Blue team's role in security

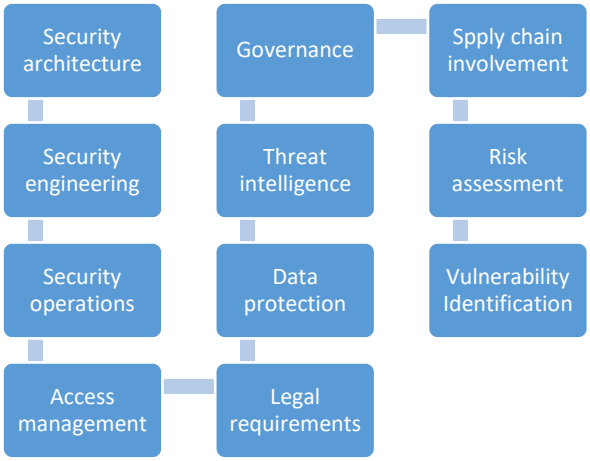
Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Even it was not named "blue team", the concept of blue team has been used in the past decade more often within organizations, generally in contrast to red team. In this article we are focusing on the concept of blue team, especially on practical methodologies and their implementation within the organisation. We also reveal the interaction with the red team. Thus, this article is aimed at outlining the main directions to be taken by small or large organisation in terms of preventing, identifying and mitigating security incidents, together with practical examples for each step of the blue team framework.

Blue team can be defined as all personnel within an organisation with responsibilities at identifying or responding to a security incident in the context of ensuring the security defence of the organisation. The activity that has to be undergone by the blue team in order to be able to identify and respond to a security incident involves also preparation and implementation of security measures.

The role of the blue team can be placed in the organisation depending on the specific steps from the sections below that are implemented and on the type of IT systems/data that needs protection.[1] The blue team should be in close contact with departments that can assist with the incident identification mechanisms (such as operations team: networking, infrastructure, software development) and with incident investigation and management (compliance, legal, data protection officer, risk management). The roles of each department should be clearly established before an incident occurs and periodically revised and adjusted to the specifics of the organisation and based on lessons learned.

To fully benefit from a red teaming exercise, the red team and the blue team should interact in certain points of the process, go through it and discuss the manner in which both teams have viewed the events with the purpose of producing a report to be used for future improvement by the blue team.



[1] Susan Lincke, "*Security Planning: An Applied Approach*", Springer, 2016.

1. Methodologies and practice for implementing blue team

There are specific steps that can be implemented in order to assist the blue team in detecting potential threats or attacks, but also on the analysis and response side. Some steps are manual and entail experienced security professionals within or outside of the organisation. In addition, certain steps can be automated either through configuration or specific automatic tools (especially ones based on machine learning).

In order for proper identification of threats/attacks to be achieved, there are three main ingredients that are needed: data (collected from the network, devices and servers), baselines (such as network baselines) and threat intelligence.

There is a series of best practice methodologies that address certain points that should be covered by the blue team,[2] including the ones mentioned below, NIST SP 800-61 - Computer Security Incident Handling Guide, NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response, NISTIR 7622 - Notional Supply Chain Risk Management Practices for Federal Information Systems and ISO/IEC 27035 information security incident management standard.

The European Central Bank published the TIBER-EU Framework, which includes guidelines for the two perspectives (red and blue teams): How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming and TIBER-EU White Team Guidance.

In this article we are outlining a framework of the main points to be covered by the blue team, with reference to the relationship between blue team and red team.

Further, the actions of the blue team have to be viewed in the wider legal context of the organisation, as there may be specific regulatory requirements in terms of identification, investigation and notification of authorities when an incident occurs, including in the banking sector, energy sector, for organisations under the NIS Directive and obligations under the data protection legislation. These legal obligations have to be integrated into the manner in which the blue team operates throughout the entire cycle of its activity.

The main steps to be taken by the blue team[3] by reference to the activity of the red team is detailed below, in the Figure 1. It is worth mentioning that, for the blue team, there are two different types of actions taken that have to be correlated and calibrated in order to ensure swift and proper response to any potential incidents.

On the one hand, the blue team has to build internally the hardening of systems, gathering of threat intelligence and implementation of proper security measures based on internal analysis. This is the passive phase of the blue team activity, which has to be properly performed before occurrence of an attack.

On the other hand, there are the actions that the blue team has to take in order to identify, investigate and respond to an attack. This is an active phase of the blue team activity that entails interaction with the threat actor.

[2] https://www.bsigroup.com/en-GB/Cyber-Security/Managing-your-IT-and-cyber-security-incidents/Standards-for-managing-IT-security-incidents/ , last accessed on 14 March 2021.
[3] Diogenes, Yuri, Ozkaya, Erdal, "Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics (English Edition)".

The important aspect is that the two types of actions both have a cyclic approach, as there are lessons learned from the active phase that have to be implemented in both the active and passive phase and there are new threat/security measures identified in the passive phase that, once implemented, also improve the active phase response of the blue team.[4]

Generally, within red teaming exercises, it is assumed that the blue team has already gone through the passive phase and is currently engaged in the active phase.

This section focuses on the passive phase, with the active phase being detailed in the next section.

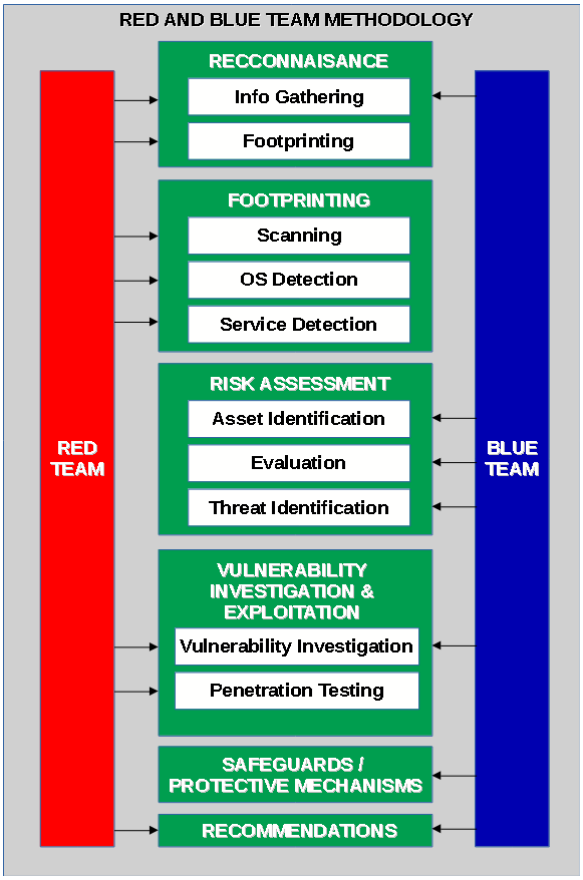


Figure 1 – Red and Blue Team Methodology

Reconnaissance: During the reconnaissance phase, the red team is trying to identify as much information as possible about the organisation and about potential vulnerabilities in a passive manner, by accessing various publicly available information and information gathered by other threat actors previously. The same type of information is targeted by the blue team in order to have an overview of the information that can be known by threat actors: from information made publicly available by its employees in social media to information sold by threat actors that targeted the organisation previously. This type of information helps the blue team to figure out the manner in which threat actors are likely to try to attack the organisation and focus on diminishing the chances of success for these vulnerabilities first.

[4] Alan J White, "Blue Team Field Manual (BTFM) (RTFM) Paperback".

Foot printing and risk assessment: For the foot printing phase, the red team is performing scanning activities in order to enhance its knowledge about the organisation and potential vulnerabilities that can be exploited.

The corresponding phase in the blue team focuses on risk assessment and threat hunting. This entails that the blue team takes into account the knowledge it gathered through threat intelligence, best practices, overview of the threat landscape and previous attacks on the organisations and identifies use cases concerning potential threats and evaluates their likelihood. This exercise is especially useful in order to identify the risks on which the organisation should first focus and attempt to mitigate them through implementation of technical or organisational controls.

Prioritisation should also take into account the data classification / CIA rating for the data stored in the IT systems in scope. If certain IT systems are maintained by third parties, an integration exercise for a coherent approach in terms of blue team tasks with these third parties has to be in place.

Thus, the two actions (of the red and blue teams) have similar objectives, even if these are from different viewpoints.

Vulnerability identification:

There are various manners in which vulnerabilities can be identified by the blue team, including vulnerability scanning[5], penetration testing, analysis of threat intelligence, for the IT environment managed by the organisation or by entities in its supply chain.

Given the changing organisation IT landscape and the changing attack types, such types of analyses should be performed periodically, with a periodicity established based on the threat landscape, risk rating, types of data in the IT systems and internal/external resources available.

The difficulty stems from identifying vulnerabilities in the supply chain. On the one hand, this can be identified through continuous monitoring of threat intelligence or monitoring/auditing of vendors used by the organisation. On the other hand, given the wide range of vendors, sub-contractors of vendors and tools/code of third parties used directly or indirectly by the organisation, it is difficult to monitor or review all aspects of the IT systems and services offered by these entities.

In case of more regulated sectors, such as banking, insurance, energy or entities falling under the NIS Directive, additional steps should be taken to ensure vendors undertake obligations about implementing security requirements. It may be argued that certain steps also stem from GDPR requirements on state-of-the art security measures being implemented, as detailed under article 32 of the GDPR.

Safeguards and protective measures:

The main point to start from in this case is the design of a security architecture and implementation of secure coding practices. In case of existing IT landscape and legacy IT systems and networks, these can be adjusted in time and prioritizing on the most vulnerable parts, as these have been identified through risks assessment or vulnerability identification.

There are several approaches that can be taken in order to achieve this objective. In this section we are outlining the zero trust architecture, the ten design principles for defensible architecture mentioned in literature and the main directions for security controls.

[5] https://github.com/rabobank-cdc/DeTTECT/wiki , last accessed on 14 March 2021.

Zero trust architecture has been gaining ground in terms of approach towards defendable systems and is based on the following main principles outlined by the NIST publication[6]:

- All data sources and computing services are considered resources: this ensures that each data location is properly hardened or has implemented adequate security measures.
- All communication is secured regardless of network location: all communication within the organisation or external communications are properly secured.
- Access to individual enterprise resources is granted on a per-session basis: this is in line with the need-to-know principle and goes further in ensuring that the authentication and authorisation takes place for each session.
- Access to resources is determined by dynamic policy: this entails that the state of client identity, client device and requested application/service are monitored in order to identify any abnormalities that can be an indication of compromise. This analysis may include other behavioural and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets: this entails that, on the one hand, there is a clear overview of existing software and hardware used within the organisation and also that the relevant CIA ratings and security controls in place are constantly monitored for adequacy and identification of needed updates/changes.

The below steps should be implemented as a repeated set of steps in order to improve the security measures and security architecture, with periodic evaluation for improvement.

Proper training of relevant staff is essential for the blue team role. This training has to be in line with recent trends in attacks, investigation techniques and blue team management framework. Thus, they should address both the technical side and the governance side.[7]

The above are in line with the **10 design principles for defensible architecture:**

1. Assign the least privilege possible – limiting user access to the data/IT systems they need for the work tasks.

2. Separate responsibilities – this ensures that each department/person concentrates on specific tasks that work well together for identification, analysis and remediation of incidents.

3. Trust cautiously – implementing zero-trust approach within the organisation and outside the organisation.

4. Simplest solution possible – given the fast pace in which new threats appear, in order to be able to act swiftly and effectively, the organisation should approach risks and vulnerabilities on a risk-based approach. Further, complex systems without a specific purpose for the complexity may be difficult to manage on the long run.

5. Audit sensitive events – a prioritization has to be established in terms of events (e.g. alerts, logs) in order to allocate appropriate resources.

[6] NIST SP 800-207, "Zero trust architecture".
[7] Luis Tello-Oquendo et al., "A Structured Approach to Guide the Development of Incident Management Capability for Security and Privacy".

6. Fail securely and use secure defaults – ensure that proper mechanisms are in place for data protection and business continuity in case an incident occurs.

7. Never rely upon obscurity – as discussed in specialty literature in cryptography, for all security aspects, the obscurity of IT systems or tools used should not a factor in the security approach (except, of course, for passwords, keys, etc.). Obscurity may bring an additional layer that the attacker has to overcome, but additional steps should be taken to ensure proper security measures are in place.

8. Implement defence in depth – in correlation with lack of obscurity, multiple layers of identification of incidents and prevention of incidents should be implemented. This ensures that it takes threat actor a longer period of time and additional skills to enter and compromise the system. In this manner, the organisation has a higher probability of identifying the incident and/or prevent/remediate it before damages to IT systems occurs.

9. Never invent security technology – organisations should review the security products/services landscape in order to choose existing tools – either open-source or not. Creation of tools from scratch may prove expensive and time-consuming. Cooperation and use of tested solutions is the best approach in terms of security.

10. Find the weakest link – this entails thinking like an attacker and red teaming exercises are useful in this respect. An IT system or an infrastructure is as safe as it weakest link.

The controls implemented for protection of data and of IT systems have as main goal the detection and prevention of incidents. Periodical assessment of the efficiency of such controls has to be conducted, either in the risk assessment and/or separately.

Controls can cover a wide range of aspects. A list of proposed controls that can be tailored on the specific infrastructure of the organisation can be found, for instance, in NIST's SP 800-53. The main points that should be covered are: checking on domain expirations, including email filters, threshold, and spam rules, implementing two-factor authentication, denying long relay request, application whitelisting, segmentation, managing keys securely, proper configuration and patch management and securing group policy settings. Further, through the architecture and implementation of IT systems, the aim of the organisation should be to diminish the attack surface.

Further, security awareness training is essential as well,[8] given that the human factor has great influence on the success of certain types of attacks, especially based on phishing.

Recommendations: Recommendations are part of the red/blue team exercise and involve the exchange of information between the teams in order to increase the security of the organisation based on the vulnerabilities identified or exploited by the red team. As a best practice, it is recommended that this occurs throughout the red/blue team exercise and not just at the end of the exercise. A step-by-step debriefing between the two teams can help the blue team with valuable information about each step of the exercise, instead of learning just a summary of the vulnerability exploited by the red team at the end of the exercise. For example, the manner in which the red team performs reconnaissance – e.g. the use of certain OSINT tools now known by the blue team – can help the blue team in real life scenarios by increasing the knowledgebase of the entire team.

[8] Joel Brynielsson, Ulrik Franke, and Stefan Varga, "Cyber Situational Awareness Testing".

2. Incident handling by the blue team

For the purpose of incident handling, the blue team has to take a cyclic approach in order to improve each stage with each iteration of this cycle, either in red teaming exercises or in real-life attacks.

As in the case of the passive phase, in this active phase, the blue team has to work with various departments within the organisation and with external entities. A non-exhaustive list is provided below. For the below steps of the blue team activity, it can interact with one or more of the below. For instance, for incident detection, blue team establishes the rules for detection based on discussions with other teams and, afterwards, receives the incident alerts from the incident response team. Further, depending on the structure of the organisations and the internal resources available, the below activities may be performed by multiple departments or by the same department. In the below, we refer to blue team as performing certain activities and this references covers also the activity of the below departments.

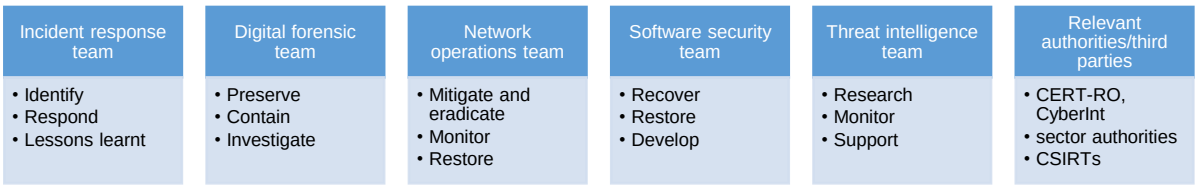


Figure 2 – Departments and entities involved in incident handling

In terms of steps to be taken by the blue team, we have outlined below the main four phases of the incident handling: scoping (gathering of relevant information to ensure proper incident identification), identification and assessment (steps to be taken to identify incidents and to analyse them), remediation (identifying and applying initial response and remediation steps, but also remediation steps to be considered for medium term) and lessons learned (identification of aspects that can be changed in the business process, IT environment or incident handling process to prevent similar incidents happening in the future or, at least, earlier detection of such incidents).

These four phases correspond to the responses of the blue team shown in Figure 4 that reflect adequate response to the cyber kill chain steps. Detection and deceive is part of the identification and assessment phase, whereas deny, disrupt, degrade and destroy are part of the remediation phase. These responses depend on the moment in the cyber kill chain that the incident is identified by the organisation.

Figure 3 – Cyber kill chain

Figure 4 – Blue team cyber kill chain response

a. Scoping

The first step in incident handling entails determining main areas and mechanisms for identification of incidents.[9] Of course, in order to cover all aspects of security, physical, infrastructure, networking and IT system security angles should be covered. This means that the organisation has to ensure it has an updated list of IT systems and infrastructure, which can be obtained through an internal framework outlining roles and responsibilities of departments in the organisation to keep the list updated. Shadow IT generally exists within the organisations, but the aim is to minimise or eliminate this through awareness and proper data collection and aggregation. This ties in with the passive phase actions taken, especially in terms of risk analysis, but also with further threat intelligence gathered constantly on the potential threat specific to the architecture and sector of the organisation.[10] Nevertheless, for any detection solution chosen, after a proof of concept is made, analysis on the scaling up of the solution has to be analysed, based on the existing infrastructure (and the types of IT systems and layout of networks) of the organisation and any extension plans.

In addition to the data from the IT systems stored/managed by the organisation, the IT systems stored/managed by third parties should also be analysed. The analysis of data can entail sending raw data from the IT systems maintained by third parties to the incident handling team in the organisation or sending just the incident data. There are pros and cons for each situation. On the one hand, if only incident data is sent, this means that the organisation relies on the third party for incident identification. Further, analysis of only a limited amount of data about the organisation's IT systems may lead to not detecting all incidents. On the other hand, if the third party if managing IT systems for multiple organisations, it can gather sufficient data to identify more accurately incidents. In case incident handling is left to the third party (or its sub-contractors, as part of the supply chain), best practice entails that the organisation establishes with the third party the standards the latter follows to ensure proper incident handling framework. In certain instances, periodical monitoring or auditing may be useful to review that this framework is properly implemented.

With the extensive use of cloud systems, cloud providers, as provider, have to be involved in a constant cooperation with the organisation in terms of threat identification. In this case, generally, cloud providers allow penetration tests to be performed on their systems, provided prior approval is obtained from the cloud provider. Further, in case vulnerabilities are identified in their systems or in the supply chain used by their system, cloud providers have taken an active approach and, aside from notifying their clients about the incidents/vulnerabilities, have also issued appropriate mitigation plans and tools in a timely manner.

The lessons learned from previous incidents, aside from integration into the risk assessment, should also be included in the incident identification framework. The creation of this identification framework is also closely tied with threat hunting. Threat hunting exercises can be useful in identifying potential incidents or future incidents and should take into account the outcome of the risk assessment and a prioritisation of threat intelligence gathered.

---

[9] https://blog.cyberint.com/threat-hunting-with-the-mitre-attck-framework , https://www.siriussecurity.nl/blog/2019/5/8/mapping-your-blue-team-to-mitre-attack , last accessed on 14 March 2021.

[10] https://digitalguardian.com/blog/threat-hunting-mitres-attck-framework-part-1 , last accessed on 14 March 2021.

Moreover, analysing of historical data may prove useful, as new threat models have been developed since the first time that data was analysed. This entails that intrusions not detected during the first analysis may be detected during a subsequent analysis. This is especially useful when the intrusions are still active in the organisation environment and steps can be taken to address them.

The aim of such extensive analysis is to identify and document relations between events that have occurred in relation to the organisation or to other organisations in order to understand better the threat landscape. Generally, more data can lead to useful information, if properly analysed. Determining relevant rules or pattern identification can prove sometimes difficult in practice. Approaches that can be taken by companies include using third parties for the analysis, establishing rules by experience or using machine learning approaches.

In this case, legal requirements for log retention and sharing should be observed. A balance has to be made between the legal requirements to delete data and the practical need for data for analysis. Further, both internally and externally, the organisation has to implement the need to know principle, allowing access to data only for individuals that need to access such data to fulfil their job tasks and balancing need for data with legal requirements to delete data. Access to data – need to know basis. When sending response process instructions to operations team, disclose only needed information.

Further, the organisation can explore the use of honeypots for both defence (to deflect threat actors from the actual IT systems/infrastructure used by the organisation) and for threat information gathering (obtaining information about existing threat that are targeting the organisation). The honeypots are generally placed within the organisation perimeters (behind the firewalls), but, for specific reasons, they can be placed before the firewalls. Honeypots can be implemented and analysed third parties or by the internal team of the organisation.

In case of a red teaming exercise, during the various stages of the exercise and especially after the reconnaissance and recommendations phases, the red team can provide useful information in this respect.[11] If scoping suggestions are made during the scoping phase of the blue team, the red teaming exercise can prove useful for the blue team by experiencing in practice new types of detection.

The data quality is essential for accurate incident detection. The data quality should be monitored and periodically adjusted to reflect the relevant data for detection. The main characteristics of data include:

- Accuracy – integrity of data and lack of errors in data collection and transmission.
- Completeness – the analysed data should be complete in terms of timing and data sources.
- Consistency – the data received from various entry points should not be contradictory.
- Timeliness – data should be up-to-date and proper historical data should be available.

The goal for maintaining data quality in incident analysis is to reduce the time it takes to fixing, validating and correlating data, but it is also useful in order to be able to rely on data from multiple sources during the analysis and enhance use of automation in the incident identification process.

Aside from the practical commercial aspects, use of an external SOC/CSIRT, there are certain legal points to consider[12] (such as, commercial secret sharing with third parties, ensuring timing

[11] David Mugisha, "Cyber Security: Improving Cyber Defense Through Coherent Joint Red Team and Blue Team", Journal of Defense Modeling & Simulation, 2019.
[12] The Forrester Wave™: Enterprise Detection And Response, Q1 2020, https://reprints.forrester.com/#/assets/2/482/RES146957/reports, last accessed on 14 March 2021.

responses and notifications from the third parties, ensuring third parties comply with legal requirements applicable to the organisation in terms of incident handling).

Generally, the data anonymisation cannot be achieved in such situations, as the SOC and CSIRT teams need to have access to the entire infrastructure relevant for the role they are playing in the blue team. Nevertheless, data minimisation and need to know principles should be implemented in this type of exercise. In addition, the retention period and deletion should be implemented.

The scoping phase is closely tied with business continuity and disaster recovery, as it represents the trigger for setting in motion the steps necessary to keep the activity of the organisation going until the incident is properly investigated, contained and remediation are in frameworks, including ones from NIST and ISO (ISO 22301 Business continuity management systems requirements, ISO 22313 Business continuity management systems guidance).

b. Discovery and assessment

For the discovery step, the organisation has to ensure that proper data is collected from within the organisation IT systems (network, hosts, servers) in order for the identification methodologies to be applied to this set of collected data.[13] The assessment of the data collected is essential in determining the main direction for further investigation, data collection and assessment.[14] This step generally is implemented as a cyclical step, as it may take several iterations until the relevant data is obtained and the relevant types of threat / attacks are searched for.

- **Hypothesis driven investigations** – when the blue team has indications that threat actors may target specific organisations or specific vulnerabilities. This can be achieved through threat intelligence gathering or through sharing of existing attacks within the sector/national/international community.
- **Known indicators of compromise (IOC) or indicators of attack (IOA)** – given the current types of attacks, the blue team identifies within the organisation's infrastructure the preliminary steps in the cyber kill chain that were used in previous attacks. Depending on the step in the cyber kill chain, this may give the blue team a heads-up that can help in reducing the footprint of the attack or its consequences. Without knowing IOCs or IOAs from other previous attacks and scanning the infrastructure for these, attacks can go undetected for large periods of time.
- **Advanced analytics and machine learning** – these can be used to identify potential anomalies in the fingerprinting of a system, device or in the traffic of a network or towards/from a server/database. This step entails choosing the appropriate algorithm for each situations. In certain cases clustering may help identify the areas of concern and in orders fuzzy logic may prove more useful. This can be decided and implemented on a case by case basis, as the blue team considers most fit for delivery of swift and useful information in order to allow time for the blue team to react to the potential threat/incident.

According to Bianco's Pyramid of Pain[15], in order to slow down or stop a threat actors, relevant information should be obtained about the attack approach and mechanisms, preferably early on the cyber kill chain. Thus, with a low value in terms of detection, the organisation may consider binary

[13] Don Murdoch, "Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder. 2nd Edition".
[14] https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System , last accessed on 14 March 2021.
[15] http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html , last accessed on 14 March 2021.

hash values, IP addresses and domain names. These are easy to change by the threat actor once they are compromised and are also generally shared within the security community and are embedded in certain security solutions. The more valuable information that can be gathered is network/host artefacts, tools and TTPs (Tactics, Techniques and Procedures). These are very particular for the attack and/or for the threat actor and represent valuable information that allows organisations to stop the attack at its early stages. General tools that can be used for the blue team responses to the cyber kill chain include the following, mapped to the response steps.

For detection, there are various methods that can be used, as detailed above and may include: web analytics, NIDS, HIDS, audit logs, SIEM, vigilant users.

In order to deny an attack throughout the cyber kill chain, various tools can be used, including NIPS, proxy filter, firewall ACL, patches, outbound ACL.

Similarly, for disrupting the cyber kill chain may be performed by various tools, including NIPS, DLP, DEP, Inline AV.

Deceiving is usually achieved through DNS redirection or honeypots. Degrading the attack is usually performed through queuing, tarpit, limitation quality of service.

Containment may be achieved through various methods: trust zones, app-aware firewall, EPP, inter-zone NIPS, firewall ACL. This generally relates to the implementation of zero trust architecture.

In both red teaming exercises and real life scenarios,[16] once information about the environment being breached has been detected, there are a series of steps to be taken in a specific order:

- Alert the appropriate persons within the organisation, as per internal procedures. This may include the blue team, incident response, legal and risk departments, board of directors. Generally, a roles and responsibilities matrix with thresholds sets-out the specific situations in which each department is notified and the input needed from each department. In addition, role play exercises should be performed prior to incidents in order for all individuals from each department to be aware of their role and for all department to work swiftly together.
- From an organisation perspective, it is essential to implement at this stage the internal procedures in place for notification of relevant authorities in case of incidents. This type of roles have to already be included in internal procedures or instructions and rehearsed by the team members prior to an incident occurring. Generally, there are multiple authorities (and, in certain cases, affected individuals/client) that have to be notified in a particular case, but viewed from different angles.
- The relevant persons within the blue team decide the containment and context analysis to be performed. At this stage, external parties may be called-in to assist on specific investigation points.
- Throughout the process, the identification of relevant evidence concerning the incident and proper preservation thereof is necessary.
- After analysis is completed or, even, in some cases, after partial analysis is completed, a remediation plan is discussed. Further on the remediation steps in the next phase of the incident handling.

During this phase, the role of third parties (such as vendors) involved in the IT systems affected by the incident is essential. This entails that prior contractual provisions are in place to outline the

[16] Don Murdoch, "Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback".

involvement of third parties: allocation of third party team members, access to third party logs or documentation, response times for questions and root cause reports, mitigation steps to be taken by third parties. This type of additional services may have an impact on the workload of the third party and on the cost of the contract.

The communication of threat information to other entities within the same sector of activity or other communities should be performed in an anonymous manner, without giving valuable commercial/architecture/personal data information. One common information model used widely is the STIX model.

The secondary aim of the discovery phase is to limit the false positives, while analysing the events in a more complex context in order to be able to identify patterns for threat/attacks.

For this phase, specific metrics can be created in order to improve the process, such as estimated time to detection or estimated time to recovery. This correlates to metrics of the red team, such as mean time to compromise, mean time to escalation, mean time to detection.

c. Response process development

The response development should identify the steps to be taken to repair the affected systems, to eradicate the part of the intrusion that is still in the network/IT system (e.g. reinstalling applications/OS, using back-up version of application before indications of compromise existed in it, eradicating viruses).

Building on the defence in depth principle, additional security measures identified during the incident assessment can help in case of future incidents in ensuring that the parts of the defence in depth structure that had been damaged are identified and repaired swiftly and, further, that the actual data/IT systems are not compromised.

The remediation has to be performed based on the CIA rating of the application/IT system/network involved in the incident and based on the level at which the incident occurred (e.g. at the level of the firewall, within the email server, within the application server through privilege escalation from an employee laptop).

In certain cases, correlation with other affected entities or instructions from authorities or from vendors may also be needed.

In terms of implementation of remedial steps, the relevant IT/business owners of the process/IT system should be involved in the process and should agree on the budget and timeline. In certain cases, the buy-in of the board of directors may be needed.

The remediation steps may change before they are implemented or afterwards. Thus, as in the case of controls, they should be periodically reviewed to ensure that they represent the most efficient and effective manner to prevent the occurrence of future similar incident.

Follow-ups should be performed in order to ensure that remediation steps have been implemented properly both internally and, if needed, by third parties.

d. Reporting and lessons learned

The reporting of incident analysis results should be made internally, within the security team, before the relevant internal stakeholders (including the board of directors, risk management), but also before authorities, if this is required under the law. Further, from a public relations perspective, constant reporting to the public may also be useful.

The lessons learned step after an incident occurrence is useful in order to identify internal processes within the organisation that should be improved either for identifying incidents, increasing security prevention measures, improving employee awareness, updating incident handling procedures or updating agreements with third parties providing IT services to the organisation.

In the case of a red teaming exercise, this is the phase of recommendations that entails discussions about the steps taken by the red team.

The knowledge base for incident response can also be improved by the lessons learned in the incident handling exercise.