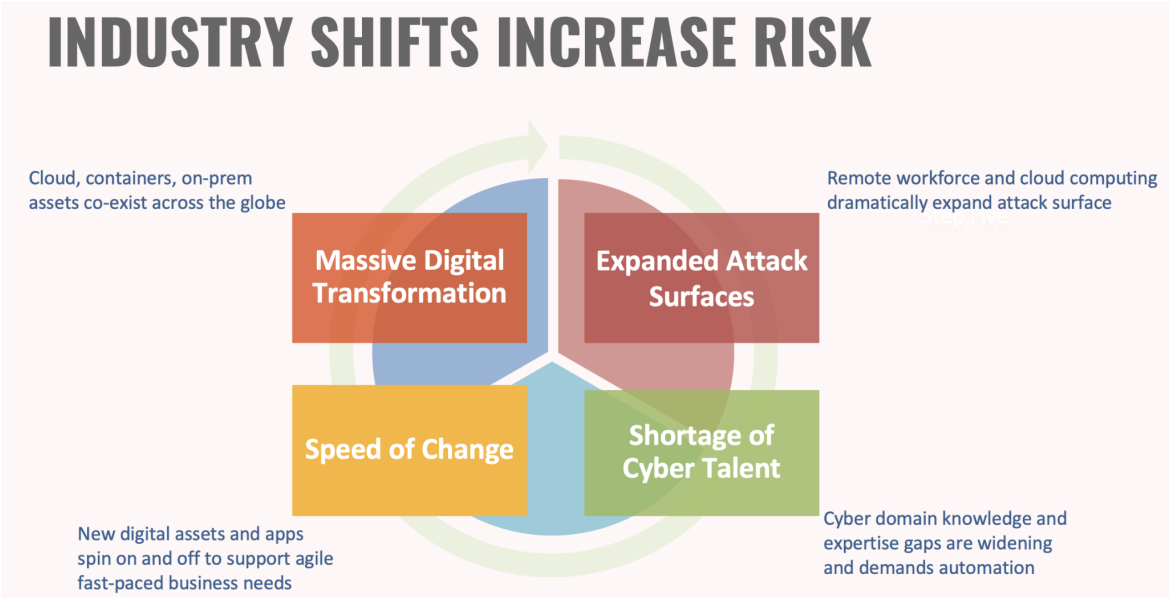
Cyber Exposure Management

Introduction

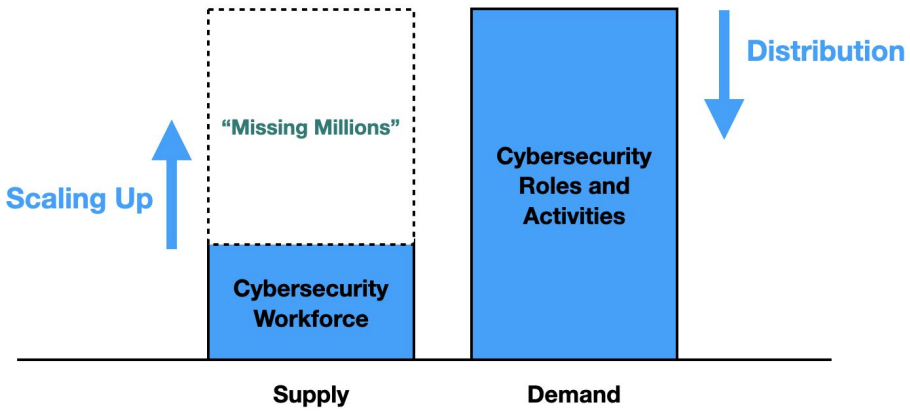
Criminals are becoming more sophisticated and aggressive by the day, and security teams are increasingly under-resourced, dealing with a barrage of risks and potentially facing unwanted digital assets exposure. A cyber attack in the U.S. occurs every 39 seconds. The attacker's focus is shifting to leveraging vulnerabilities to infiltrate organizations' infrastructure. In IBM's 2021 X-Force Threat Intelligence Index, vulnerabilities surpassed phishing as the most common attack vector - exploiting vulnerabilities (35%), surpassing phishing (31%) for the first time in years. Recent attacks on the Colonial Pipeline and SolarWinds have placed a greater spotlight on the issue as companies rapidly brace to protect their digital infrastructure.

Cybersecurity leaders need to adopt a new approach. One that centralizes all risks and provides a decision framework to illuminate the most significant risks and direct the effort of the team to address the most critical risks first. The way organizations manage this exposure is already undergoing a radical and rapid transformation. This paradigm shift is exacerbated by continuously evolving changes to infrastructure, supporting a remote workforce, budget restructuring, and other business, compliance, and security drivers. Not to mention a rapidly expanding attack surface that goes well beyond the scope risk managers are used to managing. Adopting automation and modern technologies like artificial intelligence and machine learning makes this transition more manageable than ever before. Knowing the best path forward will aid organizations in managing their risk exposure to their digital assets.



Source: NopSec, Inc.

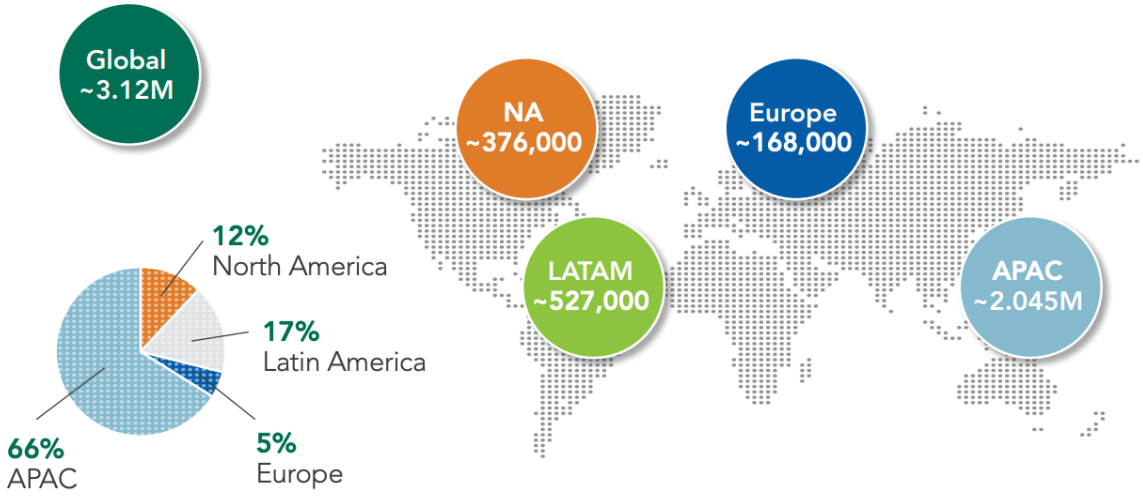
Investments in cybersecurity are at an all-time high. Although there is a rapid increase of new entrants into the industry, public and private sectors in the U.S. face a common problem—a chronic shortage of skilled workers. 360,000+ American jobs remain unfilled, according to a 2020 survey by a cybersecurity training nonprofit called (ISC)2. Worldwide, the cybersecurity gap remains at 3.1 million. More entry employees are selecting careers in this high-demand industry. In addition, we are witnessing mass migration of the existing workforce is transitioning from other disciplines to address this gap. Despite this large influx of labor, the overwhelmingly large gap remains.



Source - The Actual Cybersecurity Workforce Challenge

The Cybersecurity Workforce Gap by Region

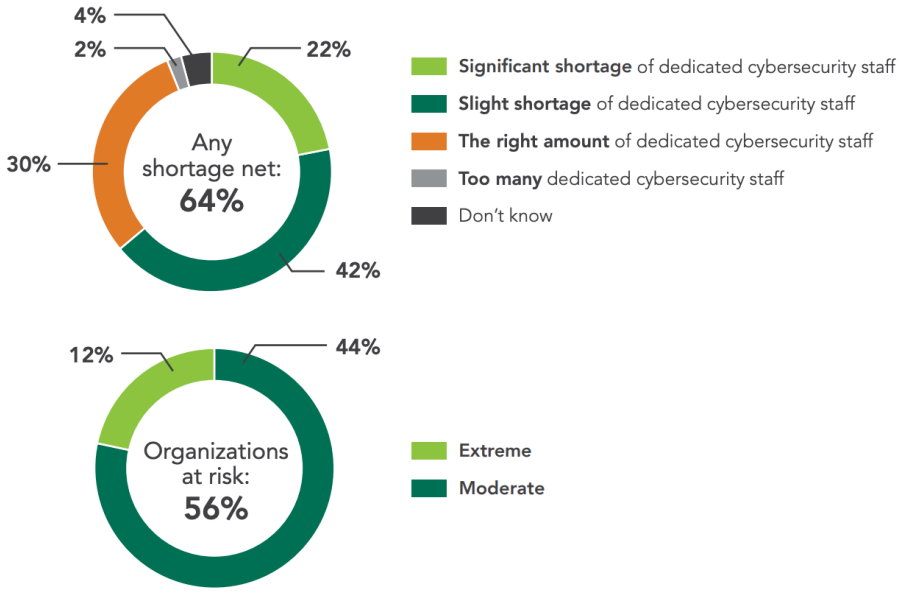
The global gap in the cybersecurity workforce varies by region, dominated by a gap of more than 2 million in the Asia-Pacific region.



Source: [2020 survey by a cybersecurity training nonprofit called (ISC)2]

Cybersecurity Staffing Levels and Security Risks

Cybersecurity professionals report staff shortages at their own organizations, and security risks that spring directly from those shortages.



Source: [2020 survey by a cybersecurity training nonprofit called (ISC)2]

“If You Can’t Measure It, You Can’t Improve It.”
-Peter Drucker

The scariest thing about cybersecurity is that an alarmingly large number of organizations are still not fully aware of which assets are connected to their environment. How could a security team possibly reduce their exposure to attacks if they don’t know what needs to be protected in the first place?

First, let's define what an asset and attack surface is. An asset is any hardware or software within your organization’s IT environment. It includes but is not limited to servers, networks, desktops, smartphones, tablets, laptops, virtual machines, cloud-hosted technologies & services, web applications, and IoT devices.

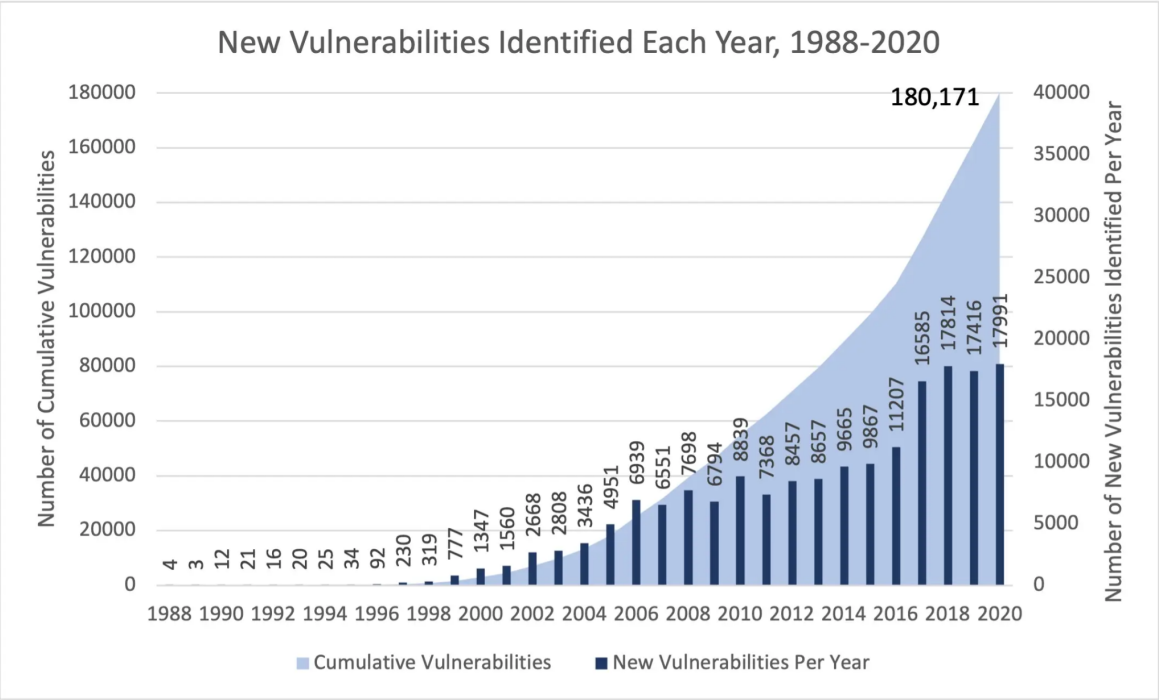
An attack surface is the total number of points/vectors through which an attacker could try to enter your IT environment.

A point-in-time vulnerability assessment is an excellent start to understanding risk and how it impacts assets in your environment. However, these static approaches, along with traditional vulnerability management programs, miss giant chunks of asset inventory leaving weak points in your assessment. In addition, a point-in-time assessment only captures vulnerabilities when periodic scans are run, which means the picture at any one time is only a single snapshot of the past. To further exacerbate this, point-in-time assessments do not cover many non-CVE risk items such as password reuse, misconfigurations, user behavior, and many more use cases (see Mitre ATT&CK for a comprehensive list). This makes managing your attack surface increasingly difficult and ultimately exposing you to threats that could have a significant financial and operational impact on your organization.

Vulnerability tools natively don’t understand the compensating effect of deployed security controls as part of their approach. Mapping vulnerability metrics to business context cannot be achieved using the traditional methods that have been utilized over the past two decades.

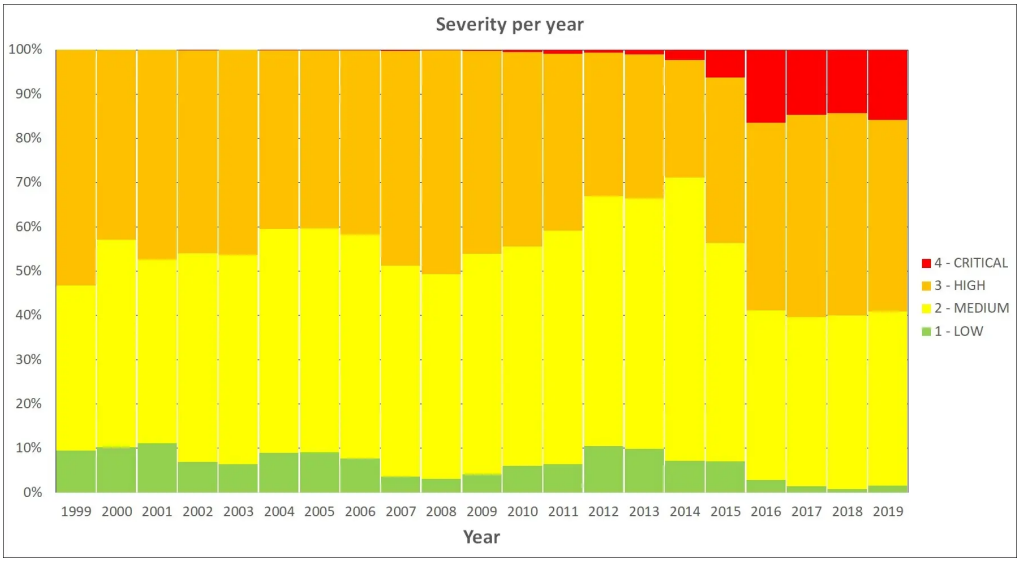
In addition to the technical constraints, the frequency of scans is inadequate to keep up with the rapidly increasing sheer volume and criticality of today’s vulnerabilities.

The diagram below shows exactly what over 30 years of vulnerabilities looks like. They are piling up as each year passes.



Source: IBM

In addition to the increase in volume, so is the severity.



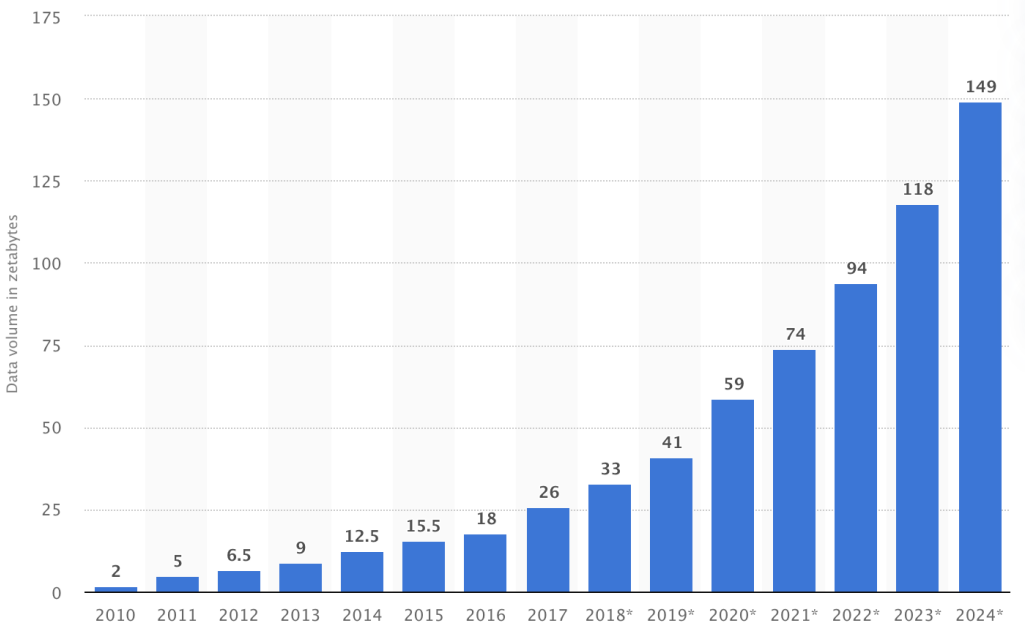
Source: IBM

The Data Problem

Data volumes are rapidly expanding, so this problem will only multiply exponentially. Between now and 2024, the volume of data that will be created, captured, copied, and consumed worldwide will

double in size. Embracing the use of cloud provider services like data lakes and SaaS will make life easier. Relying on these services provides slightly less control, but it is very much worth the trade-off when working with a small team with the added advantage of very minimal overhead.

The volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024 (in zettabytes)



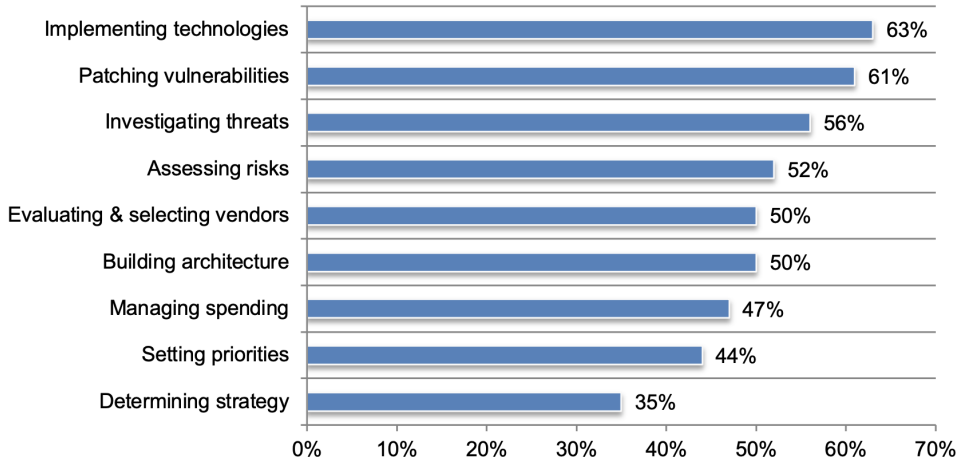
Source: Statista 2021

Aggregating security log data from vulnerability scanners and prioritization platforms gives you an easy way to analyze all the vulnerabilities in your network. This is important not only to meet compliance mandates, but also to keep network attacks at bay. Organizations need to prioritize the collection of logs that have security value to ensure that time and resources are used efficiently. This can be a particularly important challenge to overcome early on as analyzing a number of data sources can quickly become very noisy, irrelevant, and can take up unnecessary space and cycles. It is equally important to normalize and extract indicators so proper actions can be taken to respond and recover from security incidents. Another challenge that can arise is that the duplication of data can cause the amount of repetitive data to multiply out of control. Over two-thirds of organizations use more than one vulnerability scanning solution (Gartner). If the results of these tools are not properly deduplicated in an efficient and automated manner, SOC Teams could very easily find themselves overwhelmed.

Patching vulnerabilities, investigating threats, assessing risks, and setting priorities are all key cybersecurity roles in the SOC. All of these responsibilities are inundated with repetitive manual

tasks that produce less than results. These are all areas that would significantly benefit from a streamlined solution built on automation.

Figure 2. Which of the following best describes your cybersecurity role?
More than on response permitted

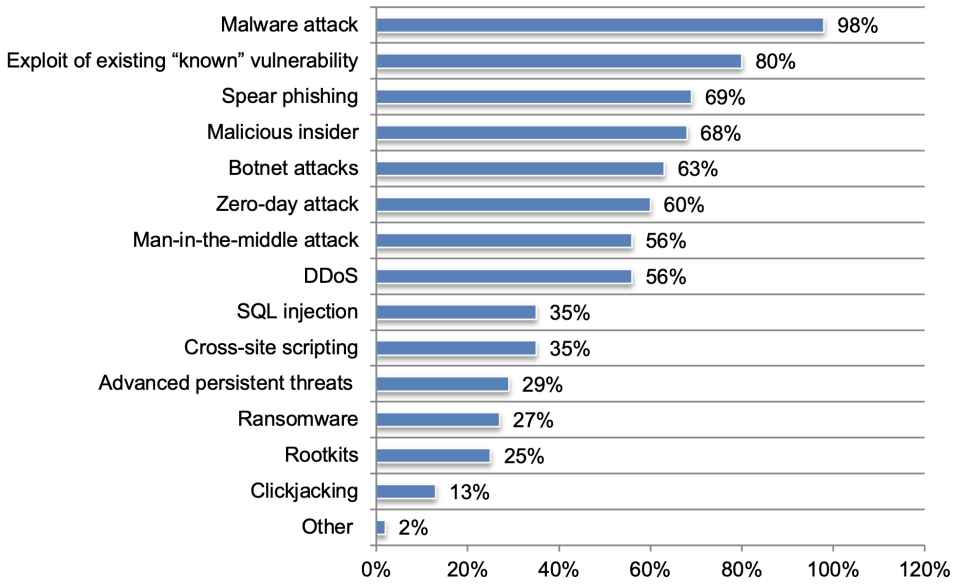


Source: Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center

Prioritization

Identifying what vulnerabilities need to be remediated is only part of the equation. At the same time, deciding on what to remediate in what priority order is another part of that equation and is arguably the most difficult to achieve. In the research below, findings identified that over 80% of SOC teams had exploits or compromises from existing "known" vulnerabilities in the past 12 months. Put simply, if they had proactively patched the vulnerabilities they already knew about, they would not have had the security incident that exposed their organization to unnecessary risk. This emphasizes the fact that SOCs need to invest in prioritizing their remediation efforts and reducing the time it takes to patch the vulnerabilities in their environment.

Figure 6. The exploits or compromises the SOC has identified over the past 12 months
More than one response permitted



Source: Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center

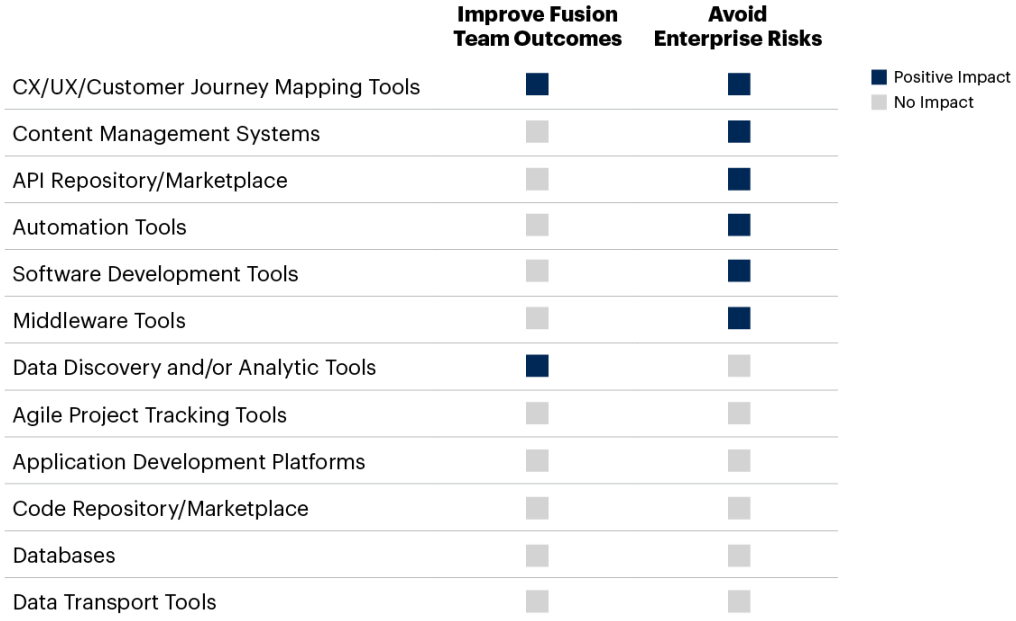
Organizational Dysfunction

Operations teams are still operating in silos, with security teams often being wholly isolated on their own deserted island. But why do these silos still exist? The common excuse is that the security team needs to prevent access to certain sensitive records and therefore requires its own tools. There is simply no need for today's organizations to run separate tools or even separate processes, whether to manage incidents, changes, configurations, or any other functions in this day and age. Despite this, the challenge still persists.

The root of this problem stems from organizational structure and stakeholder ownership. Organizations do not need to restructure their organizational chart to make this possible; they just allow security to develop over time as a more natural part of the cycle. As time goes on and this type of structure proves its worth, you can put a more permanent organizational structure into place. Having a streamlined process in place with combined tooling teams can standardize and automate their workflow and mature their collaboration. Ultimately significantly improving their performance metrics and reducing their exposure to risks.

The industry is moving in the right direction as over 84% of organizations have built at least one Fusion Team, which Gartner defines as 'cross-functional teams that use data and technology to achieve business outcomes.' The benefits of this approach are increasing in popularity as well as its collective utility.

Using IT-Recommended Customer Tools Helps Organizations Avoid Risks
Impact of Fusion Teams Using IT-Recommended Tools



n = 994 fusion team leaders
Source: 2019 Gartner Digital Business Teams Survey
Note: Enterprise risk is the likelihood of fusion teams having to rework or retire a digital solution due to information risks such as data breaches and cybersecurity threats.

712778_C

Gartner

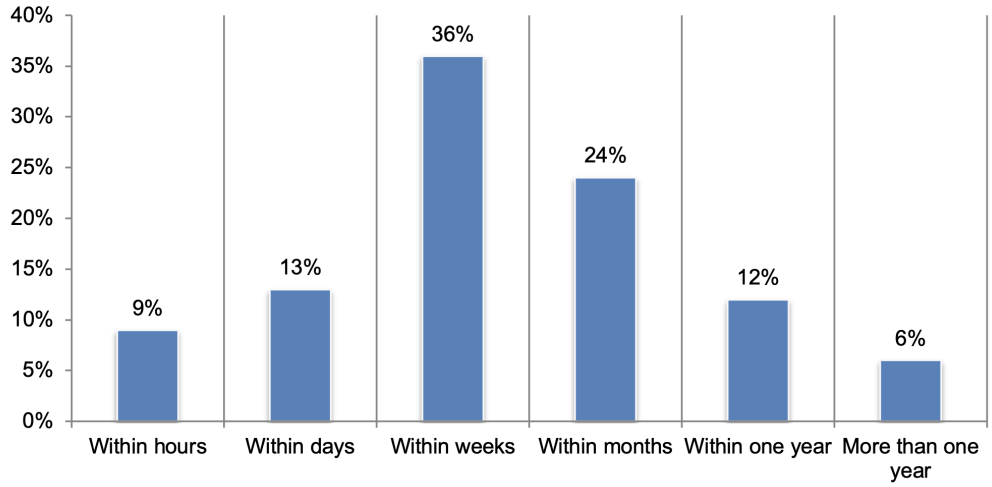
Source: Gartner

Chaotic Workflows

According to IBM's Cost of a Data Breach Study, the average total cost of a data breach is $3.86 million globally and $8.64 million in the United States. On average, it takes 280 days to identify and contain a breach. This is a heavy price to pay for not replacing legacy technology and an outdated approach.

According to a recent SANS Incident Response (IR) Survey, 14% of firms indicate that the time between compromise and detection is between 30 to 180 days. Of those that detected an intrusion, nearly 10% said it took up to 90 days to contain. Over 42% state it takes months to over a year to resolve a threat.

Figure 7 On average, what is the MTTR for a security incident in your SOC?



Source: Ponemon Institute's research into [Improving the Effectiveness of the Security Operations Center]

Every environment is different, and as a result, requires a different set of needs for detections. Teams need the ability to create custom-tailored rules that can be properly tested, versioned, and programmatically managed in version control. The more upfront investment and automation made into this approach will determine when the return on investment is realized and by how much as each day goes by.

Lack of Metrics

Organizations don't typically calculate their mean-time-to-patch (MTTP), which means they do not know the fraction of time they spend exposed. If a patch is not released in an emergency, it is generally scheduled in the next maintenance cycle, which on [average is between 60 and 150 days].

So, how do you know whether your patch management program is successful or not?

To answer this question, you should have the following key performance indicators (KPIs) available:

- Target MTTP along with historical performance over time
- Number of unpatched vulnerabilities by elapsed time and severity
- Level of effort spent patching (e.g., hours spent or Full-Time Employee percent allocation)
- Financial costs associated with vulnerabilities being exploited by attackers

The Overall Picture

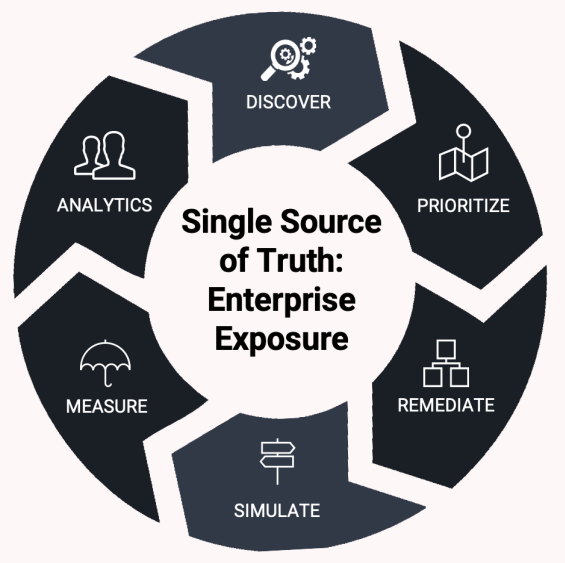
Business Impact Analysis (BIA) is often performed using subjective metrics such as “high,” “medium,” or “low” rather than in financial terms. Therefore, CISOs and security teams need to do a lot of manual work to gather information from multiple reports and different tools to calculate their overall cyber risk. Many organizations don’t even try because the mountain is so high to climb.

Vulnerability assessment and management is one of the essential functions of any enterprise security program. It is so critical that it can make or break the security of an organization. Before exploring the nuances of what constitutes an effective vulnerability management program, it is essential to understand what we mean by vulnerability management - and it goes far beyond just basic patching.

Considering all these factors provides security teams with a platform they can rely on to effectively address risks by fixing the vulnerabilities that have the most significant impact on reducing the attack surface available to hackers. Knowing what to consider and what questions to ask is the first step in efficiently tackling cybersecurity.

What is Cyber Exposure Management?

Introducing Cyber Exposure Management (CEM) - CEM is a novel way to holistically address the entire lifecycle of the core elements required to discover, prioritize, remediate, simulate, measure, and analyze risks to your specific operational environment.



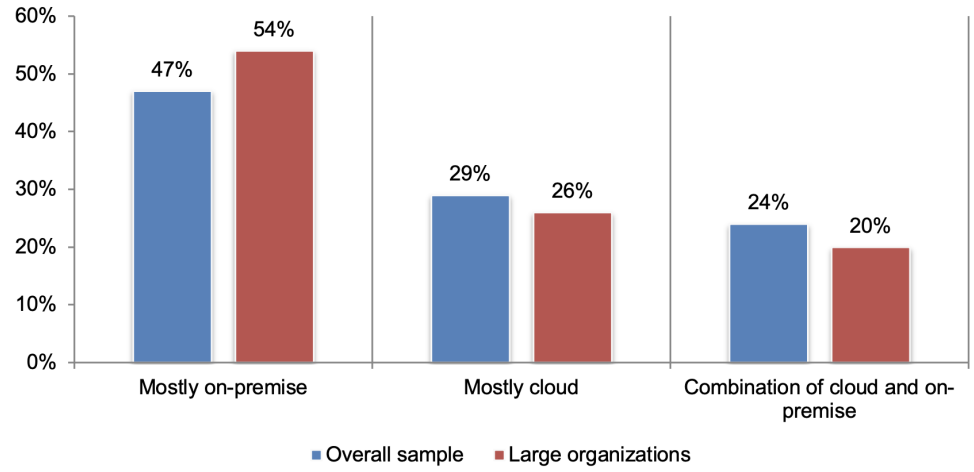
Source: NopSec

This Requires Complete Digital Risk Visibility Into…

- The aggregated external and internal attack surface
- 360-degree asset visibility, business impact, and criticality
- Topology, policies, and segmentation of network infrastructure
- Security control identification, simulation, and validation
- Prioritization of uncovered attack vectors
- Automation at machine speed to reduce friction, risk, and time to remediate

***Special Note:** Cyber Exposure Management has some overlap with an adjacent solution, segmented as Cloud Security Posture Management (CSPM), in that they both address vulnerabilities in cloud environments. CEM differs from CSPM because it is infrastructure agnostic and is not limited to only the cloud and is fully dynamic and continuous, where CSPM is static. CEM is ideal for organizations with a hybrid infrastructure and requires a continuous automated solution to identify and reduce risk exposure.

Figure 3. What best defines the IT infrastructure that houses your SOC?



Source: Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center

Data Aggregation

Modern SOC teams need to have the ability to have visibility across their entire ecosystem. This includes being able to collect data up and down the stack to get as much context as possible to include but not be limited to cloud, container, asset, configuration, network, database, host, and application data. By prioritizing the collection of logs that have security value, ensure that time and resources are used efficiently. This can be a particularly important challenge to overcome early on as analyzing a number of data sources can quickly become very noisy, irrelevant, and can take up unnecessary space and cycles. By using a modern approach, SOC teams can unify islands of

technology and data streams to more efficiently and effectively reduce their threat exposure. With this updated model, SOC teams can cut out the noise and focus solely on an actionable shortlist of priorities that are backed with high fidelity. This data synthesis takes the guesswork out of data planning and provides serverless scale and real-time detection and alerting, improving key security metrics like Mean Time to Patch (MTTP) so organizations don't can worry less about Mean Time to Detect (MTTD), Mean Time to Investigate (MTTI), and Mean Time to Respond (MTTR).

Reduction of hay

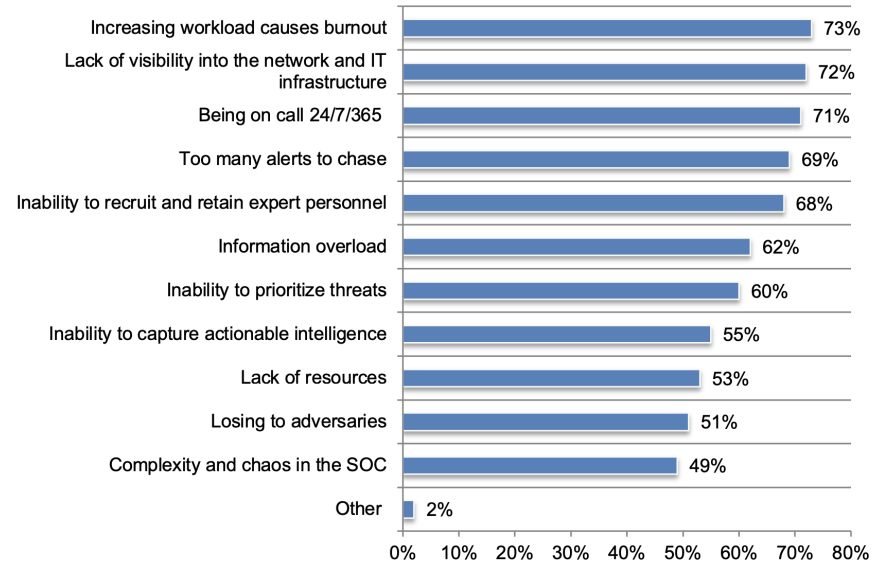
Despite the benefits, most cybersecurity solutions are easy to deploy, maintain and manage. Modern security tools such as Extended Detection Response (XDR), Security Information Event Management (SIEM), and Threat Intelligence Platforms (TIPs) often use a data lake structure and cloud analytics to centralize events. This enables security teams to narrow down events that need the most attention. Effectively finding the proverbial needle in a haystack.

The value and effectiveness of using these cybersecurity best practices are highly dependent on the sources of data it has access to and how well it has been architected, tuned, and maintained. Over the years, the industry's approach has been to keep piling on more "hay." The challenge with this approach is that it often generates false positives and too many alerts, which results in alert fatigue, or apathy, about alerts which leads to high-priority threats being ignored. This can cause critical incidents and even data breaches to go unnoticed much longer than ever intended. In many cases, this lapse can cause dire fiscal and reputational consequences.

According to Dimensional Research's 2020 State of SecOps and Automation survey, 92% of organizations agree that automation is required to address the growing number of alerts, as well as the high volume of false positives. Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center revealed that, on average, security personnel in U.S. enterprises waste approximately 25% of their time chasing false positives because security alerts or indicators of compromise (IOCs) were erroneous. The report also highlighted the need for security operations center (SOC) productivity improvements, citing that security teams must evaluate and respond to nearly 4,000 security alerts per week. Still, 65% of organizations use only partially automated alert processing, and 75% would need no fewer than three additional security analysts to deal with all alerts on the same day.

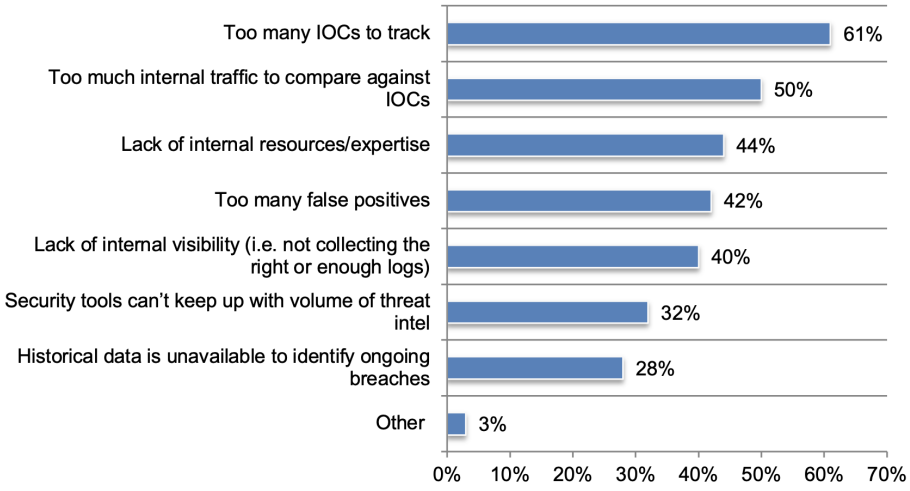
The 2020 Dimensional Research survey on the State of SecOps and Automation found that 70% of enterprise security teams have seen the volume of security alerts they have to manage more than double in the past five years, while 83% say their security staff experiences "alert fatigue." For those teams with higher levels of automation, handling the higher levels of alerts today is easier, 65% of those teams with high levels of automation stated they were able to resolve most security alerts during the same day, compared to only 34% of enterprises where low levels of automation are in place currently.

Figure 16. what makes working in the SOC painful?
More than one response permitted



Source: Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center

Figure 20. What challenges does your threat hunting team face?
Three responses permitted

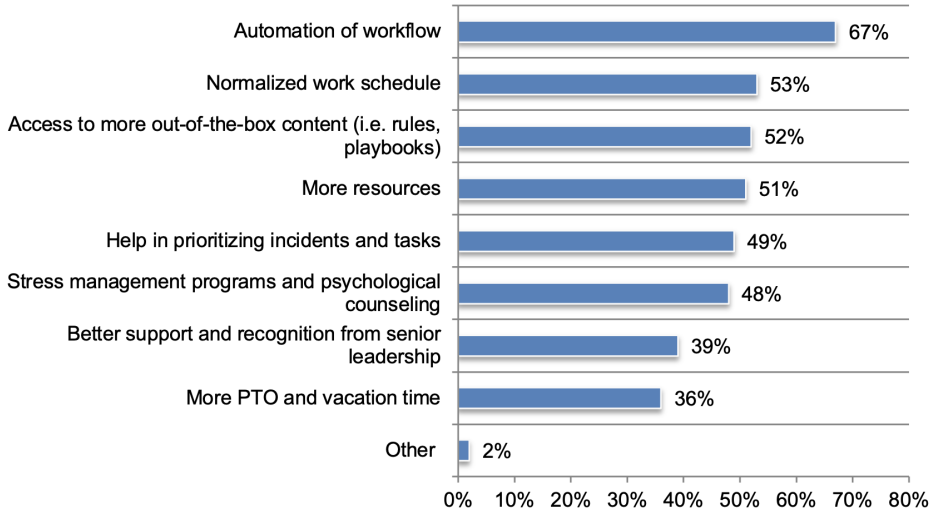


Source: Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center

Automation

In order to achieve a well-oiled SOC machine, it requires a balanced investment in people, process and technology in order to be successful. The ask is crystal clear, backed by research from Ponemon, SOC teams need help prioritizing their work, streamlining their workflows, and incorporating automation into their daily lives. Delays in meeting these demands have resulted in a mental health crisis and overall resentment for their leadership. By leveraging technology to do the heavy lifting, processes can be streamlined and alleviate the burden on the people that are ultimately responsible for the security and operational health of the business.

Figure 18. What steps can be taken to alleviate your SOC team's pain?
More than one response permitted



Source: Ponemon Institute's research into Improving the Effectiveness of the Security Operations Center

Continuous Improvement & Due Diligence

Just like any effort, it is paramount to measure your progress. Modern solutions have built-in real-time reporting functionality that allows operators and stakeholders to be informed about the operational readiness of their organization at any given moment. This enables them to evolve their maturity level to re-evaluate their Service Level Agreements (SLOs), Service Level Objectives (SLO), Key Performance Indicators (KPIs), as well as other measurable metrics that can be utilized to exceed business objectives.

Where is the Market Headed?

Teams need to rapidly figure out how to do more with less. 20 years ago, organizations could go days or even weeks without ever seeing a single attack on their infrastructure. Now there are multiple every second. Mindless machines methodically recon the internet for weak points that can be exploited. By 2025, enterprises will have to contend with an environment where they have to battle multiple data breaches at once. So what was once something that makes the newspaper's front page today will now be a new norm for organizations around the world.

Knowing this growing threat is coming near, organizations are investing in cybersecurity at unprecedented rates. Investments in technology that reduce risk exposure are currently at double-digit growth, resulting from risks highlighted during the global pandemic crisis. These investments include but are not limited to solutions that identify and reduce attack surface weak points, prioritize and remediate more efficiently, allow teams to collaborate more effectively, and improve their overall operational readiness to minimize the likelihood and impact of a data breach.

Best Practices

Simple checklist:

1. Attack Surface Management - Discover and manage organizational asset inventory
2. Risk-Based Vulnerability & Configuration Management - Prioritize what is important for your specific organization
3. Security IT Operational Workflow & Collaboration - Automated Remediation
4. Risk Simulation & Attack Emulation - Gamification to improve operational readiness
5. Security Program & ROI Reporting - Measure key metrics and drive results
6. Risk is everyone's responsibility - Leverage synergy across IT Operations and Security

Summary

Security operations teams will get the most out of the investment of their money, time and resources by implementing modernized Threat Exposure Management best practices for the newly revolutionized world.

This goal will not be achieved without the right focus and embracing a new mindset. The challenges highlighted in this publication highlights significant challenges that do not bode well for setting a SOC up for success. Still, the research also suggests organizations can consider the following actions to make the first positive steps.

1. Address Analyst Burnout - Challenges in the cybersecurity industry have contributed to the global challenge that is becoming known as the "Great Resignation." Leaders face a mandate to reduce the stress and pain of working in the SOC. The inability to have enough experienced security analysts will prevent organizations from improving the SOC. The number one recommendation from respondents is to automate workflow.

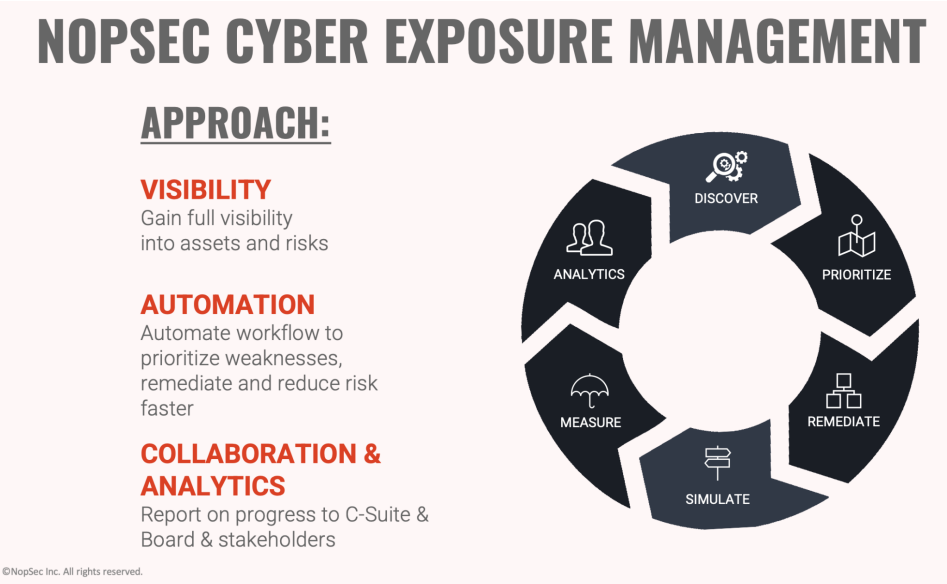
By paying attention to these basic needs, leaders will foster a more successful SOC and a stronger security posture.

2. Team Alignment - Often, the needs of the business and the needs of the SOC are in alignment – everyone wants to eliminate threat exposure, but not at the expense of an oversubscribed budget. Leaders need to tear down the organizational walls and silo issues between the Security and IT Operations Teams. This will improve the overall morale of the organization and be realized in tangible ROI in both operational efficiency and effectiveness as well as in financial impact.

3. Support Your SOC with a Modern Approach - Don't wait for a negative impact before dedicating larger budgets toward people, process and technology. By making legacy approaches obsolete and adopting a modern approach will enable organizations to gain full visibility into their business ecosystem, be able to prioritize what is truly important to their environment and work as an effective team to eliminate risk to their business assets.

Next Steps

NopSec operates with one mission - to help people make better decisions to reduce security risks. The NopSec Team is passionate about building technology to help customers simplify their work, manage exposure risks effectively, and empower them to make more informed decisions. NopSec's software-as-a-service approach to Cyber Exposure Management offers an intelligent solution to dramatically reduce the turnaround time between the identification of critical vulnerabilities and remediation.



- **Discover**
  - **Attack Surface 360:** External Attack Surface Management
  - **Managed Detection:** Managed Vulnerability Assessments
- **Prioritize**
  - **IT Asset Prioritization:** Asset Inventory & Prioritization
  - **RBVM Core:** Infrastructure Cloud & Endpoint Risk-Based Vulnerability Management
  - **RBVM Container:** Container RBVM
  - **RBVM Config:** Configuration Hardening
  - **AppSec AVC:** Application Vulnerability Correlation
- **Collaborator**
  - **Collaborator:** ITSM Ticketing Automation
  - **InControl:** Compensating Control Validation
  - **Defender:** Patching Remediation Automation & Orchestration
- **Simulate**
  - **Risk Simulator:** What-if Scenario Analysis
  - **KillChain Emulator:** Visualize & Validate Kill Chain
  - **ThreatForce:** Threat Intelligence Aggregation & API Service
  - **Managed Pentest:** Managed pentest services
- **Measure**
  - **PowerIntel:** Executive Metrics & ROI Reporting
  - **Full Stack Insight:** Full Stack Program Insight & Analytics
  - **TeamRed:** 3rd Party Pentest Aggregation & Metrics
  - **VendorRisk:** 3rd Party Vendor Risk Metrics

Learn how to manage your exposure to threats and request a demo today.

Schedule a Demo Today!