SANS

Analyst Program

Whitepaper

A SANS 2021 Report: Making Visibility Definable and Measurable

Written by **Barbara Filkins** and **John Pescatore**

June 2021

Infoblox

Defining Visibility

Throughout 2020, a recurring theme emerged across SANS survey results: the need for improved visibility into all aspects of security. Although visibility—or rather, lack of visibility—is a concept easily understood by most, the term remains subjective, and perception can vary widely depending on stakeholder role.

More and more boards of directors are recognizing the strong correlation between cybersecurity and business health, and they are looking to security managers to define strategies and recommend investments in robust cybersecurity processes and controls. As reported by Security Boulevard,[1] the strategic importance of cybersecurity is evident in board composition; Gartner found that at least 40% of boards now have an officer who has cybersecurity expertise.[2] Board members are demanding dynamic, real-time, unified critical data and visualizations for business-critical security metrics. Such security metrics are critical for the board and executive management to evaluate business governance and risk-management performance and to make strategic decisions.

Visibility does not lend itself to a precise definition—the meaning will differ depending on who is looking. Yet organizations need to establish a visibility strategy that complements their security profile in order to assess where they should direct resources to improve for the future.

To achieve this, organizations need to take an interdisciplinary approach, as SANS did in this report. We sought insight from key individuals within SANS, including curriculum leads, instructors, and analysts. The common message which emerged was that good visibility encompasses the triad of people, processes, and technology. It is a means of communication across differing organizational aims, management vs. technical goals, and business vs. security objectives. We focused on what is needed to get there—allowing stakeholders to build an in-depth picture of organizational security while still focusing on those elements most important to their role.

The Starting Point: A Working Definition

Cybersecurity professionals consistently place visibility at the top of their recognized needs lists. But what exactly is the definition of "security visibility"? There is no single definition, because different stakeholders have divergent expectations of visibility. (See the "Stakeholder Expectations Based on Roles" sidebar.) But none of these stakeholders operates in a vacuum. There are interfaces between each role. **Therefore, to achieve organizational visibility into security, organizations must align what are often viewed as divergent goals.**

Stakeholder Expectations Based on Roles

Stakeholder expectations of visibility depend on answering the questions central to their role, as follows:

- **Senior management needs a concise view of threats and risks, both current and trending:**
  - **Is security risk in my industry rising?**
  - **How well prepared is my organization to detect, protect and defend?**
  - **Is the risk to my organization increasing (or decreasing)?**

  Senior management also has to answer traditional questions, including:
  - **Am I spending the right amount of money?**
  - **Am I better off than I was this time last year?**
- **Operational security teams need a high-level (near real-time) view of vulnerabilities, events and threats, plus the ability to see all the details quickly. Their needs and questions include:**
  - **Are there signs of malware in our systems?**
  - **Can we detect whether workforce members are misusing their access?**
  - **Are we going to pass PCI compliance?**
- **Analysts concentrate on the baselines of what is considered normal behavior, generally using techniques similar to those used in business analytics. Questions here are:**
  - **Which devices are trying to communicate with known malicious sites on the internet?**
  - **What systems are probing our networks?**
  - **Are we seeing any indications of [insert latest threat]?**

[1] "The Importance of Board Members in Building a Cybersecurity Strategy," https://securityboulevard.com/2021/05/the-importance-of-board-members-in-building-a-cybersecurity-strategy

[2] www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-

To be effective, **security visibility should include people, processes and technology, keeping in mind both the mission of the organization and demographics, such as industry, workforce size, roles and location.** These demographic characteristics can be viewed as a set of independent variables that will influence what metrics or performance indicators will be most critical.

A working definition for security visibility within an organization starts with integrating various security concepts across an organization. To develop this structure, SANS turned to the concepts that are followed for safety management, using the definitions for the four pillars of a Safety Management System[3] to structure these areas: policy, risk management, assurance and promotion.[4] Figure 1 presents these areas, which have been adapted to the concepts surrounding cybersecurity.

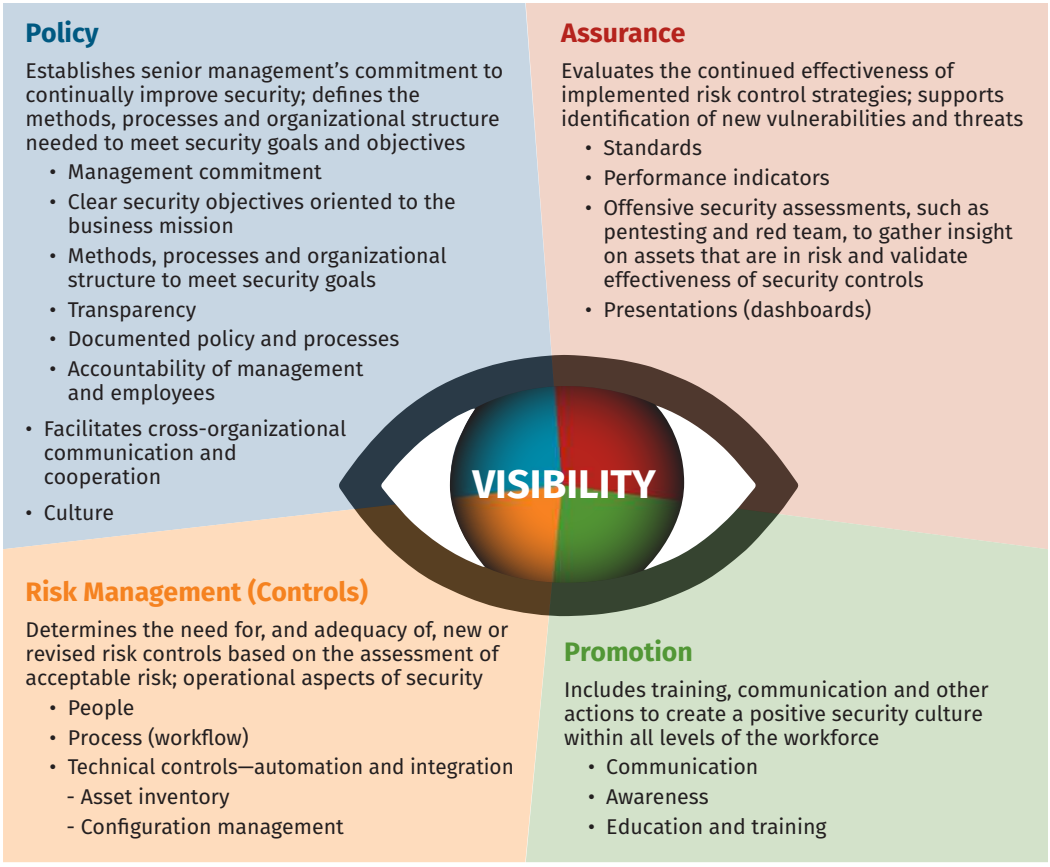

Figure 1. Elements for a Working Definition of Security Visibility

Visibility begins with organizational (domain) knowledge, which sets and maintains purpose for any analysis and outcomes, affixing meaning to what is being visualized. Effective visibility is organization-specific, but the process of developing a definition can follow a consistent road map—the approach SANS is taking in this paper.

Understanding the Challenges

Developing a systematic approach to visibility is challenging because each core area is unique in its own right. The following list describes their unique challenges:

- **Policy—**The first major challenge is establishing organizational commitment to security, both as required by regulation as well as what is needed to protect and defend the business. Development of a strong security culture starts with understanding security risk across the enterprise, knowing how the pieces—from management commitment to asset management to operational security—fit together to reduce that risk to an acceptable level. To facilitate cross-organizational communication and cooperation, stakeholders at all levels (analysts and management alike) need to be able to comprehend what they are looking at in the context of their roles. They also need to ask and answer the right questions, including why certain data needs to be protected or why certain activities need to be recorded and monitored.

[3] www.faa.gov/about/initiatives/sms/explained

[4] www.faa.gov/about/initiatives/sms/explained/components

- **Risk management—**To effectively estimate and communicate risk requires completeness, accuracy and relevance of information needed to address the questions being asked. Asset inventory and management remains a challenge for many organizations, especially with the 2020 shift to remote work. In the SANS 2021 Endpoint Monitoring in a Dispersed World Survey, only 25% of survey respondents indicated that they use endpoint monitoring solutions that have cloud- or DMZ-based servers, which is needed for data capture even if devices are off the organization's network.[5] This has a big impact on how organizations could maintain visibility into their endpoints. Central management only goes so far when it is limited to the corporate network!
- **Assurance—**Monitoring and evaluating implemented controls is crucial to finding out if the controls are performing as expected (e.g., controls are in place, designed appropriately, operating effectively and monitored regularly), in an effort to reduce risk exposure. The challenge here is separating the effectiveness of the implemented controls from the often artificially contrived requirements in regulatory compliance monitoring. Case in point: The organization was deemed PCI-compliant by the PCI Qualified Security Assessor (QSA), but still suffered a PCI-related incident.[6]
- **Promotion—**Developing a strategy that includes training, communication and other actions to create a positive security culture within all levels of the workforce—the human elements—is not as straightforward as instrumenting the network. In the aviation world, data on human performance and reliability are considered by many technical experts as "soft," not receiving as much attention as technical data. As security professionals, we also tend to have this bias, where numbers and hard data are easier to deal with. But security has its subjective elements, covering a wide range of topics that often lack measurable elements that can help predict the reduction of risk as it relates to improved visibility.

According to Lance Spitzner, Director of SANS Securing the Human, "Visibility isn't a term that is used much [for the human side]—but it should be. [Here], visibility would involve insight into two questions:

- What are the organization's top human risks?
- How good is our ability to manage (reduce) these human risks?"

The challenge here is how best to answer these questions. The indicators and metrics are not necessarily as objective as answering the technical questions.

Getting Started: Developing an Organizational Visibility Strategy

Visibility provides insight into an organization's ability to deal with vulnerabilities and respond to incidents. Consider the following questions as a starting point to help address what is needed in each of the core areas:

- **Policy**
  - **Where are the dark spots in my organization's ability to detect, protect and defend?**
  - **Are the trends improving or getting worse?**
- **Risk management**
  - **What are the current (and potential) attack surfaces?**
  - **What are known or latent vulnerabilities, such as either in code and in the runtime?**
- **Assurance**
  - **Is the organization on the right side of compliance and privacy laws?**
  - **What have my recent offensive security assessments, such as pentesting and red team exercises, shown to be my vulnerabilities?**
- **Promotion**
  - **What did the results of the phishing exercise demonstrate is needed in continued user awareness?**
  - **Have my organizational needs for recurrent security training changed in the past 6 to 12 months?**
  - **Is my organization proactive in disseminating security lessons learned to my workforce for strengthening my culture?**

[5] "SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey," March 2021, www.sans.org/reading-room/whitepapers/analyst/2021-endpoint-monitoring-dispersed-workforce-survey-40200, p. 6.

[6] "Compliant but not Secure: Why PCI-Certified Companies Are Being Breached," www.csiac.org/journal-article/compliant-but-not-secure-why-pci-certified-companies-are-being-breached

Importance of Knowing What Visibility Means

Several recent major events, such as the SolarWinds[7] attack and the Exchange server breach,[8] demonstrate the need for visibility that moves beyond the reactive. Focusing on the timeline in Figure 2, we note:

- **Early visibility of the high market share and heavy adoption, installation on sensitive internal networks and the broad reach across corporate systems by SolarWinds would have indicated it was a likely target for attackers.** Enterprises could have prioritized proactive behavior profiling and anomaly monitoring.
- **The attackers compromised SolarWinds' systems and were active for three months before SolarWinds released the malicious Orion update.** If SolarWinds had proactive visibility of the vulnerabilities that enabled the attackers, or even just reactive visibility into their actions in traversing internal resources, SolarWinds would have known the update had potentially been compromised and would not have released it.
- **Once the compromised update was installed and active for up to 10 months on corporate networks, the compromised software took many actions that had never been necessary for previous versions.** Post-event investigations identified many opportunities for impacted enterprises to quickly detect unusual and potentially malicious activity initiated by the compromised SolarWinds Orion.

Security States

- **Reactive—Respond to past and present threats, rather than anticipate future dangers. Acting on lessons learned from an incident is an example of reactive security.**
- **Proactive—Prevent major incidents before they happen. Knowing the vulnerabilities in the infrastructure and addressing them relative to known threats is an example of proactive security.**
- **Predictive—Use advanced contextual analysis (and tools such as artificial intelligence and machine learning) to identify possible threats before they become incidents, enabling preventive measures to avert costly losses and other negative outcomes.**

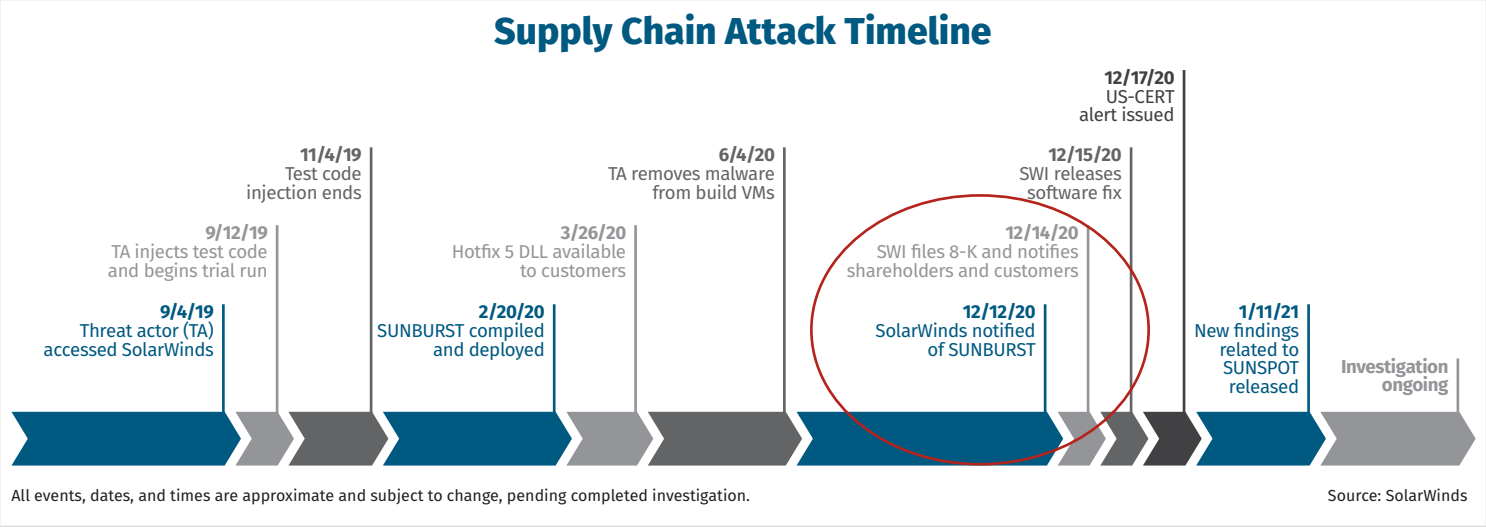

Figure 2. SolarWinds Supply Chain: Attack Timeline[9]

[7] www.cisecurity.org/solarwinds

[8] www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html

[9] "New Findings From Our Investigation of SUNBURST," https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst

Shaping Visibility

Visibility is traditionally oriented toward the status and configuration of technology (i.e., devices, applications, endpoints and networks). According to Frank Kim, Fellow and lead for both the SANS Cybersecurity Leadership and SANS Cloud Security curricula, "We also need visibility into users (identity, access, risk profile) and key business processes (M&A, entry to new markets) as well as technology processes (DevSecOps)."

This statement is borne out by results from "Effectively Addressing Advanced Threats," where the top major infrastructure visibility gaps are related to data and/or access. See Table 1.[10]

Table 1. Visibility Gaps, per SANS Survey

Rank	Visibility Gap
1.	Lack of visibility into what data is being processed in the infrastructure and where
2.	Access to sensitive information by insecure, unmanaged devices
3.	Misuse by organizational insiders
4.	Not knowing with certainty where sensitive data is geographically located or stored
5.	Unauthorized access to sensitive data by individuals
6.	Inability to audit for user access
7.	Inability to respond to incidents traversing the infrastructure
8.	Poorly configured or secured interfaces (e.g., APIs)
9.	Poor configuration and security of quickly spun-up application components (e.g., containers)
10.	Malware intrusion
11.	Unauthorized access to sensitive data by applications
12.	Unauthorized access to the infrastructure by outsiders
13.	Misconfiguration or vulnerability of hypervisors and other virtualization managers
14.	Recognizing downtime or unavailability of applications when needed

Moving to the cloud drives the need for comprehensive visibility. The 2021 custom survey "Network Security in the Cloud" (not yet published) found that 68% of respondents consider cloud services a core part of their network, with 66% saying that cloud use has grown since the start of the coronavirus pandemic. Nearly 50% of respondents cited the lack of visibility into what data is being processed in the public cloud has become more pronounced as their organizations have moved to a more remote model. According to the SANS 2021 Cloud Security Survey, the leading challenge respondents face in adapting incident response and forensic analysis to the cloud is lack of real-time visibility into events and communications involved in an incident.[11]

Visibility may be best viewed as a means of communication that connects a key organizational question to an outcome/answer (or a set of outcomes/answers) supporting a decision or prompting action. The relationship between risk and visibility in terms of the situational awareness needed to make risk decisions might be summarized as:

Risk + Visibility = Insight and ability to take action

vs.

Risk + No Visibility = No action or wrong action

[10] "Effectively Addressing Advanced Threats," July 2019, www.sans.org/reading-room/whitepapers/analyst/effectively-addressing-advanced-threats-39105, p. 4.

[11] "SANS 2021 Cloud Security Survey," April 2021, www.sans.org/reading-room/whitepapers/analyst/2021-cloud-security-survey-40225, p. 10.

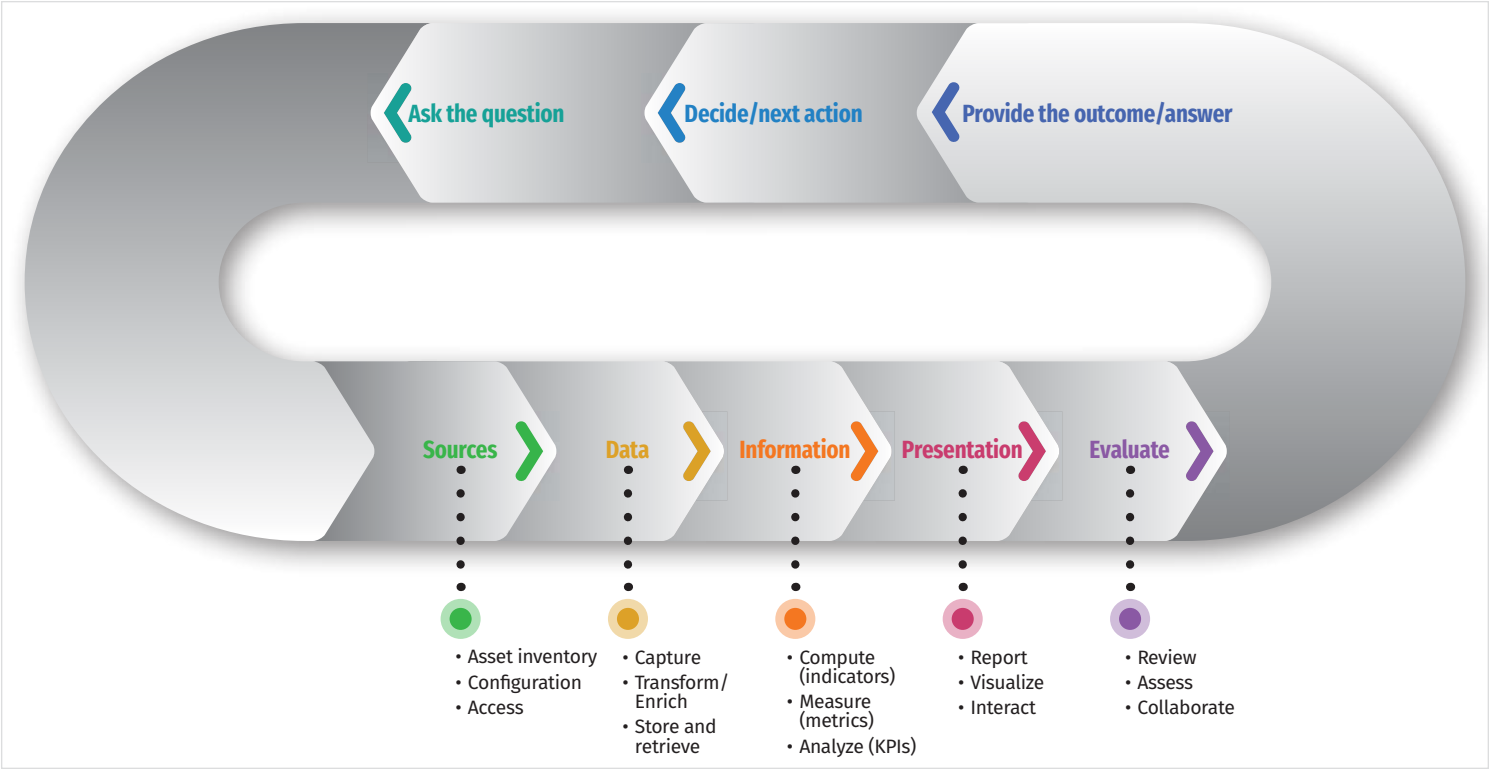

Figure 3. Visibility Road Map Relationships

Figure 3 outlines the set of steps that constitute the road map to achieving visibility.

In the following sections, we will discuss each step—with the caveat that many depend on the use of data science and analytics best practices. This paper will touch on pertinent details, but not go into great depth.

Sources: Consider What You Can't See

IT and security professionals alike recognize the important of knowing what is in their infrastructure. Most professionals who responded to the 2020 SANS Network Visibility and Threat Detection Survey feel that a lack of visibility into the devices on their network poses a high risk.[12] In addition, results from a recent study indicate that nearly 80% of organizations with a lack of visibility into their assets report roughly three times as many incidents.[13]

Visibility into what is on your infrastructure versus what you are managing is critical to visibility from two key standpoints. First, knowing what is attached to your infrastructure enables you to gain insight into the full view of what you (or your SOC) are tasked with securing and what issues might be occurring—that is, what are possible vulnerabilities, and what potentially latent issues might allow an attacker to take advantage of those vulnerabilities? Here, the use of offensive security solutions to assess the organizational attack surface can be crucial to distinguishing between all assets and those assets that are at risk from actual attacks. Activities such as pentesting and red teaming exercises can reveal real-world issues that you can't see (but attackers can).

[12] "2020 SANS Network Visibility and Threat Detection Survey," March 2020, www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490, p. 5.

[13] "Study Shows 79% of Organizations Acknowledge an Asset Visibility Gap, Leading to 3X More Incidents," www.bloomberg.com/press-releases/2021-04-27/study-shows-79-of-organizations-acknowledge-an-asset-visibility-gap-leading-to-3x-more-incidents

The second key reason to understand your infrastructure is that you need to know and trust what sources can provide reliable data, enabling you to gain insight into what is going on. Are there any gaps in the sources of the data you are looking to collect for visibility? Do your visibility requirements necessitate the inclusion of any new devices?

Detecting and characterizing those rogue devices generally requires use of multiple visibility methods. Rogue devices rarely will have cooperative host-based security agents and often will not respond to simple network scans. Use of DNS records and/or network access control (NAC) system logs can enhance visibility into rogue elements.

The CIS Controls described here are a starting point for a proactive approach to managing sources, especially with the implementation of the following CIS Control families:

- **CIS Control 1: Inventory and Control of Enterprise Assets**
  This control family actively manages (inventories, tracks and corrects) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things [IoT] devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. It also supports identifying unauthorized and unmanaged assets to remove or remediate.[14]
- **CIS Control 2: Inventory and Control of Software Assets**
  This control actively manages (inventories, tracks and corrects) all software (operating systems and applications) on the network so that only authorized software is installed and can execute and so that unauthorized and unmanaged software is found and prevented from installation or execution.[15]
- **CIS Control 4: Secure Configuration of Enterprise Assets and Software**
  This control establishes and maintains the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).[16]
- **CIS Control 5: Account Management**
  This control uses processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts and service accounts, to enterprise assets and software.[17] It works together with CIS Control 6.
- **CIS Control 6: Access Control Management**
  This control uses processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator and service accounts for enterprise assets and software.[18]

> **"Basically, you want to know what assets are attached to your infrastructure, how they are configured, whether they are managed and who can access them. Obviously, you want to try for 100% on all counts, but that may not always be possible.**
>
> **"Another metric I frequently use is 'well-managed versus wilderness percentage.' There will be unmanaged devices on most networks. I'd like a representation of what the percentage of assets observed on the network [are] versus assets we assert we have full cybersecurity instrumentation installed."**
>
> **—Chris Crowley, Senior Instructor and SOC Course Author, SANS**

[14] www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets
[15] www.cisecurity.org/controls/inventory-and-control-of-software-assets
[16] www.cisecurity.org/controls/secure-configuration-of-enterprise-assets-and-software
[17] www.cisecurity.org/controls/account-management
[18] www.cisecurity.org/controls/access-control-management

Data, Data Everywhere

Especially in the world of cloud computing, security visibility is data-driven, dependent on data collection—both subjective and objective—from various sources. Data relevant to visibility can be broadly separated into two categories: endpoint (including mobile devices, workstations, server, virtual devices and IoT) and network.

Endpoint data typically includes OS and version, information regarding running applications and processes, user context and network data, including port utilization and established connections. Respondents to the SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey[19] also would like to be able to acquire better visibility into sensitive data (e.g., personal health information, proprietary company information) stored or used on an endpoint, memory-based artifacts and machine-to-machine connections.

The network, however, remains the lowest common denominator. Table 2 shows data that is currently collected from networks, according to the SANS 2020 Network Visibility and Threat Detection Survey.[20]

From the currently unpublished results from a 2021 SANS survey,[22] **50% of respondents actively use network metadata to prevent, detect or respond to threats in the public cloud, with 81% using and collecting traditional L2-L4 network (NetFlow) data and 75% using application-level metadata**, allowing the successful identification of:

- Behavioral patterns of network communications
- Advanced tactics, techniques and procedures (TTPs)
- Rogue assets and services
- Command and control (C2) traffic
- Specific network indicators of compromise (IoCs)

"The single best metric for assessing visibility is [the] ability to sweep the enterprise. This can be both a time-based metric and a quality (percent completion) metric. The measurement is: Given a specific indicator of compromise (including but not limited to: file, file hash, mutex, hostname, IP address, user account), how long would it take you to assess 80%, 90% and 100% of assets under your control for the presence of that indicator? The asset can be further subdivided into categories such as: servers, workstations, mobile devices, or other appropriate categories."

—Chris Crowley, Senior Instructor and SOC Course Author, SANS

Table 2. Network Data Collected[21]

Data Type	% Who Collect
Active directory/LDAP login attempts	89.2%
DNS transactions	71.4%
DHCP transactions	64.0%
HTTP payloads	62.1%
IPFIX/NetFlow/Host-to-host connection data	60.1%
Certifcate metadata	43.8%
SMB/CIFS methods	41.9%
Database methods	40.4%
Other	2.0%

Encrypted Traffic: An Impediment to Network Visibility

In the 2020 Cloud IR Survey,[23] close to a third of respondents (32%) cited inadequate visibility into encrypted network traffic as a key impediment to effective cloud IR at their organization.

Close to 40% of respondents to the SANS 2020 Network Visibility and Threat Detection Survey said that 50–74% of their internal network traffic is encrypted, and most respondents indicated that they worry about encrypted traffic obscuring visibility into threats on the network.[24] Yet, if the 2019 SANS SOC survey is any indication, most are not using any type of TLS interception, even if the technology has been implemented.

This raises the subsequent concern as to why organizations *aren't* using decryption to achieve visibility. Is it because of privacy concerns? Or are the reasons more technical, such as performance limitations due to the decryption process?

[19] "SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey," March 2021, www.sans.org/reading-room/whitepapers/analyst/2021-endpoint-monitoring-dispersed-workforce-survey-40200 (Note: This data is from survey results not included in paper.)

[20] "SANS 2020 Network Visibility and Threat Detection Survey," April 2020, www.sans.org/reading-room/whitepapers/detection/paper/39490, p. 4.

[21] www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490, p. 8.

[22] "A SANS Survey: Network Security in the Cloud," to be published June 2021, www.sans.org/reading-room/whitepapers/analyst

[23] "2020 SANS Enterprise Cloud Incident Response Survey," September 2020, www.sans.org/reading-room/whitepapers/cloud/paper/39805, p. 6.

[24] "SANS 2020 Network Visibility and Threat Detection Survey," April 2020, www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490, p. 7.

Data collection has its own unique set of questions and metrics, as shown in Figure 4.

A Focus on Information

Capturing source data and correctly transforming it into information is the key next step for measurement and assurance. Analytics algorithms (rule-based or AI/ML based) sort data, then convert it into actionable information (metrics and KPIs).

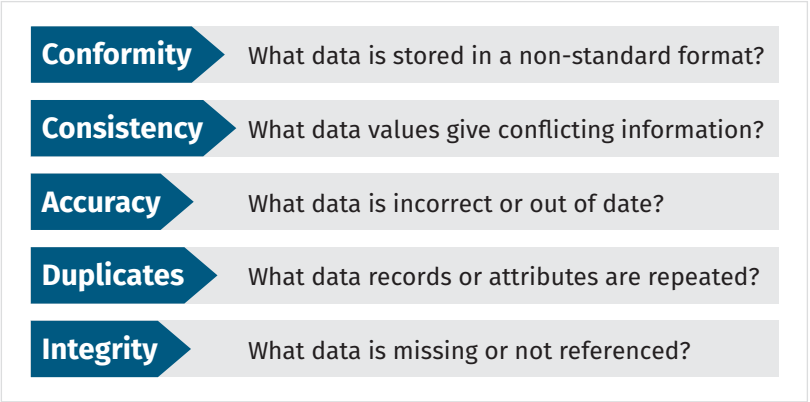

Figure 4. Data Quality Metrics[25]

Metrics and Measurement

In simplest form, a metric is nothing more than a measurement recorded to track some aspect of business activity and measure the success or failure of that activity's performance. Metrics are quantifiable, allowing an organization to specifically state results and show how well the actual activities are performing with respect to a set target.

What is challenging here is selecting the key metrics and then—because an unused metric is worthless—determining their effectiveness. Developing usable metrics is not as simple as it sounds. See Figure 5.

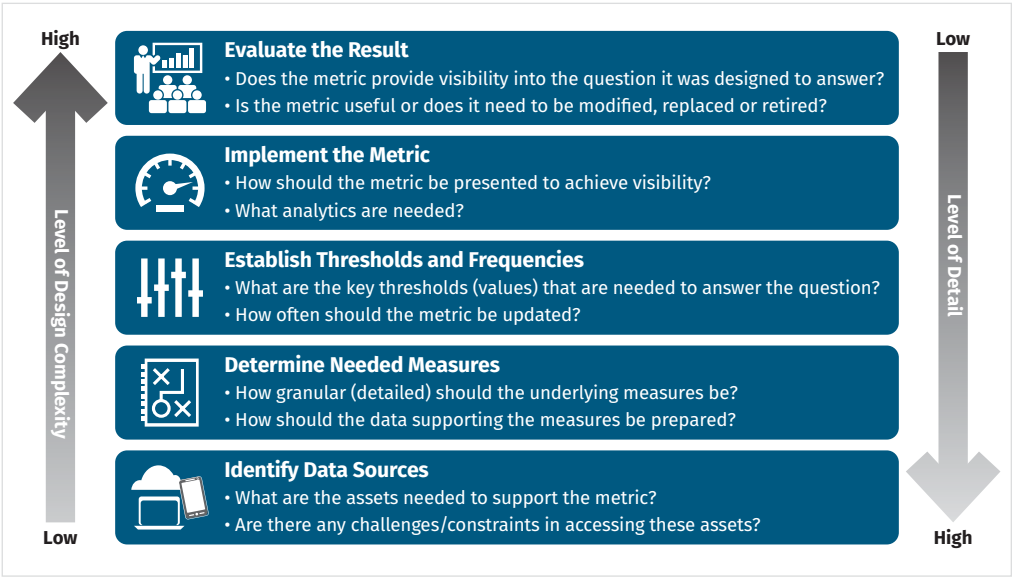

Figure 5. Deriving Information from Data: Building Metrics[26]

The level of detail is highest at the lowest level of design complexity, where the greatest number of data elements will be collected from various endpoints. The level of detail decreases as design complexity increases, where this data ultimately will be aggregated, rolled up into chunks of information for presentation to stakeholders.

Measuring the Business: Security Performance Indicators

How do you achieve visibility into how effective your organization is when it comes to achieving its security business objectives? Performance indicators. While metrics track the status of a specific business process, performance indicators track whether the organization hits its business objectives/targets.

"We don't have an industry standard measurement framework that helps define this across all these areas. Certainly, we have things like MITRE ATT&CK™ that have done a great job in the detect area, but we don't have anything comprehensive for identify and protect, for example. And we don't have anything for the key business processes that security teams need to support."

—Frank Kim, Fellow, SANS

[25] https://datacadamia.com/data/quality/metric

[26] "Improving the Bottom Line with Effective Security Metrics: A SANS Survey," August 2020, www.sans.org/reading-room/whitepapers/analyst/improving-bottom-line-effective-security-metrics-survey-39720, p. 11.

Here's a simple example to indicate the distinction between metrics and performance indicators:

- **Metric (level of preparedness, but no business context regarding business objective)—**This is the number of devices on your network that are fully patched and up-to-date.
- **Business objective—**At least 80% of devices on the network should be fully patched and up-to-date.
- **Performance indicator—**The ratio of the number of devices from the first bullet above to the number of devices known on the network is less than 80%.

In short, every performance indicator is a metric, but not every metric is a performance indicator. The key difference is that the performance indicator measures how the organization approaches security and how successful that approach may be. A security performance indicator can provide visibility as to where action is needed for improvement, but not necessarily what action.

From another perspective, a performance indicator could correlate metrics around the exploitability and severity of a threat with an established business objective, the actual cost of the corresponding control. Management can then use this performance indicator to evaluate the cost of risk mitigation versus the actual impact to the business if the risk is realized.

Communicating (aka Visualizing) Security

The final step is communicating visibility. With a constantly changing threat landscape, ever-evolving threat surfaces and new threat vectors, traditional static presentation methods, such as standalone spreadsheets, reports or modular governance tools, may not be thorough enough nor effective. Stakeholders need dynamic, real-time, actionable insights.

This doesn't mean that static reports are no longer relevant. They are, especially for retrospective (historical/reactive) or forensic purposes. But when moving to a proactive or predictive security stance, the challenge becomes how to present actionable information—metrics and performance indicators—that reveal the real-time state of organizational cybersecurity in a way that is both easy to understand and act upon. There is a need for a unified view that combines data from key cybersecurity controls, rolls it up into a single actionable dashboard and provides clear insights into an organization's cybersecurity posture.

Visualization techniques make understanding easier, supporting actionable decisions regarding detection, prediction and prevention. Automation and analytics can work hand-in-hand with real-time presentation (i.e., visualization) to address the concerns around detection, prediction and prevention.

"A dashboard is a visual display of the most important information needed to achieve one or more objectives; consolidated and arranged on a single screen so the information can be monitored at a glance."

—Stephen Few, Founder and Principal, Perceptual Edge[27]

[27] "Dashboard Confusion Revisited," http://perceptualedge.com/articles/visual_business_intelligence/dboard_confusion_revisited.pdf, p. 1.

An in-depth discussion of visualization and other techniques is beyond the scope of this paper, but keep in mind the following pointers:[28]

- Focus on the important aspects and don't overload your dashboards. If everything is treated as important, nothing will be perceived as important.
- Make the important messages obvious by using sight, sound and haptics, and have those messages stand out against an uncluttered background. The KISS principle applies here.
- Limit time wasted on saccadic movement. Scanning is important in instrumented flying, and the same applies here.
- Keep in mind the display medium (e.g., paper, tablet, overhead screen).
- Try to avoid the third dimension. Paper and display screens are two-dimensional, so keep this in mind when presenting results.

A dashboard is an excellent tool for the presentation of real-time information. Designed properly, an effective cybersecurity dashboard can foster good decision making by offering actionable insights. One way it does this is by simplifying details about intricate key risk indicators and complicated visuals to communicate the most essential information. A good dashboard can help break down cybersecurity silos by bringing together a unified, holistic view based on data from different cybersecurity controls.

Dashboards are not a new concept, although the concept seems to get reinvented as revolutionary every few years. Although they are incredible tools, dashboards take work and resources to develop. This may be one reason only 5% of respondents to the 2020 SANS Metrics Survey reported that they track, analyze and report on metrics using an integrated dashboard with complete, ongoing visibility into performance metrics.[29] So, don't be afraid to go beyond dashboards!

The real goal is to seek out timely ways to accurately (and attractively) communicate the most critical information needed for stakeholders to visualize and conceptualize the complete story regarding the organization's current security posture.

Success Patterns for Visibility

Once you've decided how you define security visibility for your organization, the next step is the aforementioned gap analysis: Where are you, and where should you be? The former is relatively easy to do; the latter is highly dependent on the specific business, technology and threat environments you face. To succeed, any effort to develop or enhance security visibility needs to define an end-state visibility goal and the strategies required to get there.

---

[28] Rudis, Bob and Jay Jacobs. *Data-Driven Security: Analysis, Visualization and Dashboards*. Wiley, 2014.

[29] "Improving the Bottom Line with Effective Security Metrics: A SANS Survey," August 2020, www.sans.org/reading-room/whitepapers/analyst/improving-bottom-line-effective-security-metrics-survey-39720, p. 16.

One approach is to base this on a maturity model[30] approach, where higher levels of visibility maturity are tied to business benefits. This is most effective if the organization is already using the maturity model approach[31] for IT operations or its overall cybersecurity program. However, while formal maturity models are powerful for communicating to boards and CXOs, they carry a lot of overhead to maintain and track.

If the organization does not already use a maturity model, another approach is to look at common patterns of visibility effectiveness to define where the organization is now and how it could progress toward a higher level of performance and business benefit (see Figure 6.)

Figure 6. Success Pattern for Visibility

[30] "Cybersecurity Capability Maturity Model," U.S. Department of Energy, February 2014, http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[31] "Improving Detection, Prevention and Response with Security Maturity Modeling," May 2015, www.sans.org/reading-room/whitepapers/analyst/improving-detection-prevention-response-security-maturity-modeling-35985

The Road to Improvement

Visibility is a subjective topic—it means different things to different stakeholders. Consequently, the gaps in developing a visibility strategy abound, whether related to on-prem security, cloud or supply chain. Many perceived (or actual) gaps occur because security professionals have yet to span the chasm between a technical mindset and an understanding of the business. To again quote Frank Kim, "Business process and analyzing metrics and turning data into insights [is] about where risk actually lies. A barrier is lack of understanding of business drivers."

The human factor also must be addressed. According to Lance Spitzer, organizations need to dramatically improve visibility into their top human risks and their ability to manage those human risks. Oddly enough, the biggest barrier is that security teams often do not take human security seriously and may not even perceive it as their job. Too often, security awareness is perceived as "entertainment," effectively trivializing the subject of security when, in fact, raising awareness is critical to managing overall organizational risk, not just securing the human. This is a perception that, according to Spitzer, is—thankfully—starting to change.

Cloud computing is reshaping our world to be one that is both software- and data-driven. Visibility needs to improve across development and operations silos, including visibility into actual code: what is in code, what code is being changed and how often, who is authorized to change it, and how is it being built, tested and deployed.

Within an organization, management and security teams need to come together to achieve a strong security culture—one that is both top down and bottom up. To do this, they need to create a common "security business language" for the organization. If the security team cannot address business objectives, there is little hope that it will be effective in working with management to dramatically reduce business risk, especially in areas where the security team may otherwise have limited influence.

Summary

Even with the subjective nature of visibility, organizations can take steps to define and then measure it. In this paper, SANS has presented an objectives approach—a road map—to help organizations establish a strategy. Given that visibility in a cyber world remains data-driven, here's some basic advice for moving forward:

- State your objectives and any assumptions/constraints.
  - Decide on your objectives. What questions do you need to answer? What processes must you monitor? Which trends do you want to track?
  - Understand the roles of each audience. The C-suite may not have the same issues (or attention span) as your SOC director or analyst.
- Identify what you need to achieve your objective. What sources and data do you need to monitor the processes or track trends?
- Frame your outcomes so that your questions have objective answers. Establish meaningful metrics that measure how well things are working and can be used to identify important trends. But be careful to guard against expectation bias.
- Don't get caught up in the analytics or presentation/visualization "art." Let the data and the information speak for itself.

Above all, keep in mind the success patterns for visibility as your organization moves from no visibility through reactive to proactive and ultimately predictive security practices.

"Visibility into software development and coding is especially important where dev/ops teams are treating configuration as code—modeling run-time configuration in code and making configuration changes to run-time stacks in code—because this code captures [and] describes the infrastructure attack surface, and makes changes to the attack surface more transparent, more traceable and more testable.

"And as we have seen with the SolarWinds SUNBURST vulnerability, visibility into the code build toolchains and workflows is critical in protecting the organization from attack—attacks on the build pipeline have moved from theoretical to real."

—Jim Bird, Analyst, SANS

About the Authors

Barbara Filkins, SANS Research Director, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

John Pescatore joined SANS as Director of Emerging Security Trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this paper's sponsor:

Infoblox®