytics tools if the security industry is ever to get ahead of the adversary.

Applying Data Science Expertise to Threat Data

A Primer on Data Science Terminology

Confusion about the use of data science for security abounds because disparate capabilities such as threat analytics, machine learning (ML), deep learning (DL), and artificial intelligence (AI) are loosely and interchangeably used in marketing security tools and services. Threat analytics attempt to understand where threats to assets exist and plan mitigation strategies around that. ML, DL, and AI are used in threat analytics and can reduce the complexity of analysis performed by humans. Threat telemetry, threat data, and threat intelligence are often used interchangeably though they are different. Telemetry is the process of recording and transmitting the readings of an instrument or device, which then becomes the threat data that machines and humans analyze. Threat intelligence means that the threat data has been codified, contextualized, and correlated to make it actionable. However, not all threat intelligence is created equally. Data sources vary from commercial data feeds through in-house security technology telemetry to crowdsourced data from multi-tenant services such as managed security services (MSSs). There are many ways to get a broad set of data to analyze, but more is

not necessarily better. However, crowdsourced data can broaden the lens and if expert analysis is deployed, false positives and alert noise can be reduced. The use of commercial off-the-shelf (COTS) analytics solutions without real-world expertise isn't sufficient. To detect and thwart attacks, solutions must be trained to look at the threat landscape across multiple verticals and environments and to build models that allow analysts to see adversaries based on their understanding of the attacker's goals and tactics. It's not enough to provide a query engine with vast amounts of data and hope for accurate detection without a lot of false positives.

Combining Behavior- and Signature-based Detectors Speeds Detection

Signature- and reputation-based detectors are foundational but fall short of accomplishing the mission to thwart the adversary because pre-knowledge of the threat posed is required. Rather, when threat detection employs both signature- and reputation-based detectors plus a category of analytics that are not representational like these static ones are, the opportunity to find unknown malicious content is greatly improved. Additionally, threat researchers must seek an understanding of attacker intent, capabilities, and the opportunity coveted to add context to the threat telemetry. For example, why would attacker X target organization/person Y? Is person Y simply a pass-through target to get to a larger acquisition such as partner or customer data? Attaining context is difficult across a layered security architecture with multiple vendors, which creates a diverse security taxonomy.

Historically, the security industry has applied a long-outdated defense-in-depth approach, layering multiple best-of-breed security technologies in the architecture. Sadly, this has created a cacophony of device telemetry but no common methodology to understand it all. Managed security service providers (MSSPs), which see a broad set of threat data from a diverse universe of security vendors and telemetry, have had to create a common language with which to interpret, correlate, and codify the data. This is what Secureworks has named Defense-in-Concert, an approach that provides much needed context and intelligence to identify attackers based on behavior. Once a common language is established, both human and machine analysis can assist in determining next steps.

Applying a SOAPA Approach to Security Analytics and Operations

As stated previously, the processes, tools, and personnel used for collecting, processing, and analyzing internal and external data, then identifying and investigating suspicious activities, and remediating problems quickly before a major data breach occurs are generally referred to as security analytics and operations and often reside in a platform architecture ESG calls SOAPA (see Figure 1).

Figure 1. Security Operations and Analytics Platform Architecture (SOAPA)

SOAPA: Security Operations and Analytics Platform Architecture
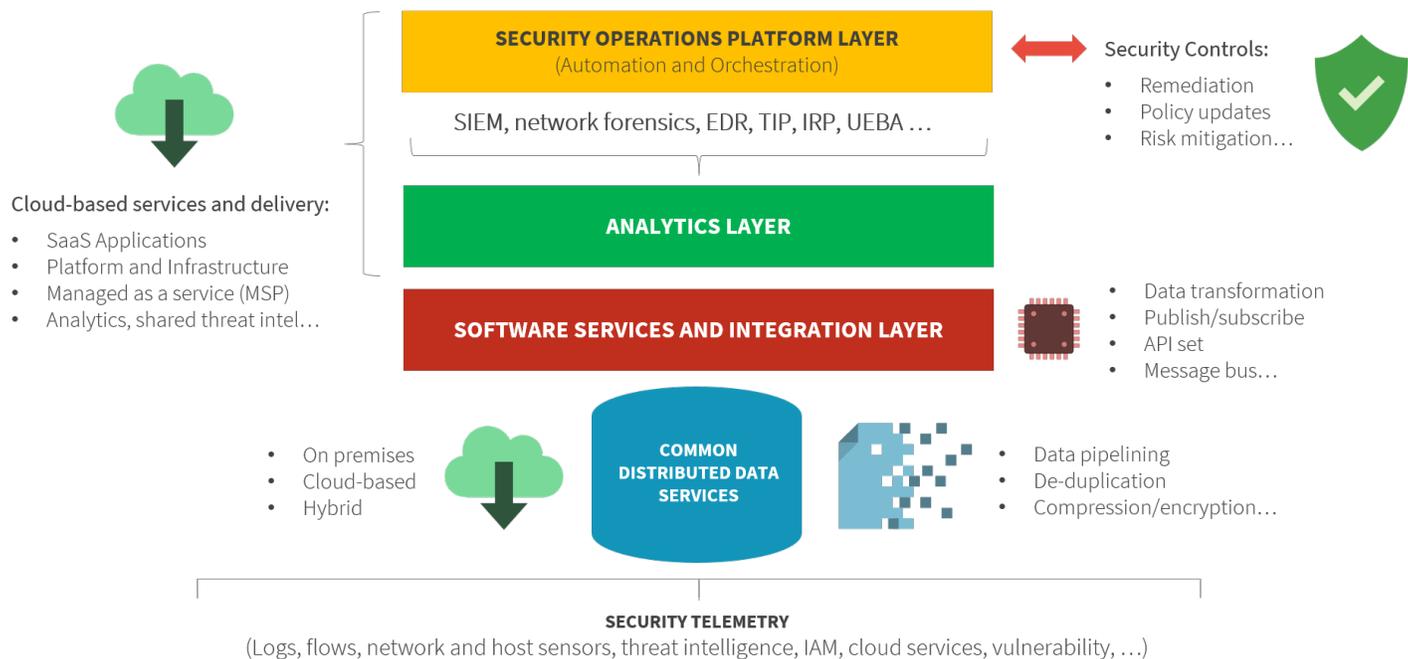
Source: Enterprise Strategy Group

According to ESG research, the most cited reason that respondents invest in security, analytics, and operations is to improve the ability to detect, contain, and remediate advanced attacks.[1] It is important to remember, however, that SOAPA is a tool that depends on what type of data is ingested to orchestrate and analyze. The adage "garbage in, garbage out," or "GIGO," comes to mind. If the organization ingests a diverse set of telemetry with no common language to interpret it, the results are compromised. Orchestration and analytics are key to improving process and are essential to augment human analysis, but it is critical to utilize a defense-in-concert approach where all vendor telemetry is normalized by a common taxonomy in order to speed operationalization of the data.

SOAPA isn't easy. The threat landscape is changing so quickly as to make it challenging to keep up with SOAPA trends.

In addition to a rapidly changing threat landscape and regulatory complexities, organizations are impacted by operational efficiency and cost. In fact, 30% of ESG research respondents state that the cost of operations is one of their top challenges with SOAPA activities, making it the most common response.

Improving Outcomes with SOAPA and Behavioral Threat Detection

How then do we put SOAPA to work in security operations (SecOps) so that threat hunters, researchers, and responders can work smarter and faster? SOAPA is AI/ML/DL's assistant in rapidly discovering the attacker's perspective, and more deeply understanding the threat landscape and behavioral tactics. SOAPA can help put these pieces together for faster and more accurate behavioral detection and help security teams stop playing "whack-a-mole." Faster detection and response imply the need for more sophisticated TTPs, which cause the adversary to go back to the design phase for malware, hence increasing *their* cycle time.

---

[1] Source: ESG Research Report, *Cybersecurity Operations and Analytics in Transition*, July 2017. All ESG research references and charts in this white paper have been taken from this research report.

We've discussed the importance of how data is used. Large quantities of generated machine data can create a high volume of false positives if the data captured isn't relevant, isn't properly codified, and isn't correlated to the right tools, and if context isn't derived. Beyond this, consider that threat intelligence is static, and that learning is dynamic. Machines can learn but not in the same sensory capacity as humans. The Cynefin framework in Figure 2 on detection and response analytics provides clear identification of this challenge. We can divide the problem and the solution into the "known" and the "unknown." In the known quadrant (upper left square), there are some threats we can see and others that may be seen or unseen but that have signatures defining them. Note that this Cynefin makes apparent that the unknown is a majority—three-quarters in fact—of the framework, demonstrating that more is unknown than known in security analytics. In the lower left quadrant, we may realize we have a problem but not know how to detect it, and this is where the industry may use tools such as data mining, predictive analytics, and supervised ML to show unknown relations among events. Conversely, we often do not know there is an issue, but detection through pattern matching (upper right quadrant) may provide user, network, or data anomalies that can be investigated. The worst analytics situation in this framework, of course, is the unknown unknown threat, with limited to no ability to detect (lower right quadrant).

Figure 2. Knowns and Unknowns in Security Analytics
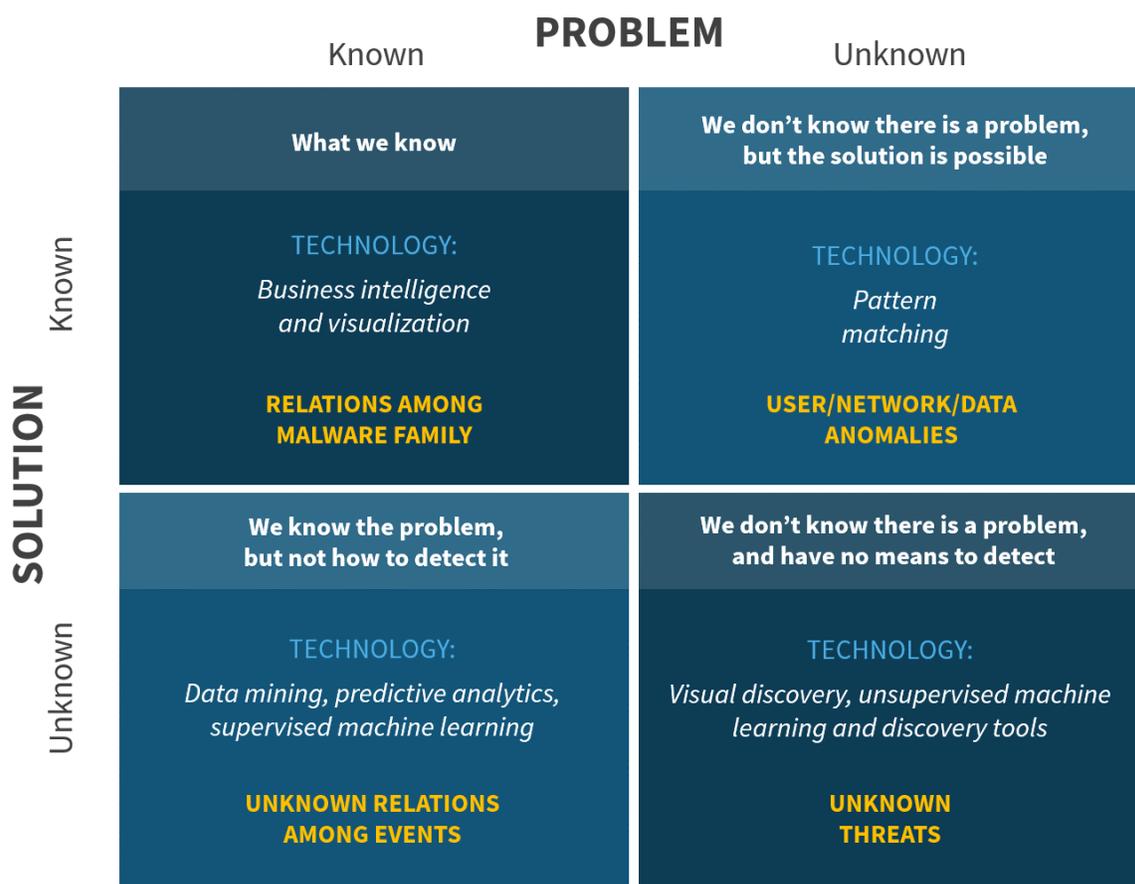
Source: Enterprise Strategy Group

Red Cloak Threat Detection and Response (TDR) Application

Red Cloak TDR is a software offering from Secureworks that extends the company's portfolio beyond its current MSS, consulting, incident readiness, and response offerings. It is a security analytics application leveraging Secureworks' extensive knowledge of the threat and known tactics employed. Red Cloak uses machine and deep learning to analyze extensive data across the IT ecosystem—in the cloud, on-premises, endpoints, network, and other vendor-inclusive sources. This data is enriched by crowdsourced threat and tactics intelligence, incident response (IR) expertise, and insights gathered from thousands of unique customer environments.

The key features of the Red Cloak TDR are:

- **Integrated Threat Intelligence** garnered through the Secureworks Counter Threat Unit research team.

- **AI-based Detections** to reduce the number of alerts and potentially detect threats that current tools miss.

- **Intuitive Investigation Workflows**, which Secureworks designed for its own team of investigators.

- **Enrichment of Alerts** to provide context to inform faster investigations.

- **Software-driven Response**, which automates containment and prevention actions predetermined by Secureworks' 20 years of investigation experience.

- **Endpoint Visibility** to assist in detection of adversaries by behavior alone with endpoint detection and response technology powered by behavioral analytics.

- **Automated Correlation** to provide event relationship across the security environment to corroborate a compromise.

- **MITRE ATT&CK Mapping** to align attacker activity with security alerts.

- **Ask an Expert Chat**, which provides the ability to hunt and remediate along with Secureworks experts or seek a second opinion from the Secureworks security team in real time if the customer is stuck during an investigation.

Tactic Graph Detectors for Behavioral Threat Detection and Response

A key differentiator of Red Cloak TDR is the use of a growing portfolio of advanced detectors, specifically the Tactic Graph Detector for behavioral threat detection and response. When signature-based systems fail, quick insight into adversary tactics are necessary to detect and disrupt advanced attacks before they put customer data, valuable intellectual property (IP), critical operations, and company reputation at risk. Adversaries often use the same tactics repeatedly, changing minor variables to avoid detection. In fact, as stated, there are millions of malware variants, but only a few hundred tactics that are commonly used. These tactics require time and investment to blend into benign activities and evade detection.

Red Cloak TDR software applies ML/DL to data gathered from Secureworks' 1,000+ incident response engagements each year, telemetry from the company's extended IT ecosystem, the MITRE ATT&CK Framework, and threat intelligence sourced from 4,000 customers. The Tactic Graph Detector discovers attackers based solely on ML/DL software to understand common tactics, behavior in other incidents, the attacker's goals, and rich contextual insights. This deeper level of contextual insight can also drastically reduce false positives as Red Cloak TDR can differentiate between malicious and benign behavior.

Red Cloak TDR leverages a library of detectors, including the company's exclusive Tactic Graph Detector, to spot advanced and unknown threats before they can cause damage. These detectors leverage Secureworks' crowdsourced insights into

tactics or behavior to recognize hidden threats based on a chain of events or behavior. This not only allows faster detection but also helps organizations stop attacks earlier in their lifecycle. It also challenges attackers' commonly used approaches, potentially forcing them back to the drawing board to create new and different tactics. When an adversary is pushed to recreate tactics, it hits them where it hurts: the wallet.

Platform Architecture

Red Cloak TDR is built for rapid innovation and is evolving into a platform-as-a-service with a broader set of applications and services. The platform can be purchased two ways: As a SaaS platform for use by an organization's internal IT security team or SOC. Or as part of a managed service—managed detection and response. Secureworks will continue to deliver a range of services—managed security services, consulting, incident readiness, and response.

The Secureworks Counter Threat Unit research team and IR teams have long sought to follow the 4Cs of threat detection and response: capture, codify, contextualize, and correlate. For Red Cloak TDR, Secureworks has captured and culled through 20 years of threat intelligence, operational experience, and IR engagements, and codified the resulting insights and threat data using machine-learning-based detectors, informed by Secureworks' knowledge of threat actor TTPs. Additionally, Secureworks' human analysts have added insight and analysis using behavioral playbook mapping. The telemetry is contextualized using real-world investigation insights from the company's deep bank of IR engagements.

Three delivery levels for Red Cloak TDR allow independent action by security analytics teams, partnership with Secureworks analysts on investigations, or outsourcing to Secureworks to perform analysis and investigation. Finally, the "Ask an Expert" function provides additional resources to help customers during an investigation irrespective of the delivery level.

The Bigger Truth

Threat detection and response is difficult because attackers are so often ahead of defenders, forcing organizations to upgrade security analytics and operations tools, skills, and processes to try to gain the lead. Security analytics and operations teams suffer a lack of experience, resources, and skills, and they work with disconnected point tools and manual processes. Utilizing SOAPA capabilities speeds analytics when combined with valuable threat data, advanced behavioral mapping, and additional human expertise. With these benefits, there is a greater likelihood of forcing the adversary to build new tactics, techniques, and procedures, which in turn increases their time to exploit. Secureworks Red Cloak TDR is built on SOAPA and intended to bolster the customer's human analysis strengths with software-based security analytics tools. Additionally, Secureworks brings 20 years of experience and crowdsourced threat data to inform behavioral detection for faster, more accurate prevention, detection, and remediation of advanced and unknown threats using data science.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

www.esg-global.com   contact@esg-global.com   P. 508.482.0188