CHAPTER 3  
Tools and Techniques for Detecting Cyber Incidents

**Overview of Chapter and Objective**

This chapter aims to help the reader describe effective techniques for detecting cyber incidents or attacks, establish best approaches for monitoring systems to detect incidents, and plan for the development of organizational processes for detecting incidents.

**O**livia settled into her office early that day at 8:00 a.m., hoping to catch up on the news before starting the daily system maintenance tasks she undertook as a junior systems administrator at her non-profit, non-governmental organization (NGO). She checked out Google News, the New York Times, and then moved on to the Mapleton Daily Gazette’s home page, which she considered the best local news source. The paper’s reporters were particularly excellent in covering the city’s local government.

She clicked on the Gazette’s bookmark below her browser bar, and nothing appeared on the screen. Must have made a mistake, she thought, so she clicked on it again. Nothing. Then she manually typed the URL into the browser bar. Still nothing. She tried again. This time the paper’s home page appeared. Metropolitan Broadband, the NGO’s broadband provider, must be working on the network again and causing intermittent outages, Olivia thought. She scanned the newspaper’s home page, and nothing interested her, so she turned to her e-mail.

She bolted upright when she saw thirty alerts from her anomaly detection system, with more pouring in every second. The alerts warned of two things: a spike in “503 service unavailable” instances for the organization’s website and a surge of requests from DNS addresses outside the usual geographic locations her organization attracted.

She opened the dashboard for the anomaly detection system. She saw that her organization’s website had experienced five thousand instances of “503 service unavailable” messages in the past 30 minutes, which far exceeded the usual five cases per month. Moreover, the DNS addresses outside the top 10 geographic locations that usually visit the organization’s website were two thousand times the amount they should be.

Olivia immediately recognized that these anomalies meant someone had leveled a distributed denial-of-service (DDoS) attack at her organization, and the attack was likely a big one – a domain name system (DNS) amplification attack. She knew that an attack like this could take the organization’s website down for days, which could eat into revenues and donations, not to mention generate lousy press and anger against the parent organization’s leaders. Olivia and the rest of the NGO’s staff had suspected that some discontented group or person could aim a significant DDoS attack at the NGO because of its frequent controversial stances. That’s why they were ready for such an eventuality.

She alerted the team to handle significant attacks like this, including the NGO’s technology vice president, the general manager, the general counsel, and her subordinate, the organization’s webmaster. But Olivia knew just what to do.

Months earlier, the NGO had switched to a new cloud content delivery network and cloud services provider who had walked her through their security capabilities and demonstrated a unique solution for heading off DDoS attacks at the outset. She called her contact at the company, who launched a new “red alert” system for allocating resources to ward off major DDoS attacks.

Within minutes, the organization’s website was operating normally, and the onslaught of alerts in Olivia’s inbox diminished. Over the next couple of weeks, the NGO team responsible for handling how attacks are detected and mitigated conducted a review and issued a report to all relevant personnel. This review offered an assessment of how the organization mitigated the incident and detailed steps for managing a similar incident in the future. Olivia, in particular, received praise for how prepared she was for the incident and how well she handled it.

**INTRODUCTION**

Welcome to Tools and Techniques for Detecting a Cyber Incidents. This chapter will help you gain skills that allowed Olivia to navigate a significant incident successfully.

We will introduce you to some key concepts for detecting cyber incidents, including:

* the importance of anomalies in the functioning of your systems and devices and how to detect them,
* how to establish monitoring systems that spot anomalies and events on an automated basis, and
* how to develop sound approaches to establishing organizational processes around detecting anomalies and events.

No technology system is secure if the organization does not have the means for first detecting a cyberattack. Before we learn how to catch a cyberattack, we’ll spend a few minutes on a bit of background.

**WHAT IS AN INCIDENT?**

The very notion of a cyberattack justifiably strikes fear in the heart of most technologists. Internet protocol technology appears in not only traditional IT and communications technology; it also appears throughout OT-specific systems, as well as home appliances, automobiles, stoplights, security cameras, and even clothing. Therefore, the attack surface for cyber intrusions and destruction grows exponentially every day.

**Voices of Experience  
*On Why Detect Is “Right of Boom”***

**Detect Looks for Weakness Exploitations**

*When I look at the NIST cybersecurity framework, I see these different words like identify, protect, detect, respond, recover. The way that I look at the distinction is by creating this noticeably clear division between left and right of boom [before and after an incident]. So, on the functions about identify and protect, that is left of boom. Boom occurs between protect and detect. Detect, respond, recover is right of boom. When it comes to vulnerabilities, they are*

*a structural weakness. Structural weaknesses are things that you find left of boom. Exploitation against those vulnerabilities is something that happens right of boom and when something gets exploited you want to go discover the exploitation*.

*Here lies the ability for us to really distinguish the meaning of identify versus detect. When it comes to the function of identify, which is left of boom, we are trying to discover these exposed weaknesses that we have in our environment. When it comes to right of boom, and the function of detect, we are looking for exploitation against those weaknesses*.

Sounil Yu, Author of the Cyber Defense Matrix, former Chief Security Scientist of Bank of America

The term cyberattack is a moving target as digital threats multiply. For this chapter’s purpose, we define “cyberattack” as an attempt to bypass security mechanisms put in place for IT and OT systems, to otherwise use an IT or OT system without authorization, or to abuse existing privileges. Most cybersecurity professionals draw sharp lines around what constitutes attacks, preferring such cybersecurity incidents as unauthorized access to be called just that, “incidents,” rather than the more inflammatory term “attacks.”

To detect exploitation of assets or “cyberattacks,” it’s vital to have ethical rules and security controls in place. This chapter will walk you through some of the most critical elements of these rules and controls.

**I. DETECT**

Detecting a cyber incident has become an ever-increasing challenge, particularly for large organizations, because of continuous change in the various systems used within the organization. Threat actors can hide their tracks within what appear to be ever-more-complex processes, with indicators of an attack or intrusion shifting constantly. Detecting anomalous or destructive system changes amid thousands, tens of thousands, or even millions of routine changes is the key to identifying a malicious cyber incident and potentially saving your organization from complete operational failure.

Cybercriminals can hide their tracks through disguise, obfuscation, and increasingly innovative methods that take advantage of undiscovered vulnerabilities, also known as “zero days.” Therefore, the most critical function of the NIST Framework in detecting a malicious cyber incident is, aptly enough, the Detect function.

We’ll walk you through crucial categories and subcategories of the Detect function so that you can understand:

* what anomalies and events are and how to detect them,
* how to establish monitoring systems to spot anomalies and events on an automated basis, and
* how to develop sound approaches to establishing organizational processes around detecting anomalies and events.

Before we move on to more details about anomalies and events, it’s important to highlight that one noteworthy trend in cybersecurity defense is the rise of community and commercial threat intelligence feeds. These feeds enable dynamic searching for malicious changes (also called indicators of compromise) such as IP addresses associated with malicious attacks, malware file names and hashes, and specific attack vectors. Many organizations have figured out how to ingest these feeds to enhance their automated intrusion detection systems.

These systems can help you gain real-time knowledge across assets, including understanding when malicious changes occur. Threat intelligence feeds can help organizations respond to cyberattacks more quickly and shift resources where needed in response to attack patterns. We’ll return to the topic of threat intelligence and intrusion detection systems later.

**A. Anomalies and Events**

To detect a cyber incident, you should first implement controls that detect anomalies and grasp the events’ potential impact. The outcome of this component in the NIST Framework is defined as “anomalous activity is detected in a timely manner and the potential impact of events is understood.” By their very definition, anomalies are low-probability events, outliers, surprises, and exceptions that happen so infrequently that most IT experts can’t prepare for them, making them very hard to detect.

An excellent example of anomaly detection is how banks catch fraudulent users. Over the years, banks have developed anomaly detection systems that sniff out fraud in credit and debit card use and establish norms that indicate unusual patterns or locations of purchases, often on a customer-by-customer basis. When violated, the banks’ fraud departments are alerted and can freeze accounts and notify customers. Anything that appears to be suspicious, whether it is a pattern of purchases, locations of purchases, or even types of purchases, is fed into banking anomaly detection systems for further analysis and action.

To detect anomalies, however, a baseline of what is normal has to be established first. Using the banking example, a bank might determine that a $1 charge by any customer in three different cities within a five-minute frame is not a regular expenditure and will flag those charges as anomalies. Some customers, however, might have legitimate reasons for incurring single dollar charges across multiple cities within a short time frame. In those cases, banks’ anomaly detection systems can ignore those transactions for those customers.

For anomaly detection systems to be effective and avoid sending too many alerts, a method for detecting anomalies must be based on a classification system that determines the difference between a “good” anomaly and a “bad” anomaly. You should continually modify any anomaly detection system you use to distinguish between the two. For example, the system might flag a new computer added to a network at first as an anomaly with alerts sent to IT staff. But, when the system is updated to accept the new computer as standard, it sends no alert.

This section of the chapter will walk you through some of the basic concepts of detecting and managing anomalous events.

**1. Establish Baseline Data for Normal, Regular Traffic Activity and Standard Configuration for Network Devices**

(DE.AE-1: A baseline of network operations and expected data flow for users and systems is established and managed.)

Before any anomaly can be detected, it is fundamental to determine what is “normal” by establishing baseline data so that you can track deviations from that data.

**Voices of Experience  
*On Anomalies and Events***

**Start Off with a Strong Foundation**

*For anomalies and events, we want to be looking at what’s happening in our environment. It’s interesting to look at the wording that NIST uses, “ensure a baseline.” You want to start off with a strong foundation. My role in a security engineering organization is to look at every source and really think about what we expect to see there. You build out your expectations from different sources. We should have started with asset management to have a sense of everything that we’re supposed to be watching in our environment. I know that a significant portion of our systems are not even talking to us at all. Maybe the agents were never installed, or the agents were installed, and they had an issue or the operating system shut them down, or there was a network problem between the system and wherever it is that you’re storing these events and the logs aren’t coming in. The worst time to find out this is happening is when you have an incident*.

Omer Singer, Head of Cyber Security Strategy, Snowflake

Establishing baseline data requires tracking many different attributes across multiple dimensions, including normal host behavior, normal user behavior, application behavior, and numerous other factors, including external factors such as IP reputation. Time is also a factor in establishing the baseline. For example, suppose a user legitimately accesses a file over and over again over weeks. In that case, that might be an anomaly not captured if the baseline timeframe is only a week for tracking incidents of that file access.

Although we’re using the term anomaly, a more accurate explanation might be “pattern of contrast” rather than static data points of “normal” and “abnormal.” Attackers can quickly adapt to static baselines, but dynamic patterns that are tracked over time and continually updated can help thwart attacker efforts to elude detection.

A frequently cited example of this pattern of contrasts is the use of dynamic DNS (domain name system) services. When the use of these services is at a low of 0.5% of regular DNS traffic, an increase to 5% is an anomaly that you should investigate because bad actors have repeatedly used dynamic DNS as part of malware campaigns.

Another good example is monitoring outbound server connections that follow a set interval. For instance, if you discover a service or server calls out precisely every 10 minutes to a set of IPs, this might be an indicator of a compromised system contacting its command and control (C&C) master.

Anomalies or patterns of contrast can apply to anything across your technical assets and are highly contingent on your organization’s systems, configuration, personnel, hardware and software assets, and many other factors. Some examples might include:

* a database server that suddenly has a lot of outbound traffic,
* a workstation trying to connect to many other hosts at once,
* a file server busy in the middle of the night when it usually is idle,
* firewall hits from a country with which your organization does no business, and
* one of your assets suddenly points to a new IP address that it had not pointed to before.

**Relevant Technical Standards for DE.AE-1**

**A baseline of network operations and expected data flows for users and systems is established and managed**

* CIS CSC 1, 4, 6, 12, 13, 15, 16
* COBIT 5 DSS03.01
* ISA 62443-2-1:2009 4.4.3.3
* ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2
* NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4

1. **2. Monitor Systems with Intrusion Detection Systems and Establish a Way of Sending and Receiving Notifications of Detected Events; Establish a Means of Verifying, Assessing, and Tracking the Source of Anomalies**  
   (DE.AE-2: Detected events are analyzed to understand attack targets and methods.)

You should perform two tasks when detecting anomalies:

* Monitor systems with tools known as intrusion detection systems.
* Send and receive notifications of detected anomalies.

These tasks are challenging because many (if not most) administrators don’t know the type of network traffic allowed in their systems. Other potential problems include:

* External parties, such as vendors, may block intrusion detection traffic.
* Networks must continue to operate while intrusion detection systems run.
* Intrusion detection systems often spit out misleading, uninformative, or false-positive messages.

Therefore, the organization’s customization is required for the intrusion detection system to help these and many other challenges.

*Once an anomaly is detected, technical personnel should:*

* verify, assess, and track the source of the anomaly and
* assess the incident’s magnitude and consequences.

Endpoint detection and response (EDR) platforms have emerged in the past decade to bring these capabilities into the hands of more organizations. The idea is that a resident software agent monitors processes, connections, and behavior on each host. These are each logged and stored before being presented on dashboards and other analytical tools to administrators. When any abnormal activity is detected, the agent allows the administrator to address the issue almost surgically. Administrators also can find similar detections across other systems with agents installed, shut off network connectivity altogether on impacted systems, or continue to monitor malicious behavior to determine the attackers’ actual targets.

Based on the risk assessment that the organization has conducted, you might deem some incidents as unimportant because the cost of addressing the incident outweighs its potential risk. For others, simple solutions might be available, such as turning off ports or reinstalling the software.

Once the anomaly is detected, verified, and its impact assessed, it helps identify the anomaly source. Often your organizational knowledge is enough to identify the source of a malicious incident. Sometimes, technical personnel have to collaborate with specialists, such as forensics experts, to determine the problem’s source. Other times technical personnel may choose to simulate the incident in a contained and safe way to determine its origin.

**Relevant Technical Standards for DE.AE-2**

**Detected events are analyzed to understand attack targets and methods**

* CIS CSC 3, 6, 13, 15
* COBIT 5 DSS05.07
* ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
* ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
* ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4
* NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4

**A WORD ABOUT ANTIVIRUS SOFTWARE**

Antivirus software is a monitoring tool that can help detect attacks. Although it’s not technically considered an intrusion detection system, antivirus software has become a necessary tool for preventing cybersecurity incidents.

The antivirus software market is filled with vendors, each with its unique advantages and disadvantages. It’s worthwhile to analyze each vendor’s offerings to see what specific features best fit your situation.

In its *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (NIST Special Publication 800-83 Revision 1), NIST recommends that antivirus solutions have the following capabilities:

* Scanning critical host components such as startup files and boot records.
* Watching real-time activities on hosts to check for suspicious activity, such as scanning e-mail and e-mail attachments for malware.
* Monitoring the behavior of typical applications such as e-mail clients, web browsers, and instant messaging software, particularly for those applications likely to be conduits for malware.
* Scanning files for known malware, including all hard drive scanning and user-initiated scans.
* Disinfecting files, which refers to removing malware from within a file.
* Quarantining files, which means that files containing malware are stored in isolation for future disinfection or examination.
* Identifying common types of malware as well as attacker tools.

NIST also recommends that organizations deploy antivirus software that uses both host- and network-based scanning. Finally, NIST recommends that organizations use centrally managed antivirus software controlled and monitored regularly by antivirus administrators responsible for its acquisition, updating, and testing throughout the organization.

You can experience conflicts between your antivirus software and some of your vendors’ software. Make sure you continue scanning data files and USB files in particular. Try resolving conflicts between your antivirus system and the vendors’ software by avoiding scans of core application files or database files.

1. **3. Deploy One or More Centralized Log File Monitors and Configure Logging Devices throughout the Organization to Send Data Back to the Centralized Log Monitor**  
   (DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.)

As each event in a system occurs, the intrusion detection system stores data surrounding that event, reviews each log event, and looks for patterns associated with an intrusion or attack. While an individual intrusion detection system can look at only one system, a log file monitor can examine data across multiple systems.

Information regarding an incident might end up recorded in several places, such as firewalls, routers, network IDPSs (intrusion detection and protection systems), host IDPSs, and application logs. For the intrusion detection (and prevention) system to work, it’s crucial to create a centralized log file.

A log file monitor can look at multiple logs from different systems. Make sure to configure all your systems and devices to send data back to the log file monitor. These systems are commonly referred to as security information and event management or SIEMs.

A recent shift in vendor solutions and practitioners’ usage has embraced user and entity behavior analytics (UEBA). These systems bring more analytics capabilities into the storage systems than SIEMs that store logs and use pre-written correlation rules to produce alerts. With more data flowing from devices and attacks increasing, you should seek solutions that create high fidelity on alerts over those that merely ingest and change logs.

**Relevant Technical Standards for DE.AE-3**

**Event data are collected and correlated from multiple sources and sensors**

* CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16
* COBIT 5 BAI08.02
* ISA 62443-3-3:2013 SR 6.1
* ISO/IEC 27001:2013 A.12.4.1, A.16.1.7
* NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

1. **4. Determine the Impact of Events Both Before and After they Occur**  
   (DE.AE-4: Impact of events is determined.)

Be proactive in determining events before they happen, a task that is made easier based on your organization’s risk assessment scenarios. However, you cannot gauge all events in advance, even though most IT and security specialists have some sense of the risks they face.

You can document many common attacks and required reactions into your organizational incident response plan. Thinking this through beforehand and agreeing on appropriate steps will allow for a much cleaner response effort. Anytime you can identify a potential incident, you should include it in the incident response plan.

For events that come as a total surprise, assess the impact after it happens. Once the dust has settled, and the incident is fully contained, capture the lessons learned in the response plans. The sooner you can capture this in the response plan, the better the information will be for use in future response activities.

**Relevant Technical Standards for DE.AE-4**

**Impact of events is determined**

* CIS CSC 4, 6
* COBIT 5 APO12.06, DSS03.01
* ISO/IEC 27001:2013 A.16.1.4
* NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4

1. **5. Develop a Threshold for How Many Times an Event Can Occur Before You Take Action**  
   (DE.AE-5: Incident alert thresholds are established.)

Establish thresholds about when to trigger incident alerts or actions taken in response to incident alerts. For example, one anomaly might not trigger an incident alert, but three anomalies within a specified time frame might. (Using the bank example, one major purchase might not trigger an alert, but three purchases in an hour from unusual locations might.) You can also use thresholds to determine privileges for access to system assets (e.g., three consecutive failed admin logins might trigger an alert.). These thresholds should be governed, reviewed, and adjusted over time while learning more about the baseline of activity established under DE.AE-1 described earlier. Use the detection processes to inform other detection and protection capabilities cyclically.

**Relevant Technical Standards for DE.AE-5**

**Incident alert thresholds are established**

* CIS CSC 6, 19
* COBIT 5 APO12.06, DSS03.01
* ISA 62443-2-1:2009 4.2.3.10
* ISO/IEC 27001:2013 A.16.1.4
* NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

**B. Continuous Monitoring**

Given the highly complex nexus of software, the internet, and IP-based connected hardware, it’s impossible to prevent security attacks. That’s why the best solution is to detect attacks as soon as possible.

**Voices of Experience  
*On Continuous Monitoring***

**Continuous Monitoring Needs to Actually Be Continuous**

*The continuous monitoring category controls I have found over and over again, is once you start the process, you don’t stop. You must explain to leadership that, you do not pay for this once and you are done. This is a continuous program you must manage and mature*.

**Continuous Monitoring Needs a Business Case**

*Which sources do I need to monitor that give me the visibility picture I need? We can monitor anything and pull logs, but it needs to make business sense. We need to own what is generating the logs and it should not be owned by a third party. As you pull those logs in, you need to determine what to do with them. The hardest part here are the discussions around if it’s to be a long-term metric that you’re going to be collecting and want to be able to measure overtime in order to know if things get better. Or is it a metric that every quarter you want to know how many incidents you have with a group of people or specific data source? You need to determine if collecting the data will be used to protect an asset or reduce a risk, just to collect the data*.

Gary Hayslip, CISO, Softbank

Periodic assessments are therefore not as efficient as continuous monitoring of systems and assets. Continuous monitoring means uninterrupted monitoring, even if you only collect data at discrete intervals.

While it may not be desirable or practical to monitor everything, at a minimum, you should continuously monitor the systems designated by your organization’s risk assessment as most critical.

This section of the chapter will walk you through strategies for developing continuous monitoring that is optimal for detecting attacks as quickly as possible.

1. **1. Develop Strategies for Detecting Breaches as Soon as Possible, Emphasizing Continuous Surveillance of Systems through Network Monitoring**  
   (DE.CM-1: The network is monitored to detect potential cybersecurity events.)

Because attackers can gain entry into networks and systems from a growing array of vectors, using a wide variety of existing and emerging attack tools, you should develop strategies for detecting breaches as soon as possible. These strategies should take into account all the various openings through which attackers can slide.

Network and host-based monitoring solutions, such as EDR (endpoint detection and response) that oversee systems’ operations via various software tools, are essential in detecting and reporting many assets’ failures. These systems will measure CPU utilization, network bandwidth, and other aspects of operations and send out messages over the network to check if operations are normal. These monitoring solutions should also send out alerts to designated destinations (e-mails, servers, or phones) to notify about anomalies.

There are built-in functions with applications that allow you to monitor devices on the network. One to start with is a traffic analyzer, either virtual or physical. Connecting a laptop or server to ingest network traffic into a security monitoring solution can be a good start.

There are also several open-source and free software solutions available. One solution that stands out for many administrators to begin network monitoring with is Security Onion. Security Onion is an open-source Linux distribution purpose built for threat hunting, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro/Zeek, Wazuh, Sguil, Squert, NetworkMiner, and many other security tools.

There are many network monitoring solutions to choose from, and it’s vital to pick the right one based on your risk assessment, configuration, and strategies for detecting breaches.

**Relevant Technical Standards for DE.CM-1**

**The network is monitored to detect potential cybersecurity events**

* CIS CSC 1, 7, 8, 12, 13, 15, 16
* COBIT 5 DSS01.03, DSS03.05, DSS05.07
* ISA 62443-3-3:2013 SR 6.2
* NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

1. **2. Ensure That Appropriate Access to the Physical Environment Is Monitored, Most Likely through Electronic Monitoring or Alarm Systems**  
   (DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.)

Although it may not always be obvious, monitoring systems and assets’ physical environment is a crucial part of cybersecurity. You can accomplish this physical monitoring in a variety of ways. Most organizations choose electronic monitoring through video cameras connected to recording equipment and closed-circuit TV systems. This method, however, requires human capital in the form of someone watching the video on a 24/7 basis to stop a cyberattack effectively and is most often used in forensic investigations following an attack.

Another method is to put critical assets in locations wired by alarm systems that rely on motion detectors, glass breakage detectors, or contact sensors.

You should correlate physical access data with network or IT access data. One scenario that proves itself is in identifying superhuman travel. As an example, you could monitor VPN access and door access to a campus. Suppose you monitor the logs to alert when those two activities happen within a short space of time. In that case, you could investigate if the user was physically in the building or accessing remotely from home.

**Relevant Technical Standards for DE.CM-2**

**The physical environment is monitored to detect potential cybersecurity events**

* CIS CSC 5, 7, 14, 16
* COBIT 5 DSS05.07
* ISA 62443-3-3:2013 SR 6.2
* ISO/IEC 27001:2013 A.12.4.1, A.12.4.3
* NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11

1. **3. Monitor Employee Behavior in Terms of Both Physical and Electronic Access to Detect Unauthorized Access**  
   (DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats.)

Maintaining a cybersecurity culture means ensuring that employees abide by the security protocols and processes in place. Most cyber incidents stem from misuse or abuse of employee-granted accounts. By monitoring user behavior and tying it to actual humans, you can determine whether the activity is legitimate.

For example, some analytics platforms can determine a baseline for typing speeds of individuals or common access folders. Once a user departs from their established baseline, an alert can fire for investigation. You can assess several behaviors this way, such as logon times, logon locations, attempts to access deactivated or suspended accounts, repeated attempts to use administrative privileges, or even the amount of data saved locally.

Therefore, you should establish methods that monitor employees’ physical and electronic access to systems and document who gains access to facilities and digital assets.

**Relevant Technical Standards for DE.CM-3**

**Personnel activity is monitored to detect potential cybersecurity events**

* CIS CSC 5, 7, 14, 16
* COBIT 5 DSS05.07
* ISA 62443-3-3:2013 SR 6.2
* ISO/IEC 27001:2013 A.12.4.1, A.12.4.3
* NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11

1. **4. Develop a System for Ensuring That Software Is Free of Malicious Code through Software Code Inspection and Vulnerability Assessments**  
   (DE.CM-4: Malicious code is detected.)

Malicious code performs unauthorized functions and causes normal systems operations to become abnormal (e.g., viruses, worms, Trojans, programming flaws, etc.). Therefore, it’s essential to develop systems that check for malicious code in software through various means, including code inspection, independent vulnerability assessments, code compare tools, and more. Ensure that all free software or shareware used in the development process has been certified as free of malicious code.

**Relevant Technical Standards for DE.CM-4**

**Malicious code is detected**

* CIS CSC 4, 7, 8, 12
* COBIT 5 DSS05.01
* ISA 62443-2-1:2009 4.3.4.3.8
* ISA 62443-3-3:2013 SR 3.2
* ISO/IEC 27001:2013 A.12.2.1
* NIST SP 800-53 Rev. 4 SI-3, SI-8

1. **5. Monitor Mobile Code Applications (e.g., Java Applets) for Malicious Activity by Authenticating the Codes’ Origins, Verifying their Integrity, and Limiting the Actions they Can Perform**  
   (DE.CM-5: Unauthorized mobile code is detected.)

Mobile code, such as Java applets, ActiveX, Flash, and a host of intelligent agents, can be executed on one or more hosts other than those for which they were developed. Mobile code is prevalent and versatile, but it is also highly vulnerable to malicious intrusion. Mobile code often attaches to widely used software and frequently requires the download of a plug-in.

Because mobile code has different origins and identities from the software to which it’s attached, you should identify and authenticate the code’s sources. Moreover, you should scan mobile code for integrity, and any actions it performs must be limited through access control or checked through verification controls.

**Relevant Technical Standards for DE.CM-5**

**Unauthorized mobile code is detected**

* CIS CSC 7, 8
* COBIT 5 DSS05.01
* ISA 62443-3-3:2013 SR 2.4
* ISO/IEC 27001:2013 A.12.5.1, A.12.6.2
* NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44

1. **6. Evaluate a Provider’s Internal and External Controls’ Adequacy and Ensure they Develop and Adhere to Appropriate Policies, Procedures, and Standards; Consider the Results of Internal and External Audits**  
   (DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.)

One problem facing security professionals is the lack of control over the security practices of key service providers. An organization can have the best security controls and processes in place, but they are highly compromised if a critical service provider has lax security controls or standards.

Therefore, it’s important to establish methods for evaluating an external provider’s security controls’ adequacy and to ensure they adhere to your organization’s policies, procedures, and standards. Examine any internal or external security audits the provider has available and check in with peers and user groups to gauge whether the provider meets your organization’s standards.

In cases where vendors need remote support, consider giving those vendors some VPN access (preferably through a proxy device) so that they are not at the core of your network. Or offer them remote access that doesn’t expose your sensitive network operations to unnecessary risk. As a start to addressing this control, apply the same or as many as possible controls from monitoring internal systems and employees to your service providers.

**Relevant Technical Standards for DE.CM-6**

**External service provider activity is monitored to detect potential cybersecurity events**

* COBIT 5 APO07.06, APO10.05
* ISO/IEC 27001:2013 A.14.2.7, A.15.2.1
* NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4

1. **7. Monitor Employee Activity for Security Purposes and Assess When Unauthorized Access Occurs**  
   (DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.)

Consider using employee monitoring software for security purposes. However, this monitoring activity may cause concern among employees; you are well-advised to implement this monitoring with great care.

Most IT and cybersecurity professionals have little interest in knowing what employees do outside the security context and typically have no desire to enforce management’s organizational productivity goals. Instead, the purpose of using employee monitoring software is to limit employee actions, often unintentional, that might harm the organization’s security posture.

**Relevant Technical Standards for DE.CM-7**

**Monitoring for unauthorized personnel, connections, devices, and software is performed**

* CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16
* COBIT 5 DSS05.02, DSS05.05
* ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1
* NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4

1. **8. Use Vulnerability Scanning Tools to Find Your Organization’s Weaknesses**  
   (DE.CM-8: Vulnerability scans are performed.)

Vulnerability scanning tools hunt for weaknesses in systems and networks, and cybercriminals use them frequently to find holes that exploit your organization’s digital assets. Their goal is to find devices that are open to known vulnerabilities.

Therefore, organizations should consider using vulnerability scanning tools to search for devices on the network that are open to vulnerabilities before attackers can take advantage of those flaws. These tools will primarily hunt for devices that need patching and, if run thoroughly, can be intrusive and even cause machines to crash.

Be careful in balancing your network and systems’ stability against a thorough enough vulnerability scan, which you should run on a regular schedule to ensure protection. While many organizations run vulnerability scans quarterly or only twice a year, a well-built vulnerability management program will scan more frequently. It would help if you attempted to scan after you deploy bug fixes, code changes, or patches. These post-change scans will allow you to identify assets that fixes didn’t install correctly. It will also allow significantly more time for the production support teams in IT and OT to develop a plan to patch found vulnerabilities.

Be careful when only identifying vulnerabilities and not taking appropriate remediation steps. If you scan and find issues but take no action, your organization might be responsible if an attacker exploits it and it’s made public.

Another risk to manage is the vulnerability scanning platform’s security. Effective solutions will require some elevated credentials to scan systems in your environment thoroughly. Be very diligent in securing the accounts the vulnerability scanning platform uses and keeping them patched and updated. Attackers sometimes target these systems to gain further access into an organization.

**Relevant Technical Standards for DE.CM-8**

**Vulnerability scans are performed**

* CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16
* CIS CSC 4, 20
* COBIT 5 BAI03.10, DSS05.01
* ISO/IEC 27001:2013 A.12.6.1
* NIST SP 800-53 Rev. 4 RA-5

**C. Detection Processes**

Cybersecurity monitoring processes deal with internal management and personnel structures of how cybersecurity incidents are detected and the adoption of policies that support threat detection. Cybersecurity detection processes are a series of practices related to planning, implementing, managing, and testing the policies that support these activities.

These processes track the identification of people who access resources and protect private information – establishing these kinds of methods and policies helps with a forensic examination and enhances detection functions. In some industries, they are even a matter of regulatory compliance. Outside of regulated industries, detection processes apply primarily to large organizations.

The challenges to establishing detection processes in any organization include:

* understanding the need to secure the entire network environment from internal and external threats,
* designing effective security monitoring,
* providing an overall picture of the organization’s security efforts for remediation purposes,
* maintaining policies and practices that correlate security reports with established policies to ease efforts in detecting suspicious activities,
* enforcing security monitoring while balancing business needs, and
* determining acceptable risk levels.

In the next section of this chapter, we’ll walk you through some critical factors you need to know to establish your organization’s detection processes.

1. **1. Establish a Clear Delineation between Network and Security Detection, with the Networking Group and the Security Group Having Distinct and Different Responsibilities**  
   (DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.)

If your organization is large enough, split networking and security detection functions between two separate teams, with each team ideally having a different chain of command. Networking involves keeping resources up and available. Security detection is about monitoring the system for abnormalities. In many cases, network administrators rate network concerns as more important than security concerns and can override legitimate concerns about security threats.

If you work in a small operation where you can’t split the delineation of functions among multiple individuals, you should consider brainstorming methods for allocating network and security functions among a few trusted individuals.

**Relevant Technical Standards for DE.DP-1**

**Roles and responsibilities for detection are well defined to ensure accountability**

* CIS CSC 19
* COBIT 5 APO01.02**,** DSS05.01, DSS06.03
* ISA 62443-2-1:2009 4.4.3.1
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

1. **2. Create a Formal Detection Oversight and Control Management Function; Define Leadership for a Security Review, Operational Roles, and a Formal Organizational Plan; Train Reviewers to Perform Their Duties Correctly and Implement the Review Process**  
   (DE.DP-2: Detection activities comply with applicable requirements.)

To ensure that your detection activities align with your organization’s business goals, operating philosophies, legal requirements, and contractual obligations, you should establish mechanisms for oversight and control. Include this as part of your established governance and risk programs by making it a standing agenda item for discussion. Where possible, bring in other parties to this: HR, legal, procurement, IT, internal audit, and business line leadership. These groups represent those with a vested interest in addressing risks identified or discussed as part of detection activities.

For larger organizations, it is helpful to create a formal detection oversight and control management function, which entails the following:

* **Initiation**: Define the leadership for security review, operational roles, and a formal organizational plan.
* **Identify relevant review issues**: Identify and prioritize the key issues.
* **Create a generic review plan**: Define all pertinent audit and control activities.
* **Deploy the procedures to guide the review process**: Train reviewers in the necessary steps for conducting reviews.
* **Implement the review process**: Assign roles and responsibilities, develop schedules, define and perform monitoring activities, and report and resolve problems.

For smaller organizations, you should consider brainstorming ways to create formal detection oversight and control management functions for those trusted individuals who already wear multiple hats and play various roles.

These reviews should provide sufficient documentation that the detection processes are in place and comply with organizational, legal, and regulatory requirements. If you identify problems during the review, you should address them before the review can continue.

Review reports should be made available to managers by easily accessible means. Since the outcome of these review processes contains valuable information about your detection processes, it’s essential to keep a record of how you conducted the review.

**Relevant Technical Standards for DE.DP-2**

**Detection activities comply with all applicable requirements**

* COBIT 5 DSS06.01, MEA03.03, MEA03.04
* ISA 62443-2-1:2009 4.4.3.2
* ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3
* NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14

1. **3. Test Detection Processes Either Manually or in an Automated Fashion in Conformance with the Organization’s Risk Assessment**  
   (DE.DP-3: Detection processes are tested.)

Once you’ve created your detection process, test each activity for conformance to risk requirements. This testing will make sure that you’ve implemented the security control properly. One way to test each activity is to use a management tool called a “process requirements testing matrix,” which has two parts. One part manages the life cycle of the process requirement, while the other manages process activities.

You can establish tests either through manual or automated processes. In a manual process, an evaluator will manually test the process. Using the banking example, an evaluator might manually try to force a transaction that the system should reject. Automated methods perform the same functions, except using a computerized process (having a program, for example, trying to force a prohibited transaction).

Use your yearly or regularly conducted external penetration test exercises or engagements to test your detection processes. These can be very informative and are made to simulate an actual attack. To truly test your detection processes and, more importantly, your team, do not announce that the “attack” is from the authorized penetration test, which is a fruitful way to tabletop or exercise your plans and previous training.

**Relevant Technical Standards for DE.DP-3**

**Detection processes are tested**

* COBIT 5 APO13.02, DSS05.02
* ISA 62443-2-1:2009 4.4.3.2
* ISA 62443-3-3:2013 SR 3.3
* ISO/IEC 27001:2013 A.14.2.8
* NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14

1. **4. Inform Relevant Personnel Who Must Use Data or Network Security Information about What Is Happening and Otherwise Facilitate Organizational Communication**  
   (DE.DP-4: Event detection information is communicated to appropriate parties.)

Event detection reporting is the goal of these processes and is critical to uncovering malicious events. Event reports show where vulnerabilities exist so that you can remediate them. It is crucial to inform relevant personnel about event detection results so that remediation occurs in an informed and effective manner.

Event detection reporting is an effective means of ensuring that security personnel can stay informed of security issues at all organizational levels. It also facilitates improved administrative communications by distributing information about security throughout the organization. Any detection information should have a pathway toward your written incident response plan. You can use these data to mature the plan’s overall effectiveness and inform your organization of gaps in your process.

**Relevant Technical Standards for DE.DP-4**

**Event detection information is communicated**

* CIS CSC 19
* COBIT 5 APO08.04, APO12.06, DSS02.05
* ISA 62443-2-1:2009 4.3.4.5.9
* ISA 62443-3-3:2013 SR 6.1
* ISO/IEC 27001:2013 A.16.1.2, A.16.1.3
* NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4

1. **5. Document the Process for Event Detection to Improve the Organization’s Detection Systems**  
   (DE.DP-5: Detection processes are continuously improved.)

When it comes to critical events, most organizations respond reactively and focus on getting back to business as soon as possible. To prevent future occurrences and gain further insight into your organization’s security posture, you should develop records and analysis that delivers insight into why the event happened and how to prevent a similar occurrence in the future.

You should, therefore, document processes for detecting events, both during and after the events. Use that information to improve the organization’s operations and systems for detecting, investigating, and limiting future incidents’ damage. Develop metrics that feed into key performance indicators (KPIs) relevant to the business.

**Relevant Technical Standards for DE.DP-5**

**Detection processes are continuously improved**

* COBIT 5 APO11.06, APO12.06, DSS04.05
* ISA 62443-2-1:2009 4.4.3.4
* ISO/IEC 27001:2013 A.16.1.6
* NIST SP 800-53 Rev. 4 CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

**SUMMARY**

Based on the practical applications of the NIST Framework that we’ve presented in this chapter, here are the critical take-aways regarding the tools and techniques for detecting a cyberattack:

* Detecting a cyber incident among thousands or millions of routine changes across systems has become increasingly challenging.
* Adding to the challenges of detecting incidents are the techniques that malicious actors use to hide their tracks.
* The Detect function in the NIST Framework focuses on spotting when anomalies and events occur in your system.
* Before you can detect anomalies, you must establish “normal” baselines.
* You can learn about events using intrusion detection systems.
* Antivirus software is a crucial monitoring tool that can help prevent cybersecurity events.
* You will find it helpful to deploy a centralized log file that looks across multiple logs across different systems.
* It would help if you considered trying to gauge the impact of events before and after they occur based on your organization’s risk assessment.
* You will find it helpful to set thresholds on how often an event occurs before you flag it as abnormal.
* It would help if you considered continuously monitoring systems designated by your organization’s risk assessment as most critical.
* It would help if you tried, to the extent possible, to monitor appropriate access to your systems’ physical environments.
* You should consider establishing methods that monitor employees’ physical and electronic access to systems and document who gains access to facilities and digital assets.
* You should consider developing systems that check for malicious code in software through a variety of means.
* You should consider identifying and authenticating the origins and identity of mobile code.
* It would help if you considered establishing methods for evaluating an external provider’s security controls’ adequacy to ensure they adhere to your organization’s policies, procedures, and standards.
* You should *very carefully* consider using employee monitoring software for security purposes.
* It would help if you considered using vulnerability scanning tools to search for devices on the network that are open to vulnerabilities.
* Establishing your organization’s detection processes can be complicated but it is extremely helpful in understanding what’s happening in your network and effectively monitoring security.
* Large organizations should consider splitting their networking and security detection functions.
* Large organizations should consider creating a formal detection oversight and control management function.
* Make sure you test your detection systems either manually or through automated functions.
* Make sure you inform relevant personnel about detection operations.
* Make sure you document event detection to improve your detection systems in the future.

**CHAPTER QUIZ**

Take this quick quiz to learn about how to manage cyberattacks. The answers are given at the end of the book.

1. **1. What is the first step in detecting anomalies that may indicate a cyberattack? (Select one.)**
   1. **a.** Develop a process within your organization for handling attacks and incidents.
   2. **b.** Install an intrusion detection system.
   3. **c.** Establish baselines for determining what “normal” is and what is “abnormal.”
2. **2. Which of the following are some of the challenges in establishing an intrusion detection system?** **(Select all that apply.)**
   1. **a.** Staff may decide that some incidents that are alerted through the intrusion detection system aren’t problems.
   2. **b.** Networks must continue to operate while intrusion detection systems run.
   3. **c.** Intrusion detection systems often issue misleading messages.
3. **3. If your organization can’t establish network monitoring solutions for all systems and assets, which of the following should you do?** **(Select one.)**
   1. **a.** Rely on your intrusion detection systems to catch cyberattacks.
   2. **b.** Run network monitoring solutions on those assets designated in your organization’s risk assessment to be the most critical.
   3. **c.** Make sure to deploy antivirus systems that use host-based as well as network-based scanning.
4. **4. Which of the following are some of the key benefits of establishing detection processes? (Select all that apply.)**
   1. **a.** The event reports generated from these processes can yield insight into avoiding malicious attacks in the future.
   2. **b.** Event reporting that occurs under detection processes helps keep relevant personnel informed and foster better organizational communication.
   3. **c.** Detection processes help us evaluate the adequacy of providers’ security practices.

**ESSENTIAL READING FOR TOOLS AND TECHNIQUES FOR DETECTING A CYBERATTACK**

M. Hathaway, ed., *Best Practices in Computer Network Defense: Incident Detection and Response* **(**IOS Press, 2014).

Nikolaos Pitropaki, Emmanouil Panaousis, Alkiviadis Giannakoulias, George Kalpakis, Rodrigo Diaz Rodriguez, and Panayiotis Sarigiannidis, An Enhanced Cyber Attack Attribution FramChapter work, *International Conference on Trust and Privacy in Digital Business***,** 213–228**.**

R. Brewer, Cyber threats: reducing the time to detection and response, *Network Security*, May 2015 at <https://www.sciencedirect.com/science/article/abs/pii/S1353485815300374>.