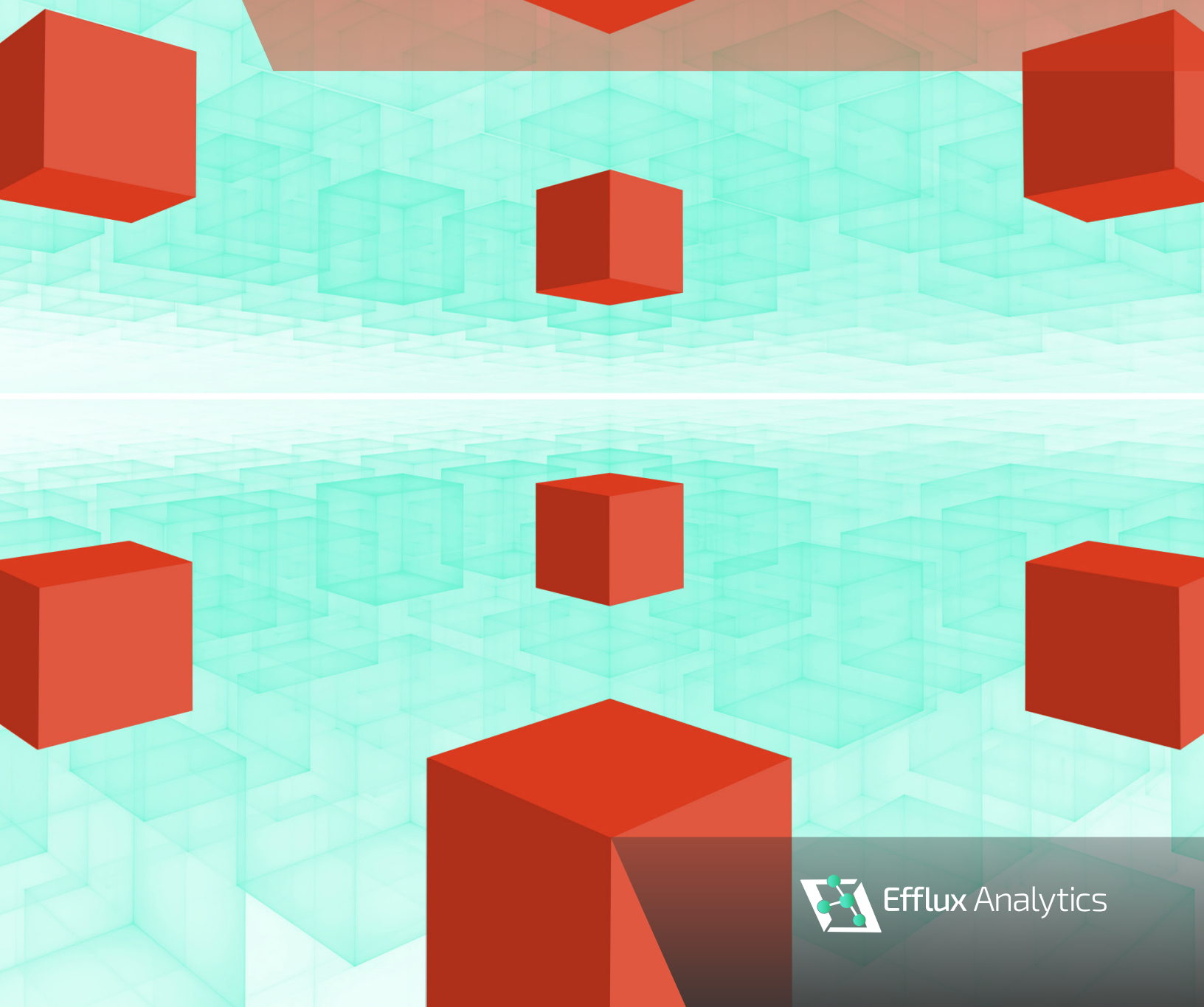
Security Automation Is Here



Efflux Analytics

Expectations of Cybersecurity Operations Are Maturing

History demonstrates that all industries go through a natural evolution from being driven by humans to being driven by machines and automation. Processes and production inevitably reach a point where automation becomes required to effectively and efficiently operate and scale. This evolution is out of necessity and a result of pressures related to factors such as volume, cost, time, and/or resource constraints. Manufacturing, supply chain, finance/accounting, HR and IT are examples of areas that have gone through this evolution. Air flight and now the move towards autonomous cars are also examples that resonate with all of us.

Over the last few years, cybersecurity has reached this breaking point as increasing volumes of alerts and resource constraints related to time, cost, and skilled security human capital are driving a requirement for automation in cybersecurity operations. Organizations are increasingly anticipating security automation to reduce the time needed to detect and respond to cyber threats. This move is becoming required to effectively and efficiently operate and scale security operation efforts. Like other business areas before it, cybersecurity operations are maturing and now increasingly being operationalized.

Security automation is a broad term and can mean different things to different people. Additionally, the different types of security automation can add confusion when talking to vendors about products and understanding how they fit into optimizing workflow. A key goal of this white paper is not only to provide context around why security automation is needed, but to also provide insights about the different types of security automation.

THE WHY: Multiple Security Pressure Points Driving Increased Focus on Security Automation

Over the last few years, cybersecurity has been cast into the spotlight as a result of the significant increase in cyberattack volumes, velocity, and damages. This has made cybersecurity top-of-mind at many large enterprises with cybersecurity achieving board level attention. Cybersecurity is being elevated within organizations with the CSO/CISO role increasingly moving outside of IT. Security is now rightfully viewed as a business and operational risk, not just an IT risk.

While the visibility and importance of cybersecurity is increasing significantly, so too are the pressures on security organizations and cybersecurity operations. For example:

- Attack volumes continue to increase. As more criminals are incentivised, this shows no signs of abating. Cloud computing, mobile, and Internet of things are continuing to drive the expansion of attack vectors.
- Alert overload remains a key challenge, and many security organizations continue to struggle with low signal-to-noise ratios. While showing improvement over the last few years, the time to detect and respond to threats remains suboptimal.
- Skilled security human capital, your most important resource, is hard to find, retain, and increasingly expensive. Security budgets continue to outpace other areas of IT, but risk calculations will force a limit in spending, requiring security teams to validate measurable value.

So like other business areas, including IT, pressures related to volume, time, costs, and resource constraints are forcing cybersecurity organizations to increasingly leverage automation. Security automation is quickly becoming a required element for security operations to become more effective at detecting and responding to threats and to scale continuous monitoring and response efforts. In short, cybersecurity is now being operationalized.

The Role of Security Operations

Before we delve into what security automation means, it's worth revisiting the basics of security operations. We utilize the broad term security operations because organizations of all sizes have security operations efforts. These range from large enterprises operating their own internal Security Operations Centers (SOCs) to smaller enterprises outsourcing security to Managed Security Service Providers (MSSPs). Throughout the rest of this whitepaper, the term SOC will be used to account for all types of security operations.

According to industry research firm Gartner, *"The traditional SOC provides device management and monitoring services for firewalls, intrusion protection systems, proxies, and other perimeter and preventative security technologies."*[1] In general, SOCs are focused on threat monitoring, investigation, and mitigation/response. The core technology used as the central nervous system of a SOC continues to be Security Information and Event Management systems (SIEMs). SIEMs represent an aggregation point for system logs and related data from multiple security and IT systems used by an organization.

1 Gartner - The Five Characteristics of an Intelligence Driven Security Operations Center – November 2, 2015

For the manager of the security team, be it an individual or a fully built SOC, there are three main roles within the SOC:

- **Tier 1 Analyst:** Monitors alerts and confirms events requiring further analysis.
- **Tier 2 Analyst:** Performs deeper investigation into events. Correlates and fuses data from multiple sources. Determines if an event is an incident that requires remediation/response.
- **Tier 3 Incident Responder:** Responds to and remediates security incidents, confirms scope of the intrusion and performs root cause analysis to prevent the attack vector used from being successful again in the future.

At a high level, SOCs key responsibilities are to monitor, analyze, and respond to cyber threats.

Not surprisingly, the need for SOCs to evolve is as constant and dynamic as the cybersecurity threat landscape. A few of the evolutions underway include:

The Quest for Increasing Visibility

This is occurring on several fronts. First, SOCs are deploying newer detection technologies to gain increased visibility into threats that are bypassing traditional, signature-based security controls. Second, SOCs are realizing that security and IT logs alone are inadequate for detecting and respond to threats. This is driving SOCs to invest in security analytics and enables them to gain greater context into network behavior, user behavior, and third-party threat indicators/intelligence.

A Drive for More Effective, Efficient & Rapid Analysis

Organizations are already overburdened with alerts and increased visibility adds to this challenge. The industry traditionally looked to SIEMs to aggregate, correlate, and prioritize security alerts. However, SIEMs were largely deployed for compliance and auditing purposes, and in many cases, have not been properly configured for threat management. While SIEMs have automated the collection and correlation of alerts, today's SOCs continue to be dependent on manual investigations to define the scope of an intrusion past the alerted host of interest. Tier 1 analysts spend the majority of their time combing through the SIEM alert queue to identify false positives and discover for the alerts that matter. Once an alert is deemed to be of interest (i.e. an event), a Tier 2 analyst conducts a manual investigation in which they look at multiple elements of context to gain a complete picture of a potential attack. Manual investigations are time consuming and imperfect. This is causing SOCs to seek out security analytics solutions that not only provide value-added context, but also enable automated SOC workflows for investigations. For example, a security analytics solution that provides post-exploit visibility can be automatically correlated with existing SIEM alert queues, resulting in reduced alert noise and increasing the overall SOC effectiveness and efficiency. Conversely, a security alert from a SIEM could trigger an automated investigation to determine if the issue behind an alert is limited to a single host.

The Need for Holistic Threat Response

Detecting a threat is important but as equally important is the ability to respond to the threat. The ability to respond to confirmed threats in a rapid and efficient manner is increasingly required. Given the various pressures SOCs are experiencing and a requirement for continuous incident response, it's no surprise there's increasing interest and usage of automated threat response capabilities.

The above represent just a few of the evolutions occurring within SOCs. A common theme is that SOCs are looking to improve not only the time to detect, but also the time to respond to cyber threats. Given the pressures on SOCs related to volume, time, cost, and resource constraints, it's only logical that cybersecurity operations are increasing their use of security automation. Cybersecurity is being operationalized.

THE WHAT:
Types of Security Automation

Security automation is a blanket term that means different things to different people. In fact, at a recent major cybersecurity conference, a network access control (NAC) vendor had a main message around security automation (say what?!). Given this, defining the different areas of security automation with the context of what works best in which scenario is key in understanding what type of security automation to deploy.

At a high level, security automation can be summarized into three main areas:

Workflow Automation

This is the automation of the typical day-to-day workflow of security analysts and incident responders. Think of this as process automation where disparate and disjointed manual processes (phone, e-mail, spreadsheets) are being automated and integrated. This is analogous to what occurred with IT help desk automation in the 1990s.

Automated Analysis

Historically, the analysis of a potentially meaningful security incident required a high degree of manual investigation and work by security analysts. Despite the widespread use of SIEMs, identifying actionable alerts and weeding out false positives still involves looking at multiple elements of context from different systems. Much of this process involved manual, mundane tasks that waste time and money. Today, SOCs are looking to automated analysis and investigation solutions to increase the efficiency and effectiveness of security investigations. Technologies in this area should focus not only on automating manual tasks, but more importantly on providing value-added context and analytics to enable more effective alert triage.

Automated Threat Response

This represents the ability to take automated countermeasures to respond to threats before data is exfiltrated. This includes deploying technologies that enable automated responses on endpoints and networks, as well as the development of security orchestration and automation solutions that provide "out of the box" and "custom" playbooks to enable automated response (i.e. confirmed malware attack, quarantine host, block IP at firewall, etc.).

The Emergence of Security Operations, Analytics & Reporting (SOAR)

Leading industry analyst firm Gartner is defining an emerging segment of the security market called Security Operations Analytics and Reporting (SOAR) platforms.

According to Gartner[2], "*A SOAR utilizes machine-readable and stateful security data to provide reporting, analysis, and management capabilities to support operational security teams. They apply decision-making logic and context to provide formalized workflows and enable informed remediation. In a nutshell, they provide intelligence that you wish you had in the original technologies.*"

Some of the key use cases Gartner indicates cybersecurity organizations should use SOAR technologies for include:

- Rationalizing the output of multiple security technologies
- Assessing the risk posture of assets using vulnerability, configuration, and other operational state data in asset, business and external contexts.
  Prioritizing security operations activities.
- Automating and enforcing remediation and response workflows.

Gartner indicates that the key benefit of SOAR solutions are they "*enable security operations teams to automate and prioritize security operational activities and report data to inform better business decision making.*" They also indicate that by 2019, 30% of midsize and large enterprises will leverage SOAR technologies to automate their security operations and make them intelligence-driven, up from 5% in 2015.

2 Gartner - Innovation Tech Insight for Security Operations, Analytics and Reporting – November 11, 2015

Security Organizations Are Expected to Operate Along the Spectrum of Security Automation

Like other business areas that have embraced automation, security automation is not an all or nothing proposition. Fully-manual and fully-automated processes represent extreme outcomes, and they will continue to operate with a mix as organizations embrace security automation.

Think airplanes. While today a lot of the operational processes involved in flying (i.e. takeoff, analysis of inflight conditions, landing, etc.) are automated, there continues to be a meaningful element of human interaction from pilots. Unless we are simply automating a mundane, repetitive, low-value process, the expertise and judgment of a skilled, human operator is required in many cases. Cybersecurity is no different, and the primary goal of security automation is to increase the effectiveness and efficiency of your scarce, skilled security human capital.

Security Automation Is Here

The use of security automation is quickly becoming a requirement for security organizations to be able to detect and respond to threats and to effectively and efficiently operate and scale cyber operations. It's becoming a requirement because of the significant pressures security organizations are experiencing related to volume, time, cost, and resource constraints.

We'll conclude with a summary look at how security automation is helping to alleviate each of these pressures.

Volume: Security analytics and automated analysis/investigation solutions are enabling security organizations to more effectively and efficiently conduct analysis on the increasing volume of security events and alerts. By leveraging automation, security analysts and incident responders can spend their scarce time dealing with the threats that matter.

Time: The volume of threats and alerts combined with scarce security human resources equates to pressures on the time to detect, investigate and respond to threats. By leveraging elements of security automation, organizations can improve SecOps workflow and achieve efficiencies of scale. Automated investigation and analysis solutions help organizations improve their ability to detect and confirm real threats. This results not only in more effective and efficient threat detection, but also in more efficient and effective incident response. Incident response focused organizations can leverage automated threat response capabilities to replace time-consuming and expensive manual remediation approaches. This enables them to scope intrusions through the discrete actions that must be taken to knock the attacker out of the environment.

Cost/Resource Constraints: Security budgets aren't infinite and skilled security human capital is increasingly expensive to acquire and retain. The adoption of security automation helps alleviate these pressures, enabling enterprises to better scale security operations. Security automation is not about replacing skilled security people with machines; it's about leveraging optimized threat detection, investigation, and response capabilities. Optimizing the current investments (technology and people) already made in your security organization efficiently scales your operations and response, and effectively reducing risk.

Automation is already rapidly evolving cybersecurity defense capabilities. It's now up to organizations to exercise it against serious cyber threats.

About Efflux Analytics

Efflux Analytics is a security operations solution that detects lateral movement on your network and automates analysis, correlating threat activity in near real-time. Its common uses are visibility for SecOps optimization, post-exploitation triage, and hunting threats inside of networks. Efflux Analytics cuts through the noise of alerts, so your security team can focus and respond faster to more threats that matter.

Learn more or sign-up for a demo at Efflux.io.

Efflux Analytics