VERITI

HOW TO GET THE MOST OUT OF YOUR SECURITY TOOLS

VERITI.AI

ARE YOU RECEIVING THE LEVEL OF SECURITY YOU PAID FOR?

Every day, thousands of new strains of malware and other threats hit the web, creating a perfect storm in the worst possible way. At this point, there really isn't much you can do to stop yourself from becoming the target of a hacker out there with malicious intentions. What you can do, however, is prevent yourself from becoming a victim of a successful attack, which is what those security tools you've invested so heavily in are all about.

11% ANNUAL GROWTH RATE OF THE CYBERSECURITY MARKET

Gartner predicts organizations spent $172.5 billion on cybersecurity-related tools in 2022 alone. That number is anticipated to grow to $267.3 billion in 2026

Some tools even do exactly what the description on their cover says. Sometimes the letters are just too small to read, and you can't tell if the products you have bought are indeed worth the hassle of deployment, implementation, integration, hours of training, and gaining knowledge about their best practices (not to mention their actual ability to lower the likelihood of business disruption). Ultimately, it all sums up to a simple question: Are you receiving the level of protection you paid for?

> *As per the experts at Forbes businesses of all types saw an increase of* ***more than 50%*** *when it came to the volume of cyber attacks that they were facing in 2021 compared to one year prior.*

A MATTER OF CERTAINTY AND EFFICACY

Fear of the next security breach does not ensure maximum protection. The exercise of the business checks-and-balances system will always limit its fortification due to the fear of impacting business applications. To create a balance between maximum security and business uptime, security teams need to gain vigilance of their own threat landscape and complete visibility of the actual value each solution brings to the overall security posture. It is the only way to achieve cyber certainty when preventing cyberattacks.

Every organization should adjust the security controls based on ongoing assessment of existing threats and security gaps. But this kind of efficacy is hard to attain as every additional security solution deployed increases the operational overhead and tips the scale in favor of using default or inadequate security configuration to keep business continuity. So how can organizations have the cake and eat it too?

INCREASE THE ROI OF YOUR SECURITY TOOLS

TRADITIONAL ROI CALCULATION

There are several ways to calculate the ROI of security products. They all start with monetizing the risk/risk reduction and the direct and indirect cost of every planned purchase. Chief among these is the idea of "single loss expectancy" (otherwise referred to as SLE for short). This is the overall reduction in value that an IT system would see from an individual threat or cybersecurity instance. Along the same lines, you have the "annual rate of occurrence" (ARO for short) to deal with the total number of times you anticipate a cyber event or related incident in a single calendar year. We can calculate the "annualized loss expectancy" (otherwise known as the ALE) by multiplying the SLE by the ARO. Here, this deals with the total monetary loss that you will incur for these types of cyber incidents. According to the latest data breach report by IBM and the Ponemon Institute[1], the cost of a data breach in 2021 was US$ 4.24 million which explains the grave need to procure the latest security solutions and the ROI it allegedly brings, or monetary loss it saves for every organization.

THE INDIRECT COST

30% of security leaders say they can’t hire enough staff to handle the workload[2]

The resources each product requires to maximize functionality are getting more expensive, so the indirect cost of every solution purchased is getting higher. This is why most organizations don't have a choice but to rely on vendor default configurations, resulting in a potentially inadequate security posture with inherent security gaps. To reduce this cost and improve the ROI of the point solutions deployed in the organization, you must first automate the process of security configuration optimization, and implement zero-business-disruption verification procedures.

35% of security leaders say they can’t find staff with the right skill[3]

Automated processes augment operations, security, and risk management teams' effort to obtain more efficient security/operating procedures e.g.:

- Automating the root cause analysis and employing machine learning and optimization playbooks to verify the organization is getting the total value of its security configurations will augment the security team's ability to improve the overall security posture.
- Reducing the amount of false positive events throughout the entire security estate, security operation teams will be able to speed up their investigation, identify high-risk events, and improve the overall MTTR dramatically
- Automating the risk assessment and providing change management for all churn of required actions from discovery through triage until remediation and validation of changes allow efficient security and risk management with minimal operational overhead and potential business disruption.

You don't need to reinvent the wheel or devise new methods for calculating the ROI to justify your latest cyber purchases. All you need is to adopt a consolidated approach, automate repetitive manual tasks, and gather security postural insights so you can restore the balance between business uptime, security posture, and the human effort to maintain them.

[1] IBM and Ponemone Institute – Cost of a Data Breach Report, 2021

[2] SPLUNK – The state of security, 2022

[3] Ibid

VERITI UNIFIED SECURITY POSTURE MANAGEMENT

Veriti's unified security posture management platform integrates with the entire security estate to maximize security and the ROI on the deployed solutions while ensuring business uptime. Veriti eliminates the unnecessary complexity and operational friction in managing multiple cybersecurity solutions by proactively identifying security gaps, misconfigurations, and false positive events and providing the root cause and means to remediate them before they occur. This allows security teams to improve the organizational posture, focus on tasks that require discretion and let Veriti's unique machine learning algorithms and automated processes cull unnecessary information until the needle finally shines through the haystack.

90%

IMPROVEMENT IN ROOT CAUSE ANALYSIS TIME

using automatic, predictive, and trailing analytics

87%

IMPROVEMENT IN MTTR

by eliminating false alarm events before any manual analysis

63%

IMPROVEMENT IN ENTERPRISE SECURITY POSTURE

without deploying new security tools

REDUCE MEAN TIME TO RESOLUTION

The latest IDC research on handling alerts in today's cybersecurity practice, states that 63% of security professionals tend to tune policies to reduce the alert volume or ignore certain types of alerts when there are too many alerts to process.[4]

With the inherent complexity of investigating multiple security sources and the over-abundance of security logs to analyze and alerts to scrutinize, there is no wonder the turnover rate of security staff is growing every year.

If your existing cybersecurity tools are telling you that you've had a breach and then, after five hours of investigation, you learn that you were dealing with a false positive, that is an unfortunate chunk of time where more important work wasn't being completed. False positive alerts contaminate every cybercrime scene with irrelevant noise (not to mention the collateral business impact each one of those events holds). They only serve to disrupt business uptime and increase investigation times without yielding much in the way of new information, meaning they should be eliminated or at least reduced whenever possible.

20%

average security staff turnover rate, as reported by senior decision-makers across the US[5]

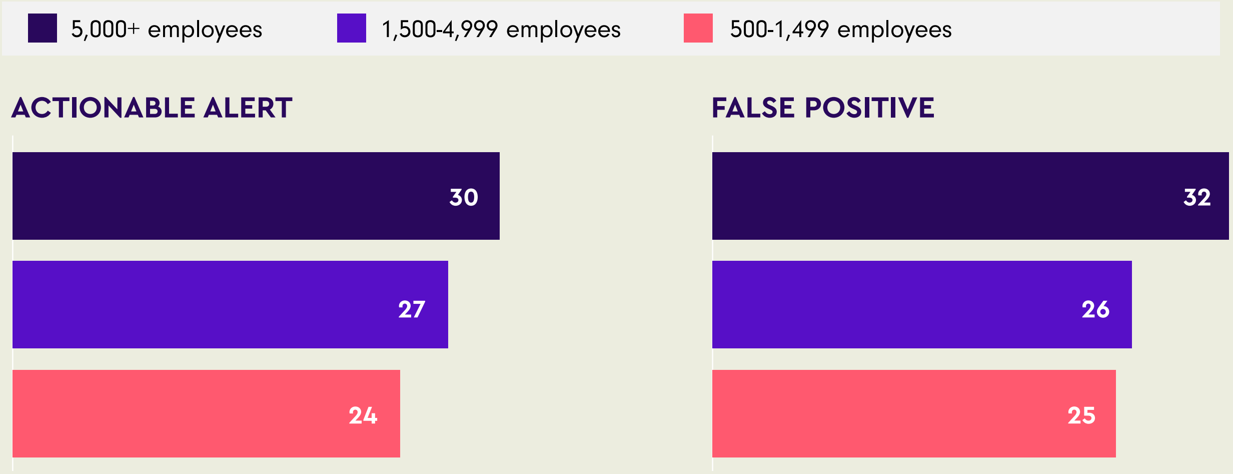
[4] IDC, The voice of the analysts, 2021

[5] https://www.prnewswire.com/news-releases/cybersecurity-burnout-the-critical-risk-for-organizations-to-address-in-2022-threatconnect-research-301466507.html

With Veriti security teams can proactively identify and remediate business disruption events such as false positive anomalies in near real-time, saving hours of trial and error. Based on machine learning algorithms (continuously analyzing traffic direction and repetitive patterns) and threat intelligence enrichment, Veriti generates actionable insights, carrying the exact root cause and the relevant remediation steps, even before the end user opens a ticket regarding an application downtime.

TIME REQUIRED TO INVESTIGATE FALSE POSITIVES AND ACTUAL ALERTS[6]

Q. How much time does it typically take for your team to investigate the following types of alerts?
(minutes required to investigate false positives and actual alerts)



AUTOMATE SECURITY INVESTIGATIONS

If cybersecurity feels something like trying to hit a moving target, that's largely because it is - the threat landscape is continuously changing. The cyber noise is getting louder and more diverse, and chances are slim that security operations will be able to keep track of the new vendor exploit patch (before two more take its place) or take care of all security alerts on time. To overcome the common alert fatigue that can lead to missed cyber detections and is a driving factor for low job retention, security organizations are implementing automation processes to enhance their investigation capabilities.

Veriti's unique integration with security vendors leverages APIs and rich telemetry to drive automated investigation and find the root cause of cyber incidents, security gaps, or business disruption anomalies. For every potential risk or actual incident, Veriti automatically generates insights and triages them based on the risk they pose to the organization, saving hours of manual analysis and helping engineers identify issues in minutes. All insights are enriched with threat intelligence feeds and include remediation instructions that can be triggered automatically or via existing organization processes.

[6] IDC - In Cybersecurity Every Alert Matters

[7] https://www.forbes.com/sites/edwardsegal/2021/11/08/alert-fatigue-can-lead-to-missed-cyber-threats-and-staff-retentionrecruitment-issues-study/

MAXIMIZE EFFICACY

VENDOR CONSOLIDATION

With the growing complexity of the security portfolio, it is getting harder to manage the security posture of the entire organization. If the risk management team has pivotal information about a new threat, but there is no visibility if the necessary change was applied successfully by operations and what the business implications were, there is not enough information to determine if the organization is safe. The fragmented, siloed infrastructure makes it hard for engineering and infrastructure teams to maintain, adjust and scale existing solutions. It also increases the investigation time due to the excessive amount of consoles and data sources the security operations team needs to handle.

The need for a management platform that provides an integrated set of capabilities across a range of security solutions is undeniable. Veriti Unified Security Posture Management platform breaks down all data silos and synthesizes all security solutions to create a single data and control plane. All log records, system and security telemetries are consolidated and correlated with internal/external intelligence feeds and security controls to provide actionable insights. These insights cover all aspects of cyber incidents' lifecycle, from proactive to reactive investigations, with root cause analysis and remediation instructions.

Cybersecurity investment will pay more dividends when using a unified platform consolidating all security solutions, dashboards, and policies into a single location to minimize management overhead and increase collaboration across the different security teams.

Cybersecurity investment will pay more dividends when using a unified platform that consolidates all security solutions, dashboards, and policies into a single location to minimize management overhead and increase collaboration across the different security teams.

HOLISTIC VISIBILITY AND SECURITY HYGIENE

organizations must prioritize security-hygiene vigilance for the entire solution portfolio to maximize the efficacy of the deployed solutions. This set of practices is crucial to staying ahead of cyber threats. To achieve better cyber resiliency, security teams need to monitor the health of each one of the security solutions, verifying they are up to date and ensuring they are correctly configured to protect the organization.

Veriti provides complete visibility and continuous monitoring across the organization's distributed, hybrid security infrastructure to answer the growing demand for a streamlined, cohesive platform. Data regarding the preventative maintenance level of security assets, the different security configurations required for each, and their current exposure level to threats are collected to determine the criticality degree of security events and the modus operandi to remediate them.

Once visibility is gained, security teams can easily manage their entire security posture from a single location holistically from the technological, business operations, and security practice perspectives with better efficacy and faster MTTR.

What would typically require a large team of Subject Matter Experts (in-house or through an MSSP) and a significant amount of time, Veriti provides at a fraction of the cost, helping IT, Risk, and infrastructure teams to better manage, monitor, and optimize the security posture of the organization. Automatically.

[8] Gartner, Emerging Technologies. Top Trends in Security for 2022