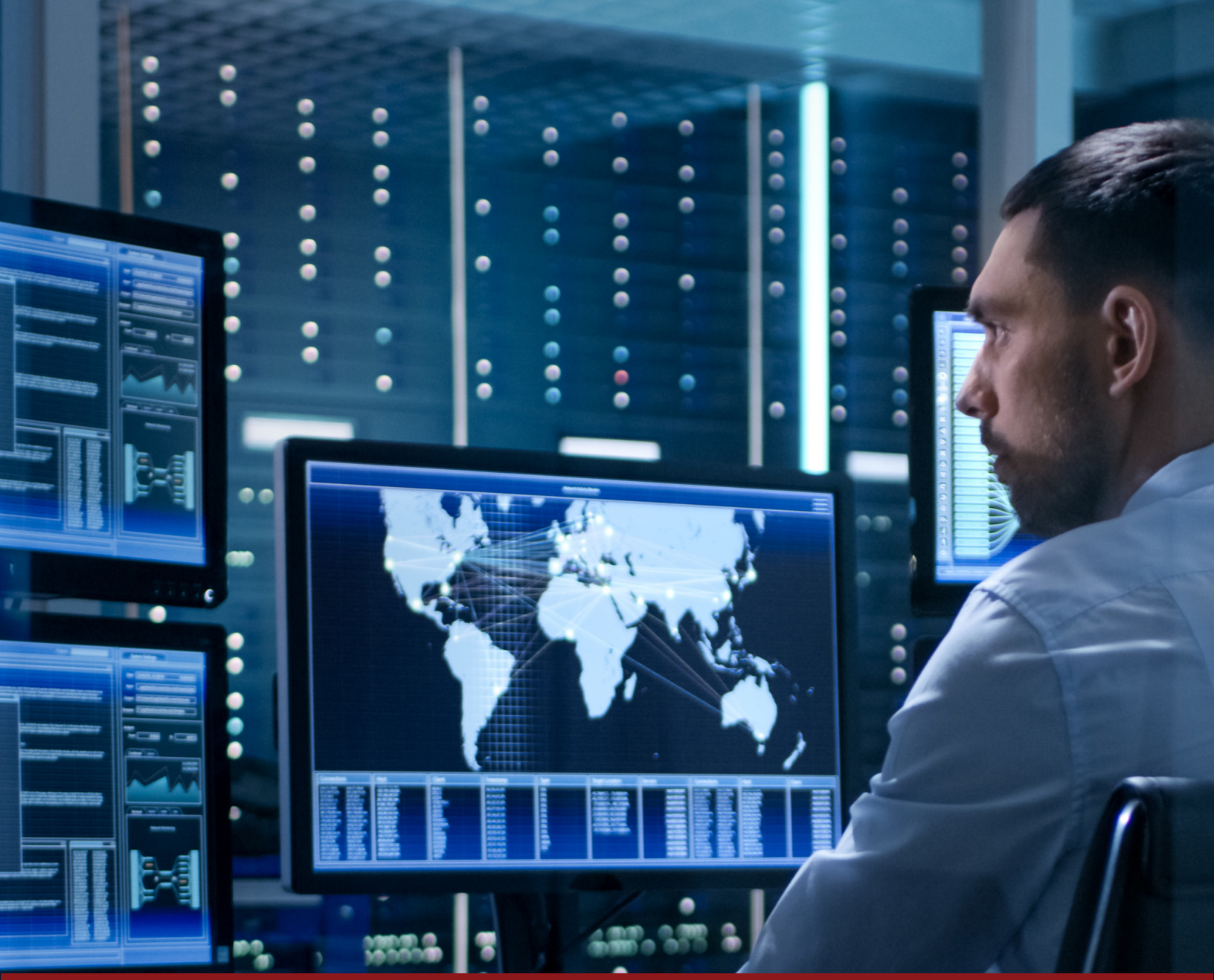


# The Critical Elements of Improving the Effectiveness of a Security Operation Center

secure OPS

So many articles and blog posts have been written on SOCs, how they are structured, what their mission and purpose is, and of course how to improve their effectiveness. There is so much good thinking out there, but the recommendations and ideas are difficult to implement, contrast with one another, and are sometimes even difficult to even understand. The goal for this brief will be to start with the fundamentals, how the SOC should work, the responsibilities of the analysts and their technology, then move into what we think are actionable recommendations to improve how your SOC performs.

## What is a Security Operations Center?

Let's start with what a Security Operations Center and how it executes a Computer Defense Network (CDN) strategy given the evolution of hackers, cyber-attacks and malware since the true birth of the current SOC in the 1990's.

Principally, a Security Operation Center (SOC) is a centralized function within a company that leverages IT security people, processes, and technology to monitor and improve an organization's security while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Today's SOC is essentially the hub which collects log data from across an organization's IT infrastructure, including its networks, devices, appliances, and databases and other IT assets across geographies. The increase of advanced threats makes collecting data from diverse sources critical, as each piece of data may provide insight into malicious behavior on the network.

**Cybercriminals Are Deploying Successful Attacks More Often than Ever**

Here is one real issue we'll be addressing in this brief - most SOCs, unfortunately, have difficulty keeping cybercriminals—even the unsophisticated ones—out of the organization. SOC analysts and other IT Security professionals are defending against sophisticated and constantly evolving malware, nation-states with hundreds of hackers, insider threats and worst of all, poorly trained employees who fall prey to phishing attacks.

*Phishing is the leading cause for data breaches, accounting for over 90% of attacks.*

*"An attacker only needs to be right once, an analyst and their tools must be right thousands of times."*
*– Quoted by every analyst everywhere*

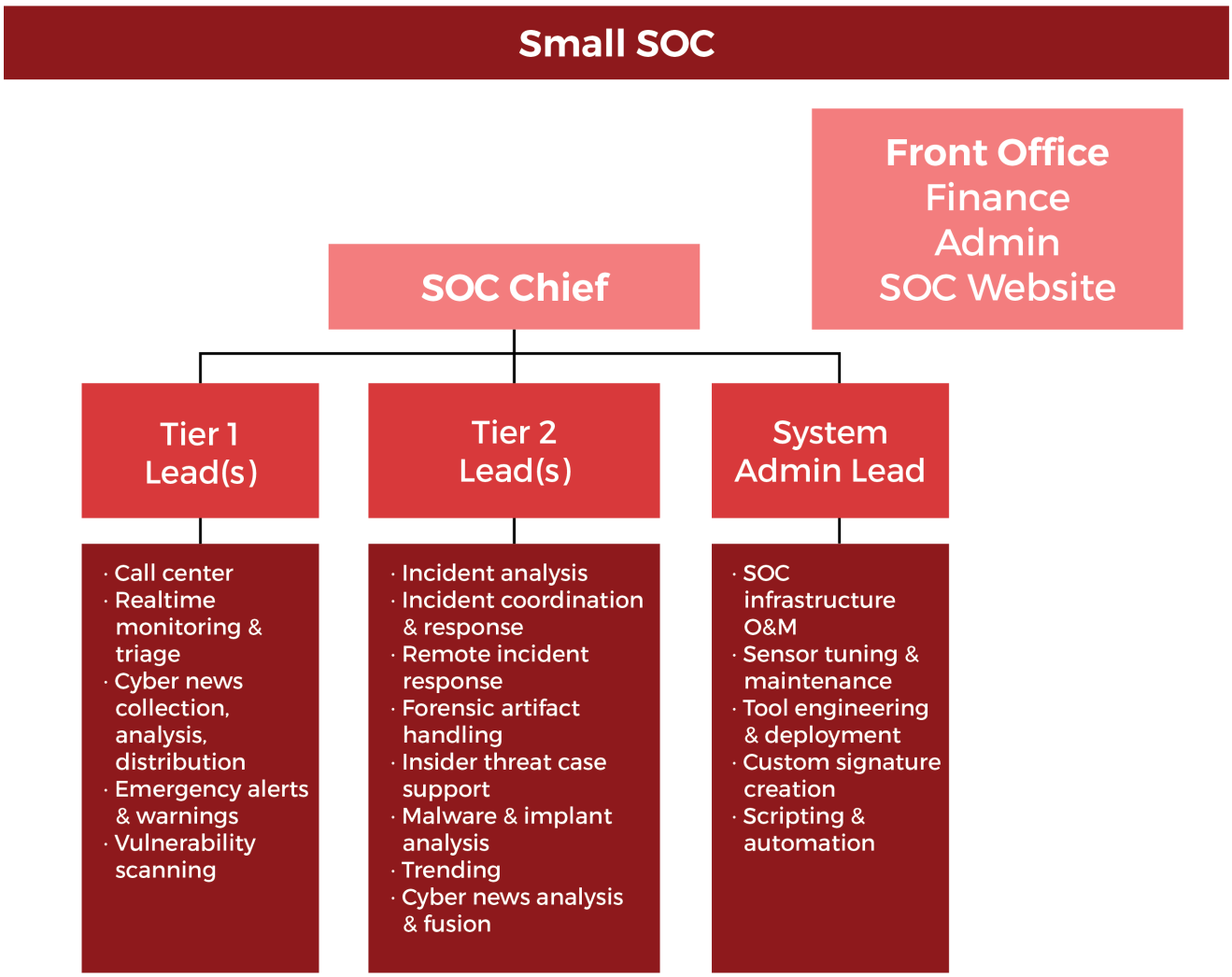
As we consistently hear in the IT security industry, criminals need to find only one way in while the good guys in the SOC must defend countless ways in, limit damage, and most difficult of all, find and remove the malware or malicious code that infiltrated the systems.

## Defining a Security Operations Center

Fundamentally, the responsibility of the SOC is to defend against unauthorized activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and remediation responsibilities. Professionals in the SOC - particularly incident response professionals and teams have been given a variety of titles and acronyms so let's list them out so you know who everyone is, they include:

1. Security Operations Center (SOC)
2. Cybersecurity Operations Center (CSOC)
3. Computer Security Incident Response Team (CSIRT)
4. Computer Incident Response Team (CIRT)
5. Computer Incident Response Center (CIRC)
6. Computer Security Incident Response Center (CSIRC)
7. Computer Emergency Response Team (CERT)

The SOC is usually led by a SOC manager/chief, and may include incident responders which we listed above, SOC Analysts (levels 1, 2 and 3) who could be threat hunters and incident response managers. The SOC reports to the CISO, who in turn reports to either the CIO or directly to the CEO.



## Small Security Operations Center Staffing

Smaller SOCs, in the range of five to 20 people, often find a relatively simple approach to arranging their staff. This is because with few people, there is comparatively less diversification of roles and there are few positions that don't involve full-time analyst work. A typical small SOC will include two or three sections:

1. **Tier 1** - Analysts often perform routine duties such as watching IDS or SIEM consoles, collecting cyber intelligence, and handling calls from employees in the organization as well as partners. As a note, how well tuned is the SIEM, the IDS's, the data feeds? Are the alerts unified into one or more SIEM dashboards, or are they split among half a dozen disparate tools? We'll talk about this critical issue.

2. **Tier 2** - Analysts who often handle in-depth analysis on incidents passed to it by Tier 1 such as log and PCAP analysis, and coordinates response to events incidents with colleagues in the SOC and partners such as MSSPs.

3. **System Administration** - Maintains SOC systems and sensors, which may include engineering and deployment of new capabilities.

## Large Security Operations Center Staffing

A large SOC on the other hand can support an organization with an advanced set of capabilities and clear separation of roles and responsibilities, for example:

1. **Tier 1** – Tier 1 is very similar to a small SOC; again, these are analysts who focus on fielding phone calls and catching real-time alerts and warnings in the SIEM or other sensor consoles.

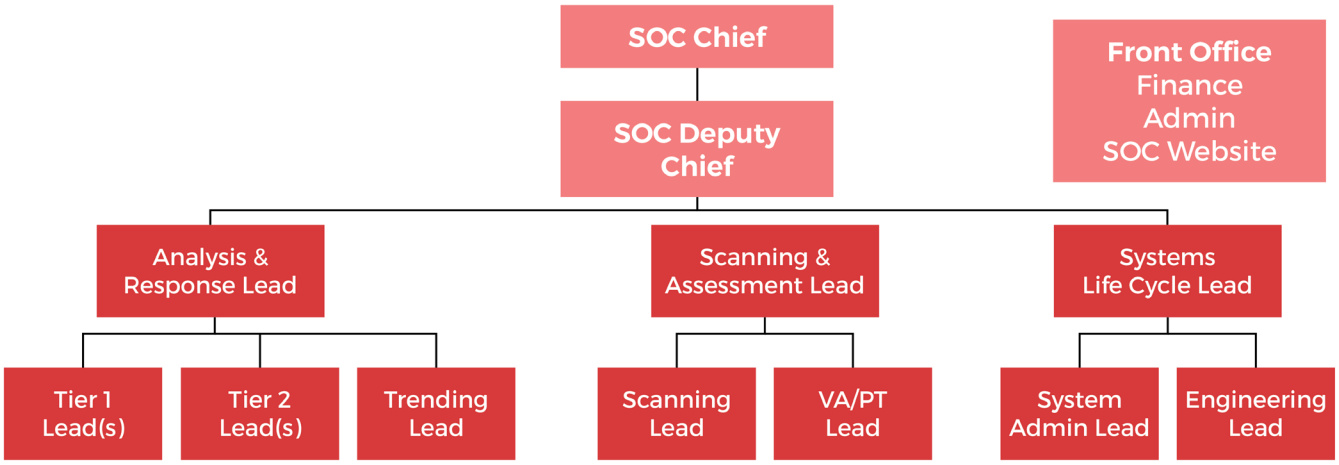
2. **Tier 2** – In a large SOC Tier 2 analysts have expanded responsibilities that include investigating events and incidents to resolution, regardless of whether it takes hours or months.

3. **Tier 3** – These analysts are infrequently called tier 3 analysts but rather, threat intelligence/analyst, cyber intel analyst or the like. They are responsible for collecting trending cyber intel and analyzing network activity and adversary TTPs over months and years. This position is often the most ambiguous because analysts are asked to handle imminent threats as well as position the SOC to handle emerging threats.

Depending on how many events a Tier 1 analyst has to handle and how many incidents or how much malware Tier 2's have to analyze, SOCs may have Tier 1 to Tier 2 seat ratios anywhere from 2:1 to 1:2.

This means that for every two Tier 1 analysts on a day shift, there could be between one and four Tier 2 analysts, depending on how operations and escalation are structured. In terms of actual FTEs, this may be more like 5:1 or 3:1, because the Tier 1 floor positions are more likely than Tier 2 to be staffed 24x7.

## Example: Large SOC




SOC are constantly evolving to deal with changes including principally:

1. The rise of advanced threats and the evolution in the cybercriminal's tactics, techniques, and procedures (TTPs)

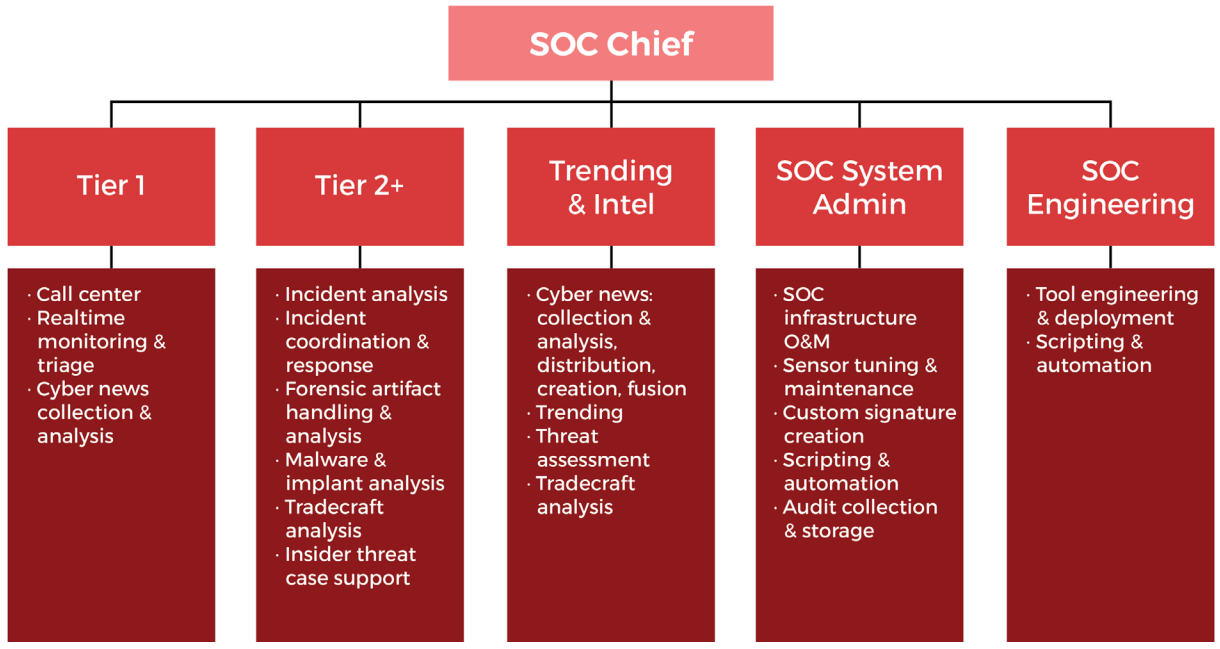
2. The organization's shift to IT consolidation and the cloud

3. The massive growth of mobile and BYOD which blur the defense borders for the IT security organization

4. The transition from the cybercriminals use of network-based buffer overflow attacks to client-side attacks or website attacks

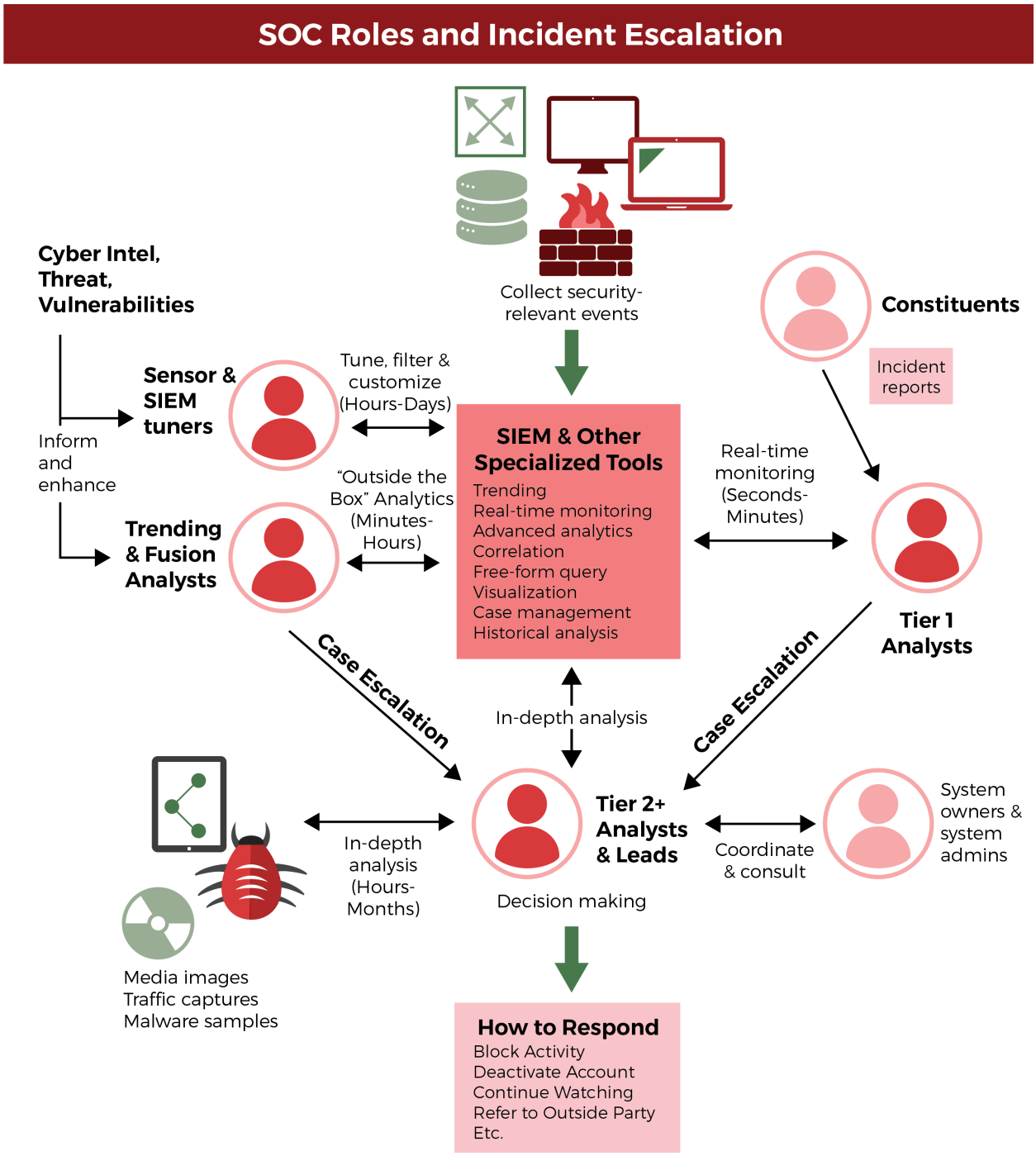
5. The lack of qualified personnel and often budget for the SOC to meet achieve its mission

## All Functions of Personnel in the SOC



Typically, SOCs are built around a hub-and-spoke architecture, where Security Information and Event Management (SIEM) technology aggregates and correlates log and other data from assets and threat intelligence feeds. The spokes of this model often include a variety of types of technology and systems including, such as vulnerability scanning and assessment solutions, governance, risk and compliance (GRC) systems, application and database scanners, intrusion detection and prevention systems (IDS/IPS), firewalls or next gen firewalls (NGFW), user and entity behavior analytics (UEBA), endpoint detection and remediation (EDR), and threat intelligence platforms (TIP).

The image below is a visual explanation concerning how the technology handles perceived attacks and how analysts are engaged in the process of handling alerts, escalating events and incidents and how they may leverage and tune their technology to prevent the next attack and eliminate false positives.



## What are the Day to Day Responsibilities of a SOC?

A typical SOC's responsibilities includes the following tasks or elements:

1. Operating the security technologies, we listed above which include SIEM's, IDS/IPS, EDR, TIP's, and lots of other new security technology that organizations want to purchase to supplement their people and processes **(many of the top security pros estimate that >50% of these technologies DO NOT reduce the chance of a breach)**

2. Prevention of cybersecurity incidents through proactive:
    a. Continuous threat analysis
    b. Network and host scanning for system and software vulnerabilities
    c. Countermeasure deployment coordination
    d. Security policy and architecture consulting

3. Monitoring, detection, and analysis of potential intrusions in real time using historical baselining and trending on security log and other security data

4. Incident response through coordinating resources and directing use of timely and appropriate countermeasures

5. Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations

Of these responsibilities, the most time-consuming is the collection, normalization and analysis of log and other data. Security logs, threat intelligence feeds, and other security-related data often overwhelm analysts in the SOC with collecting, analyzing, and archiving tens or hundreds of millions of security events per day. In addition, Firewalls, IDS/IPS and SIEM's are noisy, meaning they are constantly alerting analysts of security events which analysts must investigate to rule out an incident.

Let's clarify that last statement because it is one of the most significant problems for Tier 1 and 2 analysts. There are thousands of events that analysts must spend time investigating for every legitimate incident. Further, an actual data breach is a type of security incident. All data breaches are security incidents, but not all security incidents are data breaches. Data breaches are typically a loss or exposure of sensitive data. Thus, the progression is event, incident, breach – for every breach there are typically hundreds of incidents and for every incident there are thousands of events. This is one of the major issues for most if not all SOCs.

*The progression for analysts is event, incident, breach – for every breach there are typically hundreds of incidents and for every incident there are thousands of events. This is one of the major issues for most if not all SOCs.*

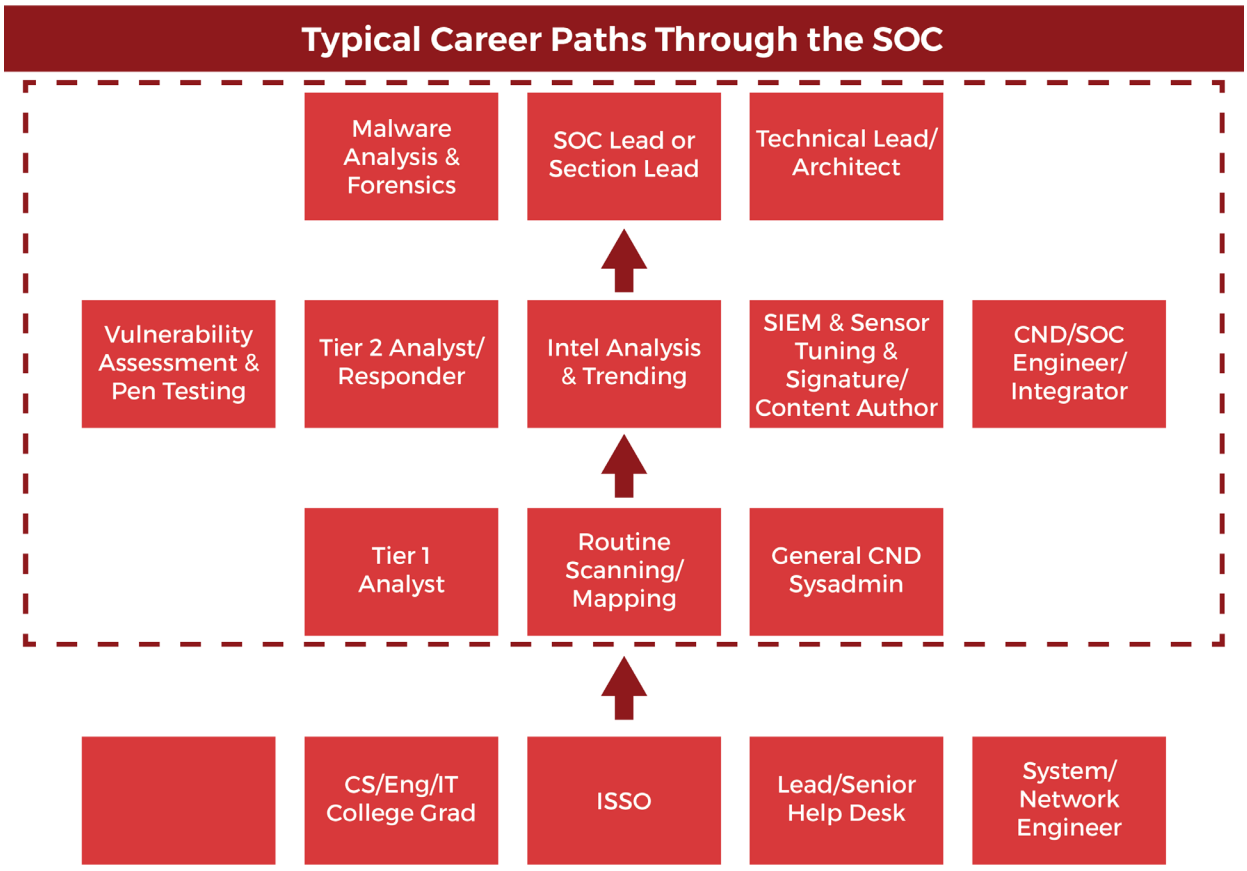
## Planning a Career in a SOC

**Tier 1 Analyst** – These are triage specialists who handle take the information that the security tools like the SIEM and IDS/IPS assets provide them and decide whether any event or alert should be escalated to Tier 2. They also run vulnerability scans and review vulnerability assessment reports. Finally, they often Manage and configure security monitoring tools. They typically have security certifications including CISSP, GCIA GCIH, GCFA, GCFE, etc.

**Tier 2 Analyst** – These are incident responders who reviews trouble tickets generated by Tier 1 Analysts. They use threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack. They also review and collect asset data including configs, running processes, etc. on these systems for further investigation. Finally, they determine and direct remediation and recovery efforts.

**Tier 3 Analyst** – These are the threat hunters who are typically known for handling penetration testing and vulnerability assessment data. They are tasked with exploring ways to identify threats that may have found their way inside your network. Using the penetration tests, they conduct on production systems, they validate resiliency and identify areas of weakness to fix. Finally, they try and optimize defense by recommending how to leverage security monitoring tools based on threat hunting discoveries.

**Tier 4 SOC Manager** – This is the COO of the SOC. They supervise the activity of the SOC team, and they recruit, hire, and train the staff. They manage the escalation process and review incident reports. They also develop and execute crisis communication plan for the CISO and other stakeholders. They also prepare compliance reports and support the ever-expanding audit process. Finally, they measure SOC performance metrics and communicate the performance and value of security operations to business leaders.



# How Security Technology Empowers the Analysts to Prevent Attacks

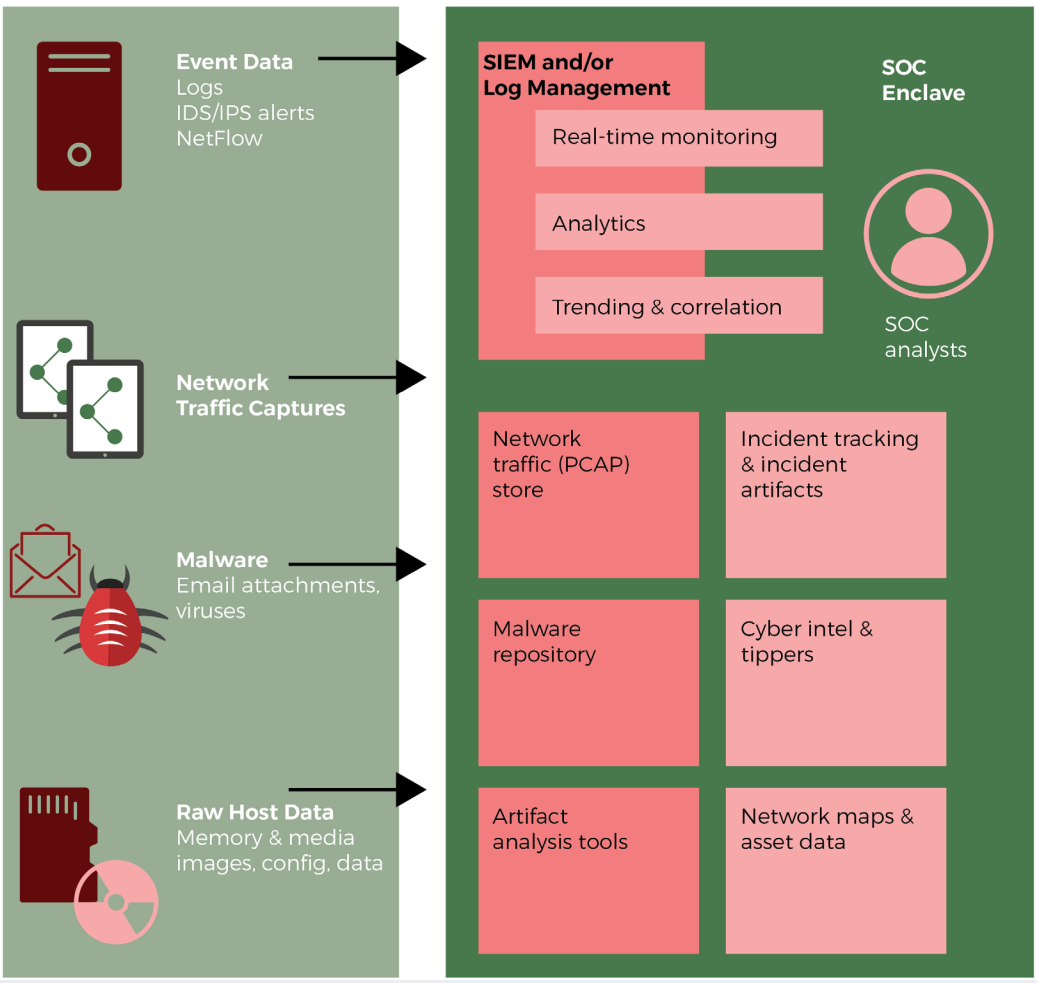
## Focusing on the Roles of SIEMs and IDS/IPS Technology – Costs and Benefits

### What is a SIEM?

Let's start with the SIEM and effective log management – it is the core of what Tier 1 and often Tier 2 analysts must leverage to understand an event or incident. Effective log management is essential to an organization's security. Monitoring, documenting and analyzing system events is a crucial component of IT security. Log management software or SIEM's automate many of the processes involved. A SIEM handles the two following jobs that prior to today's SIEM's were handled individually:

- **SIM - Security information management** - Long-term storage as well as analysis and reporting of log data. This was and is still tricky and time-consuming if you must build your own connectors to your IDS/IPS, Firewalls, DLP solutions, Application servers and so many other log generating assets in your IT environment. Most SIEM's have some connectors out of the box today.
- **SEM - Security event manager** - Real-time monitoring, correlation of events, notifications and console views. This is the key benefits of SIEM's because a good SIEM will turn data into insights and a great SIEM, tuned correctly will turn insights into visual dashboards to assist analysts in uncovering anomalies and threats.

**Typical SOC Tool Architecture**

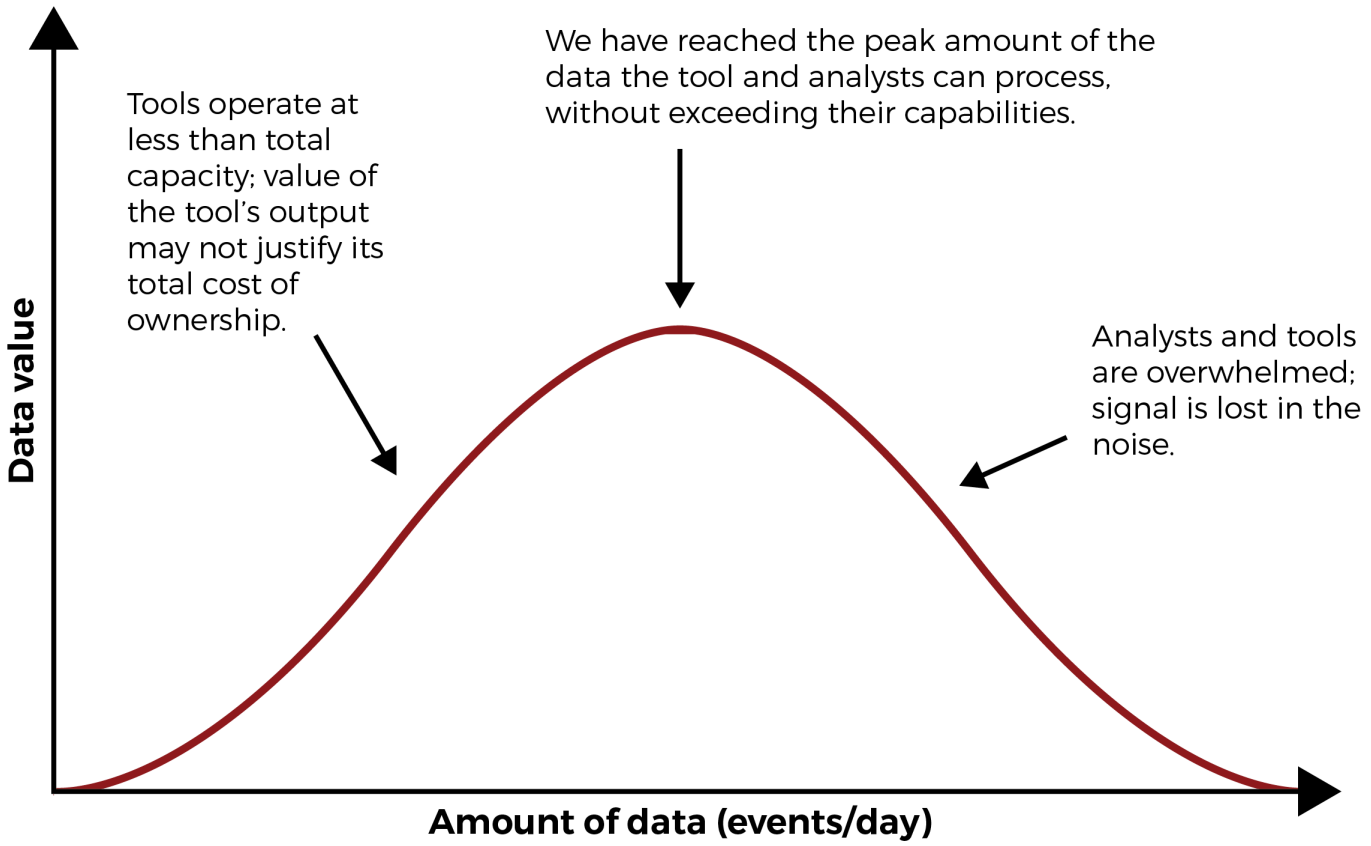


Most SIEM's have a variety of features and functionality including:

1. **Basic security monitoring** – The basic collection, normalization, correlation and analysis of logs. This is the fundamental responsibility of a SIEM.
2. **Security incident detection** – The second basic function of a SIEM is to alert security teams to anomalies or policy violations in an automated way with clear information.
3. **Advanced threat detection** – SIEM's integrate intelligence feeds that provide data on current threats which SIEM's use to identify threats.
4. **Notifications and alerts** – SIEM's can be tuned to alert security analysts when policies have been violated or threats have been identified.
5. **Forensics & incident response** – SIEM's have the ability to store logs so that when a breach or incident occurs, IR teams and digital forensic investigators have the ability to perform root cause analysis.
6. **Compliance information** – SIEM's are increasingly being used to demonstrate compliance by providing auditing and reporting concerning log-in data, user information, IP address information and data flow.

*A SIEM ingests log data from a variety of network hardware and software and analyzes the data in real time. A SIEM's purpose is to correlate events and identify anomalies or patterns of behavior like traffic from suspicious IP addresses or unusual exfiltration of data that may indicate a breach.*

## Balancing Data Volume with Value



Ok, let's say the SIEM fires off an alert that someone is trying to access a system or application that they shouldn't be accessing. At that point, the alert becomes an event. The SOC analyst will investigate the event and try and understand if the act was malicious or not. If the analyst thinks that the IP address is suspicious, or they believe they may be under attack from malware on the system will likely escalate the incident to a higher tier analyst or the incident response team.

*A SOC's main goal in today's environment is to leverage SIEM's, IDS/IPS and othe security tools that automate the early stages of monitoring, including event collection, parsing, storage, and triage.*

Now, as we said earlier, SOC's investigate lots of incidents so they don't want to initiate countermeasures immediately because there are usually negative consequences to countermeasures including:

1. If the SOC blocks benign activity thinking they are blocking an attack it may impact legitimate business

2. There are thousands of attacks per day, SOCs do not want to overreact to an attack and lose forensic evidence by disconnecting communication or shutting down target equipment

3. If the SOC deploys certain countermeasures they may alert the attacker who will then try and cover their tracks and the SOC have a more difficult time understanding the extent and severity of the attack; or if the attack is ongoing in other systems in the environment.

4. A response action could impact an organization's mission more than the incident itself

Further, there are a variety of attacks so analysts will need to gather basic information like suspicious entries in system or network, excessive login attempts, unexplained new user accounts, unexpected new files, etc., in order to narrow down the possibilities and start limiting the scope of the attack.

Understanding the extent and severity of the intrusion by watching the adversary is sometimes more effective than performing static forensic analysis on compromised systems, once the adversary is no longer present.

**The Costs and Drawbacks of a SIEM**

1. **They are Expensive!** In most cases and for most organizations they start in the tens of thousands and can easily cost over $100,000 depending on the brand and the amount of log data that is processed.

2. **They are Difficult to Operate and Manage**. In various surveys, 40% or more of the organizations that responded suggested that they don't have the expertise in-house to manage a SIEM. SIEM's are notoriously "noisy" generating many false alerts, so the better the operator, the more effective the technology.

3. **Deployments are Difficult**. Splunk and LogRhythm are the market leaders for the most part and both have their benefits, however both can be difficult to deploy but it is getting easier with cloud and hybrid deployments. Basic setups of the SIEM's are fairly straightforward, however "tuning" them to ingest the correct logs, designing access control, setting up correlations, integrating intelligence feeds and so much more can be time consuming.

**The Benefits and Advantages of a SIEM**

1. **They Help Understand Security Threats**. Plainly, the reason that companies need SIEM systems to monitor logs and report suspicious events is that most organizations generate far too much event data for any human to be able to make sense of it.

2. **They Correlate Data to Provide IOC's**. Ok, this is a little like benefit #1, however beyond just collecting, normalizing and analyzing logs, SIEM's can ingest threat intelligence feeds and many are now integrating machine learning to understand what a real indicator of compromise (IOC) is and what it isn't.

3. T**hey assist with Data Presentation**. SIEM's have the ability to present data a variety of ways including out-of-the-box reporting and customizable reports. The advantage is that analysts can visually spot trends, anomalies, traffic spikes, and so much more. The reports and dashboards can serve as the cornerstone information hub to determine where and how to drill down on any suspicious activity.

4. **They assist with Compliance Assistance**. Finally, with GDPR, CCPA, HIPAA, PCI-DSS and so many other pieces of compliance legislation on the horizon, SIEM's can make reporting on how organizations are safeguarding PII, who is accessing data, and from where.

**Focusing on the Roles of SIEMs and IDS/IPS Technology – Costs and Benefits**

**What is IDS/IPS (IDPS)?**
An intrusion detection system (IDS) will analyze and monitor network traffic for signs that indicate attackers are using a known cyberthreat to infiltrate or steal data from your network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviors like security policy violations, malware, and port scanners.

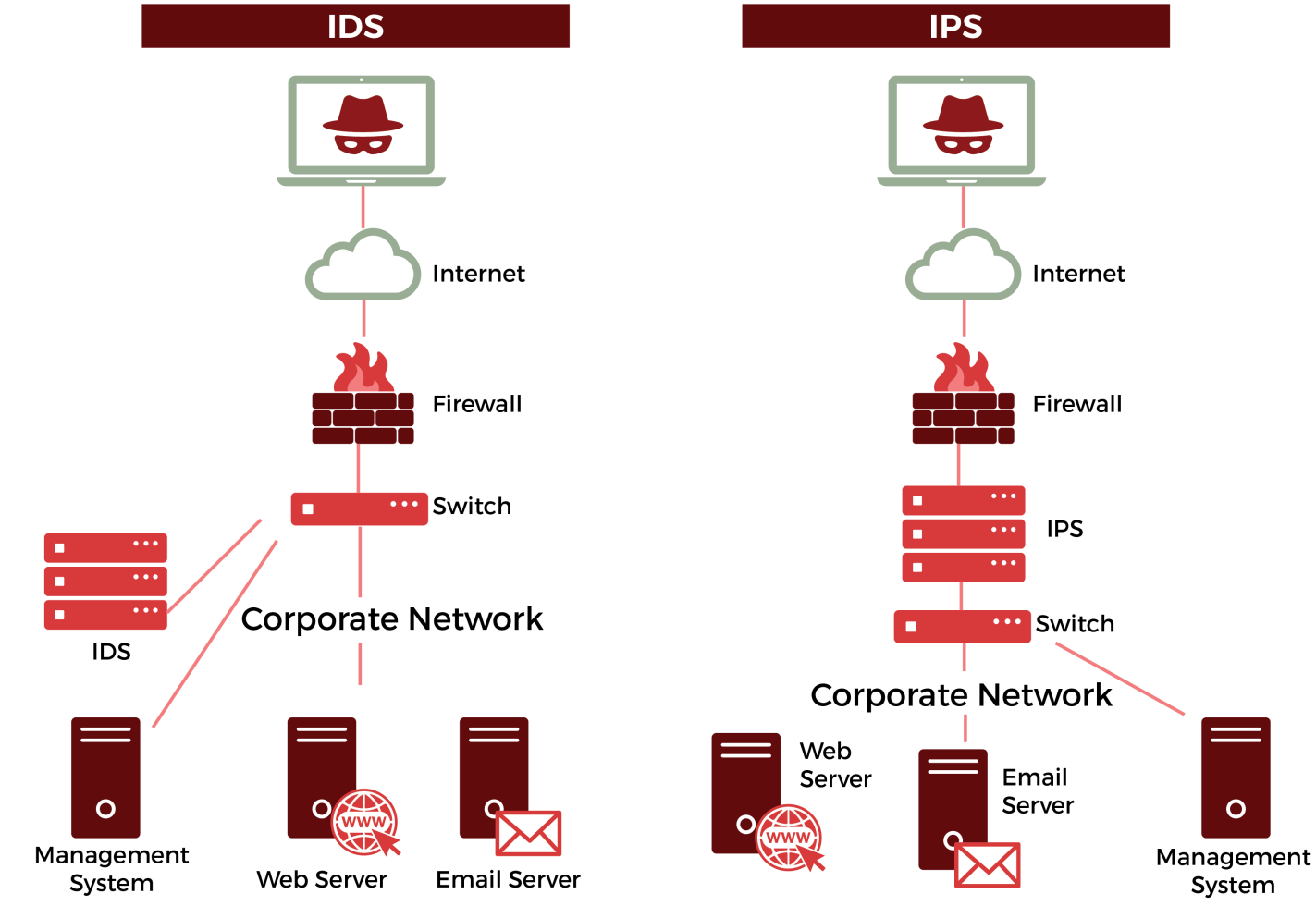
**NOTE:** This is passive technology that can only identify an attack, not stop one like a SIEM.

An intrusion prevention system (IPS) live in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively deny network traffic based on a security profile if that packet represents a known security threat.

**NOTE:** This technology can block traffic that could be malicious.

IDS/IPS (IDPS) technology behind your firewall can uncover thousands of threats daily that get past the firewall; they can also identify threats that are trying to leave the network. The challenge is that an analyst must proactively update the IDS/IPS with threats and policies and monitor it 24x7x365.

**Intrusion Detection System vs. Intrusion Prevention System**



### The Costs and Drawbacks of IDS/IPS Technology

1. **They are expensive!** In most cases and for most organizations they start significantly over $10,000 and can leak into the millions of dollars just like a SIEM.

2. **They are Difficult to Operate and Manage.** This is sounding a bit like we wrote when we described the drawbacks of a SIEM, however complexity concerning operation is certainly an issue with IDS/IPS technology. Signature libraries must be updated, they need to be administered by an engineer and false positives are frequent.

3. **They don't prevent all attacks.** IP packets can be faked, encrypted packets are difficult to read for most IDS systems, and IDS does not block attacks while IPS may block legitimate traffic if they are not tuned appropriately.

### The Benefits and Advantages of IDS/IPS Technology

1. **They Help Understand and STOP Security Threats.** The reason that companies need IDS/IPS systems is to analyze traffic coming into the systems in the organization to make certain that traffic doesn't match "known" malicious traffic. If the signatures are updated IPS systems reliably block malicious traffic.

2. **They Can Qualify Attacks.** An IDS analyzes the amount and types of attacks. This information can be used to implement new controls or adjust other security technology so that they are more effective. IDS can also be used to identify bugs or network device configuration problems. The data is useful for understanding the overall risk an organization faces of a threat.

3. **They Help with Compliance Assistance.** Finally, with GDPR, CCPA, HIPAA, PCI-DSS and so many other pieces of compliance legislation on the horizon, IDS logs like SIEM logs are excellent data and evidence that an organization is meeting its compliance requirements.

4. **They are Improving.** Machine learning and artificial intelligence is being employed by industry leaders like Cisco, McAfee, and Trend Micro which allows the IDS/IPS technology to learn the behavior of malware and better identify and block malicious attacks.

## Four Recommendations to Improve the Effectiveness of your SOC

The ultimate goal of this guide is to provide 4 or so understandable, actionable recommendations for improving SOC effectiveness. We wanted to spend the majority of the brief discussing the mission, goals, responsibilities and technology of the SOC prior to presenting our recommendations. Frankly, while our recommendations are not clearly not breakthrough ideas, many of our customers adopted these recommendations to increase the effectiveness of their SOC. In the 80/20 world, organizations should invest in projects that will provide the biggest bang for their buck; we hope these recommendations will provide that ROI.

## Recommendation 1 – Align SOC Responsibilities with the Mission of the Business

First, a significant element of a SOC's job is to maintain and provide an understanding of the organization's defensive posture and communicate it to the business or management. IT assets and challenges in most organizations is constantly in flux with the challenges we discussed in part 1 of this blog post; cloud migration, mobile, BYOD, threats, vulnerabilities, new technology, mergers… you see what I mean I'm sure.

SOCs must constantly evaluate their security risk posture as the organization's technology evolves, threats change, vulnerabilities surface and a variety of other variables. The bottom line is whether they use CIS 20, ISO, NIST or another risk-based control framework, they need to understand where their weaknesses are and how to prioritize fixing them.
The SOC is tasked with gathering and assembling the following three components in order to help the business understand the organization's overall security posture so that the business can manage the risk:

1. **Information** - Sensor data, contextual data, cyber intel, news events, vendor product vulnerabilities, threats, and taskings
2. **Analytics** - Interpreting and processing the information
3. **Visualization or Scoring** - Depicting the security posture information either in visual form or a scoring system that the management team can understand

## Recommendation 2 – Understand Your Security Posture and Manage Tasks from a Risk Management Perspective

Second, now that we understand the business risk, our security posture, our weaknesses and the priority of fixing those weaknesses we have a foundation to build on. We can now stop patching every two weeks or month and patch by system value, application criticality and seriousness of vulnerability – essentially by risk. SOC personnel will become for more effective, efficient operators because they consistently have a prioritized list of what they need to do to make the organization more secure and reduce overall risk.

Risk management and understanding security posture is more than asset inventory, vulnerability assessments and patch prioritization. Thus, let's simply lay out the three areas of the business that could be considered in the risk control and security posture assessments:

1. **Network** - Number, type, location, and network connectivity of IT assets, including desktops, servers, network devices, mobile devices, and outsourced "cloud" systems

2. **Mission** - The lines of business and mission the constituency engages in, including their value, which may be expressed in revenue, expenditures, or lives
    a. Geographic/physical location where different parts of the mission occur
    b. The business relationship between the constituency and external parties

3. **Threat and adversaries**
    a. Capability, including skill level and resources
    b. Intent and motivation
    c. Probability of attack

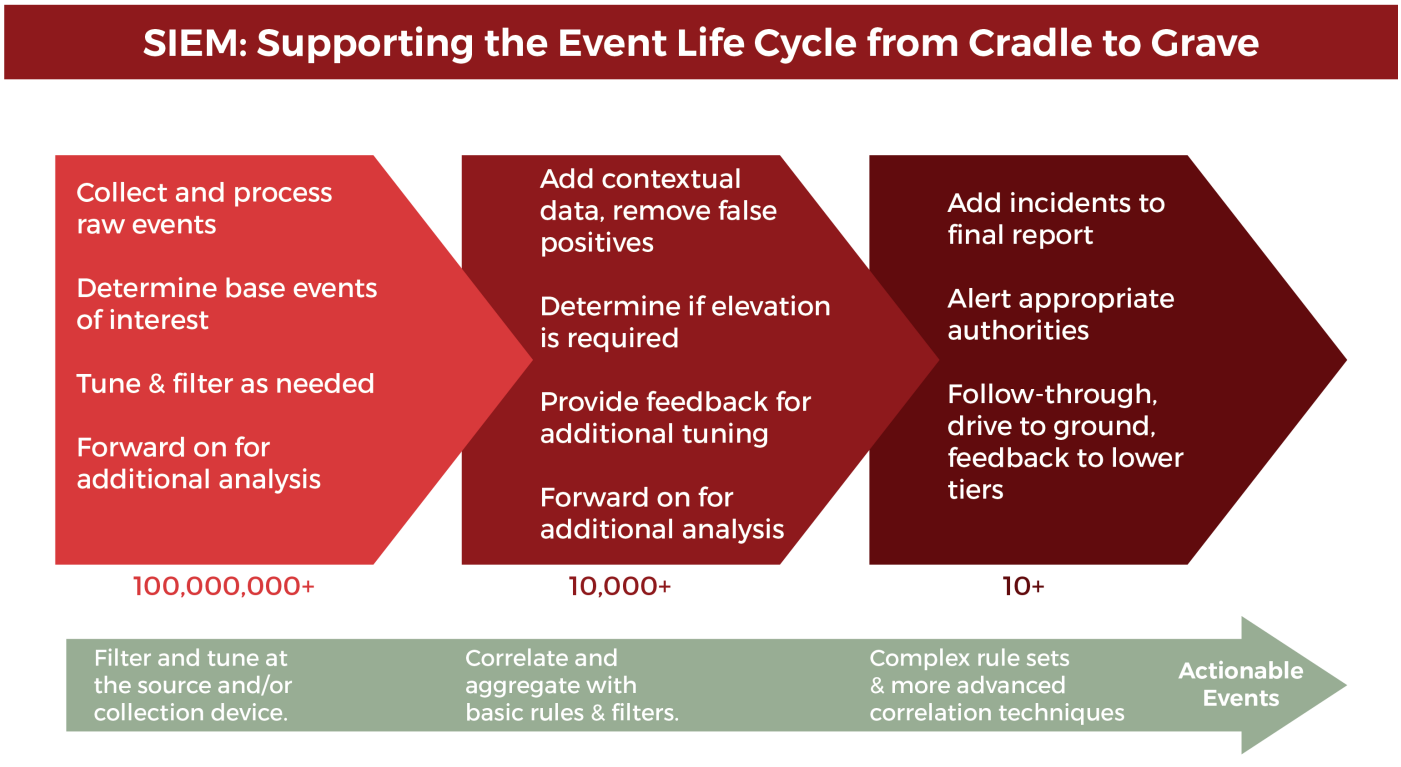
**After Gathering the Information for the Risk Control and Security Posture Assessments Start with the Following Questions:**

1. What is the patch status of the enterprise? Which patches do we really need to care about, and which are less important?
2. Is my constituency facing the serious threat of a targeted external attack such as a spear phishing campaign?
3. What is a real-time picture of possible intrusions or, at the very least, known malware?
4. To which systems should I apply different security controls that will provide the greatest overall help in preventing a given set of attacks?
5. What is changing about the threats faced by the constituency? How are their TTPs changing, and what do I have or need to detect and defend against those new threats?
6. Who is acting outside their typical lines of behavior, and is this cause for concern?
7. What is the relevance of the attacks I'm investigating within the context of the constituency mission?

## Recommendation 3 – Leverage Technology to Improve Efficiency and Effectiveness of Your Analysts – The SIEM

Now, let's discuss technology. As we suggested earlier, we have AV's, Firewalls, IDS/IPS, EDR, Sandboxes and so many other types of IT security technology. We know that much of this technology is not leveraged correctly in the SOC and that SOC analysts are overwhelmed by the inaccuracy and noise that much of this technology creates.

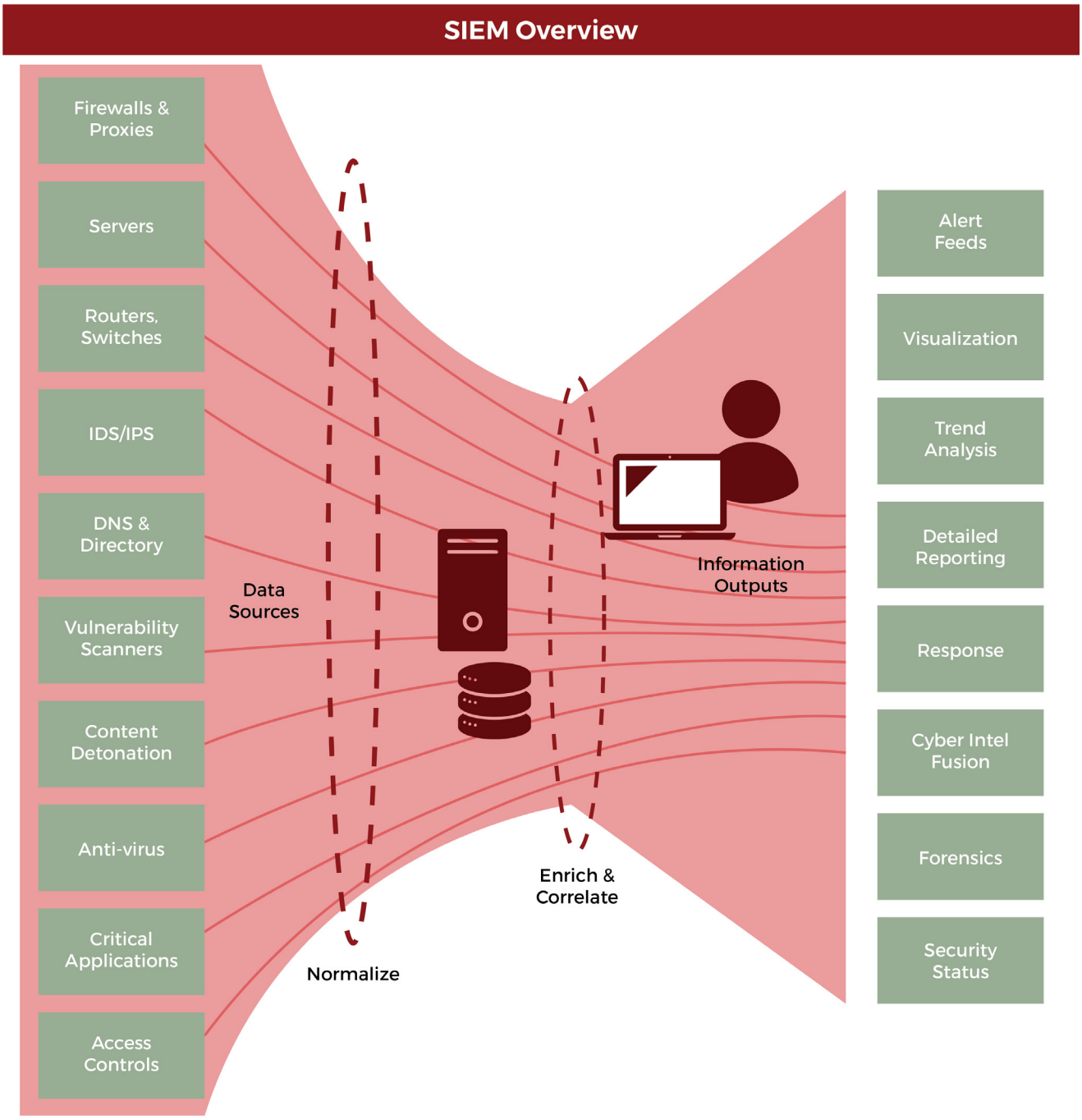
The image below provides excellent insight into how the value of a SIEM should be extracted by culling down the massive collection of logs to only the few that require context and evaluation.



IT security technology's value proposition was to make the SOC analysts more productive by collecting, normalizing, assessing and reporting in an automated way so that Tier 1 analysts could deal with only important events. It hasn't worked out that way unfortunately.

With that said, we want to be clear about the next point while keeping it simple - your first line of network defense is your firewall. The firewall allows or denies traffic in or out, while a SIEM analyzes log files. Within your IT infrastructure, you may have lots of different devices that are generating a massive number of log files.

A SIEM brings together the log data from disparate devices into a management layer, which provides visibility and the ability to detect and respond effectively to security breaches. A SIEM triages the logs for you by analyzing all the log data, and through correlation rules, behavioral analysis, and machine learning, filters down and extracts events of interest.



A SIEM will typically alarm in the case of brute force logon attempts, traffic going and coming from suspicious sources, policy violations, and so many other issues.

**These false positives fall into three buckets:**

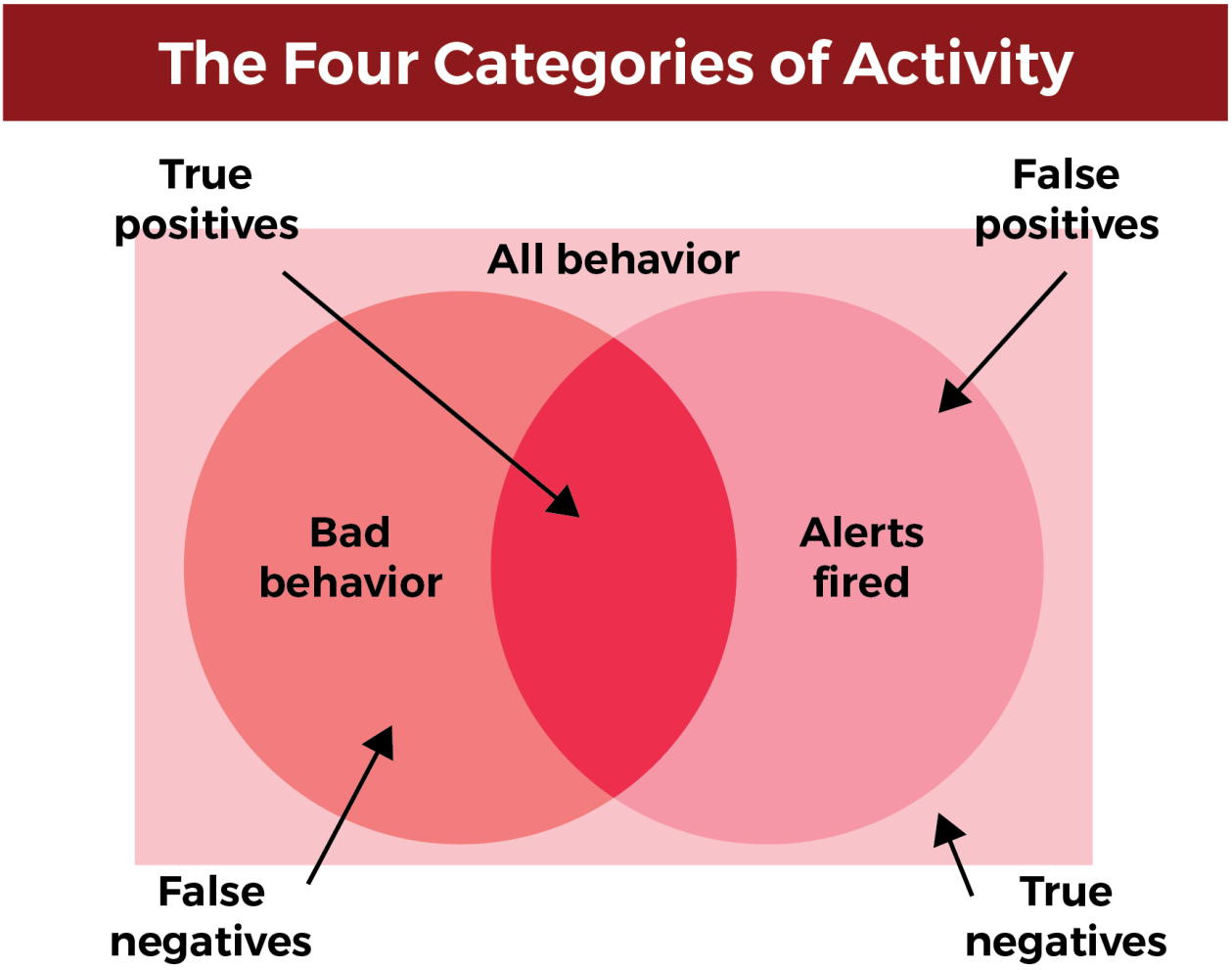
1. Indicators of operational issues

2. Policy concerns

3. Nonactionable information

We could spend pages going through the different types of alerts in the categories above, however I would suggest researching which alerts should be handled and which should be suppressed in your specific organization.

The bottom line is If there are more alerts in one day than your security personnel can review, then some level of suppression must be implemented that will bring the most important items to their attention the fastest. Reducing the number of alarms that are emanating from your SIEM allows your security team to be more efficient in the use of their time and more effective in focusing on and resolving important issues quickly when they arise.

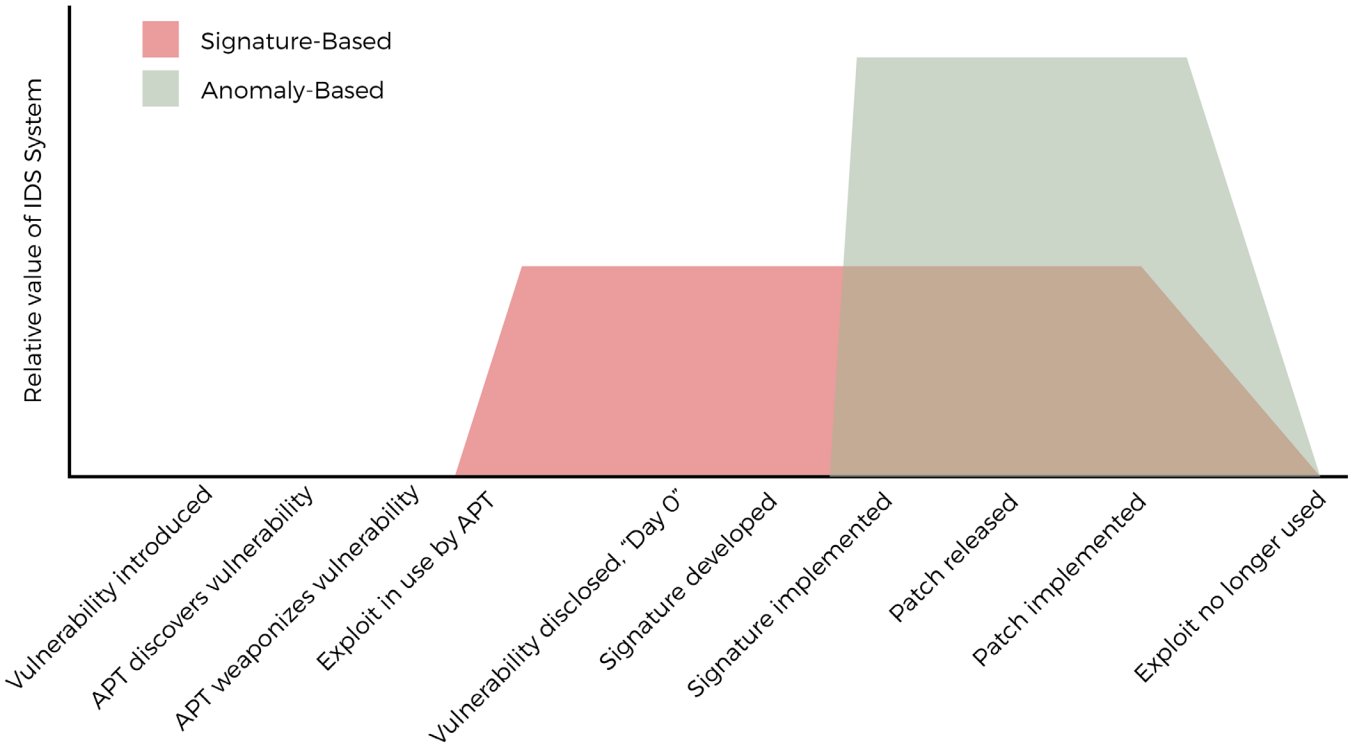


## Recommendation 4 – Leverage Technology to Improve Efficiency and Effectiveness of Your Analysts – IDS/IPS

Depending upon how often an organization is targeted, IDS/IPS devices that are not tuned properly like the problem we discussed with a SIEM, can generate thousands or millions of false-positive alerts each day and can generate false-negative responses to true threats. Obviously, like the alerts with the SIEM the analyst cannot efficiency do their job and identify real threats and take immediate action.

The reality is that if your security devices continually send false alerts, analysts will likely ignore them as well as those that are true-positive alerts. Many companies have been breached because their security teams ignored an alert that should not have been.

**IDS Signature Age Versus Usefulness in Detection**




You want alarms to be triggered in the event of malware, web attacks, and data compromise but not traffic-type or equipment-related or non-malware alarms. The Defense in Depth model which includes layers of security technology including SIEM's and IDS/IPS hasn't been bulletproof because each technology throws off an alarm and analysts simply ignore it – exactly what happened in the target breach.

## Conclusion

In trying to improve the effectiveness you certainly must start with the most basic elements of the SOC mission: prevent, monitor, detect, respond, and report. In this brief we tried to evaluate SOC improvement opportunities that presented the most significant ROI. In addition, we tried to focus on issues that plagued the industry universally.

Aligning the mission of the SOC with the mission of the business is critical in our mind. No two businesses are the same and thus the security gaps are rarely aligned so there is no one size fits all SOC or piece of security technology. Second, risk management has become a critical issue as IT security expenses have skyrocketed but attacks continue to get through. Focusing on where the sensitive data is in an organization and how to cost effectively protect it should be prioritized – as an example. Finally, SIEM and IDS/IPS issues including the need for constant tuning and addressing false alerts has been one of the most significant problems for analysts and has led to massive breaches.

We hope you enjoyed this brief and we certainly welcome any questions or comments.