STATE OF SECOPS IN 2020

The demand on security operation teams is growing exponentially. With shifts of entire platforms to the cloud, more sophisticated hacking systems coming out daily, and an increase of deployed security tools to defend, data breach and cyber-attack threats are rolling in at unparalleled rates.

As SecOps teams are an organization's first line of defense, it is their job to manage these threats, unpack the real alerts from the meaningless, and operate at a lightning speed to meet the demand. If a SecOps team is not up-to-date and diligent with their day-to-day, year-to-year operations, it can leave vulnerabilities exposed in dangerous ways.

To help better understand the State Of SecOps today, in this article, we will take a look at some recent SecOps reports from Micro Focus, Sumo Logic, and SaltStack, unpack each organization's findings, and give some insightful tips on security operations in the future.

Micro Focus State of Security Operations

Published in July of 2019, Micro Focus released a "2019 State Of Security Operations Update" that discussed trends and success factors, with real-world examples.

Opening the report stating that, "4.1 billion compromised records exposed in more than 3,800 publicly disclosed breaches in just the first six months, 2019 is on course to be a record-setting year for data breaches." With that, it is immediately clear that the state of SecOps is in unprecedented territory.

Combining years of information from over 150 discrete security operation centers, with more than 200 assessments in 12 months, in over 33 counties, Micro Focus uses this detailed 2019 SecOps analysis to address its 5 key findings.

1. Employing and securing SecOps professionals is a growing challenge
   Building a team that is reliable and there to stay is the first measure any organization should want to achieve. If a SecOps team is protecting the most valuable information, having top talent will greatly increase security. However, as the only problem, there is a big gap in trained, skilled professionals, creating a "war" of sorts.
   The report quickly points out that, "Given the industry-wide shortage of skilled security professionals, some companies are reporting that other organizations are luring their trained security professionals away. It's a lamentation we've heard echoed across industries and geographies as the talent shortage continues." SecOps is now a game of the best salaries, benefits packages, and tools provided to the professional--which leads us to the next point.

2. Investing and budgeting for SecOps is an increasing battle of costs
   A huge hurdle that any organization needs to face is how to secure proper funding to support SecOps teams. With the economic downturn of 2020, this is now more of a focus than it was before. "The struggle around budget has led to increased pressure to cut costs, with outsourcing being one of the outcomes. In a recent study, 60 percent of SOCs reported that they outsourced SecOps functions for the cost savings."
   As outsourcing might be the answer, the report also mentions that beyond looking to reduce salary, actually implementing processes will ease the current team's load.

3. Process and procedures of SecOps teams are lacking
   Finding that some of the most outstanding SecOps teams have reliable, continuously improving processes, Micro Logic stresses the need to implement procedures that improve accuracy and reduce team workload. "Without the solid foundation that processes and procedures provide, SOCs become reliant on the tribal knowledge of individual "superstars" and are less predictable in the results they produce. The lack of defined processes could also impact the accuracy of operational metrics and increase the risk of not meeting business or contractual obligations around service levels."

4. AI and machine learning could lighten the load
   Understanding that the future is automation, the implementation of AI and machine learning seems to be the tools SecOp leaders are looking forward to. Helping to alleviate the stress of not having enough trained professionals, technology could also reduce the risk of human error. However, Micro Focus urges that these tools are only effective if proper foundations and processes are in place first.

5. Clarity and direction of what is being protected by SecOps Teams is lacking
   Closing out the report with a topic that can so easily be overlooked, Micro Focus finds that "Many of the SOCs we spoke with more recently either did not have a defined mission or had not communicated it to staff and other departments. Often this meant that there was a lack of visibility and understanding of which business assets (users, applications, data, intellectual property, and so on) were the most important for the SOC to protect." A troubling understanding, it is clear that SecOps teams in 2020, especially those with huge workloads, require clear and defined direction.

Sumo Logic State of SecOps and Automation

In June 2020, Sumo Logic in partnership with Dimensional Research released a "2020 State of SecOps and Automation" report. Essentially a survey of 427 top IT security professionals, each survey was taken from employees at companies with over 1,000 staff members and significant investment in IaaS.

Releasing staggering statistics and findings, the report focuses on numbers to drive home the incredible changes and challenges happening in the SecOps industry. Sumo Logic's 3 key findings unpack what SecOps teams are currently struggling to manage. Please note that all numbers and bullet facts come from the report directly.

1. Operational issues of SecOps teams begin with the sheer volume of alerts.

- 70% have more than doubled the volume of security alerts in the past five years
- 99% report that high volumes of alerts cause problems for IT security teams
- 56% of companies with more than 10,000 employees deal with more than 1,000 security alerts per day
- 93% cannot address all security alerts the same day
- 83% say their security staff experiences alert fatigue

2. The future of AI and Machine Learning automation will positively impact alert load, but it hasn't shown help yet.

- 65% of companies have only partially automated security alert processing
- 65% of teams with high levels of automation resolve most security alerts the same day
- 92% of companies agree that automation is the best solution for dealing with large volumes of alerts
- 75% report they would need three or more additional security analysts to address all alerts the same day

3. In order to control the alert load, technology improvements are needed.

- 88% have challenges with their SIEM
- The top issue reported with existing SIEM solutions is the high number of alerts
- 84% see many advantages in a cloud-native SIEM for cloud or hybrid environments
- 99% would benefit from additional SIEM automation capabilities

SaltStack State of Xops

As Q2 2020 came to a close, SaltStack published a "State Of Xops Report Q2 2020 SecOps." Focused on unveiling how successful IT and security teams operate effective SecOps teams, using the help of an independent market research team, in January 2020 they surveyed 130 verified InfoSec and IT leaders.

Identifying 1 key finding, SaltStack focused on where SecOps teams can become stronger. Please note that these numbers are taken directly from the report.

1. Communication of security and IT, with a direction of desired outcomes.

- 54% of security leaders say they do not communicate with IT professionals

- 45% of IT professionals say the lack of communications makes their job hard
- 70% of both security and IT managers say their company sacrifice data security for faster innovation
- Most companies surveyed agreed that a major data breach would cost $707,000

Tackling bigger jobs than ever before, if communication between these teams is not inline, there is a higher risk of exposed vulnerabilities. SaltStack closes by saying, “The SecOps mantra must be to integrate security operations teams through collaboration and automation. The objective is clear - truly secure digital business by achieving consensus, fixing issues, and securing infrastructure.”

SecOps in 2020 and Beyond

Through the examination of these three reports, we see that SecOps teams are taking on bigger tasks and more sophisticated attacks without the proper tools or procedures in place to ensure safety. Implementing strong communication and clarity while focusing on what the teams need will help to reduce the risk and improve budget concerns. Investing in security that is reliable will end up saving countless organizations hundreds of thousands of dollars; therefore, it is not something that should be left struggling or overlooked.