



# New Zealand Diploma in Cybersecurity

**HTCS6707 CYBERSECURITY PROJECT**

**INDUSTRY REPORT TEMPLATE**

**STUDENT NAME: MA'ALONA MAFAUFAU**

**STUDENT ID: 1284380**

**INTERNSHIP PROVIDER: DATACOM**

**INDUSTRY SUPERVISOR: TIM CHU**

**INTERNSHIP PERIOD- START: 06/04/2021**

**END: 20/07/2021**

**DATE OF SUBMISSION**

**25/10/2021**



## TABLE OF CONTENTS

---

<b>1.1. EXECUTIVE SUMMARY</b>	<b>3</b>
<b>1.2. INTRODUCTION</b>	<b>4</b>
<b>1.3. COMPANY BACKGROUND</b>	<b>5</b>
<b>1.4. GOALS AND OBJECTIVES</b>	<b>6</b>
<b>1.5 LITERATURE REVIEW</b>	<b>8</b>
<b>1.6. PROJECT TASKS</b>	<b>22</b>
<b>1.7. CONCLUSION AND LESSONS LEARNED</b>	<b>23</b>
<b>REFERENCES</b>	<b>24</b>
<b>APPENDICES</b>	<b>31</b>
<b>ACKNOWLEDGEMENT and APPROVAL</b>	
Students Acknowledgment	40
Industry Supervisor Approval	40



## 1.1. EXECUTIVE SUMMARY

---

This report provides documentation following an internship with the Cyber Defence and Operations Centre (CDOC) of Datacom in Auckland, New Zealand. Designed to supplement and reinforce learnings from the Unitec New Zealand Diploma in Cybersecurity courses taken concurrently, the internship provided details and context regarding tools and processes which are difficult to obtain outside of a security operations centre (SOC) environment.

We begin with a brief introduction of the threat landscape of the cyber world, where I outline some of the more common attack types, the various costs to businesses and society as a result, and the role of cybersecurity in providing solutions to detect, mitigate, and protect against the multitude of cyber threats that exist on the Internet. A short description of Datacom's background and discussions around some of its core services follows, and in particular, information around the Datacom SOC. I then provide my two goals for the internship with a further breakdown of the goals into milestone objectives. A literature review section follows which provides more details around some of the tools and techniques that are elaborated upon further in the Project Tasks section. Finally, a summary of the major outcomes of the internship are discussed.



## 1.2. INTRODUCTION

---

Computer hackers have used the Internet to take advantage of weak computer systems and processes for many years (Power, 2016). The range of methods used by attackers is vast, and include attacks on network infrastructure (Rishi Iyengar and Clare Duffy, CNN Business, 2021), web applications (Armerding, 2019), IoT devices (Kass, 2021), and mobile phones (T-Mobile, 2021).

The ramifications of these attacks are large financial losses, as well as reputational damage. A 2020 report by Netscout (2021, pp. 6–7) found that the average monthly Distributed Denial-of-Service (DDoS) attack rate was 839,083 — an increase of nearly 130,000 per month from the previous year. Considering the average attack was approximately 40 minutes and the average hourly downtime cost of one critical application in an enterprise is \$300,000, when coupled with the attack frequency, the problem of DDoS is a costly one. Not only are these attacks becoming more complex in nature, their implementation has also evolved such that they are easier and cheaper for adversaries to carry out (Mirkovic & Reiher, 2004, para. 1; Palmer, 2020, para. 1). As it stands today, the use case of DDoS attacks has progressed to where cybercriminals can now sell attacks packaged as Software-as-a-Service with a starting point of \$20 USD (Cloudflare, n.d., para. 5).

Data breaches have also been on the rise, with companies suffering the blow of both the breach itself, as well as the likely loss of customers once customers find out (PwC, 2017, p. 2). As outlined in Recital 85 of the GDPR, victims of a personal data breach can suffer anything from identity theft and fraud to substantial social disadvantage (Intersoft Consulting, 2019). Take the case of Claude Beland, former president of Desjardins Group. Scammers were able to use personal breached data to steal money from three separate companies using his social insurance number (Harris, 2019). Identity theft events happened to 5.66% of data breach victims in 2017 (Hays, 2020, "What is identity theft?" section). Oftentimes, the leading cause of data breaches involves attacks such as phishing (Schwartz, 2021) - a popular social engineering tactic - and coverage by Hubbard (2015) details how Omaha-based commodities trader Scoular Co. lost \$17.2 million after falling victim to an elaborate spear-phishing campaign. Morgan (2020) believes approximately \$10.5 trillion will be lost to cybercrime by 2025.

The case for cybersecurity and its adoption across businesses has never been stronger considering the potential financial, reputational, and personal losses outlined above. As such, my internship with Datcom allowed me first-hand experience into today's cutting-edge cybersecurity tools as well as an understanding of other key concepts that help keep organisations safe. The biggest revelation to come from my internship was learning that processes and people are just as paramount as technological considerations when implementing protections against cyber-attacks.



### 1.3. COMPANY BACKGROUND

---

The company I conducted my internship with was Datacom and I carried out it's term at Datacom's Auckland office based in the CBD.

As one of Australasia's largest privately owned information technology companies, Datacom has offices across New Zealand, Australia, and Asia. As today's world relies more and more on a wide range of technologies, Datacom offers many services which meet the growing needs of companies looking to be competitive in new business landscapes.

These include services such as cloud infrastructure, data centres, software engineering, and digital process automation. The industries that Datacom's customers are from range from the public sector, to agriculture, to media and entertainment.

Datacom also offers cyber security services, with dedicated operation centres in both New Zealand and Australia. This department of Datacom is where my internship experience was centred as I was given access to the Auckland SOC to learn more about their security management, vulnerability assessment, and end-point detection and remediation services (Datacom, n.d.; Datacom Group Limited, n.d.).



## 1.4. GOALS AND OBJECTIVES


---

On entering the Unitec internship with Datacom, my expectations of the outcomes of the experience were centred around gaining a high-level understanding of the roles, the processes, and the technology used in a CDOC. To put into more concrete milestones, my main two goals for this internship were:

1. To gain the skills needed to be confident enough to apply for entry-level cybersecurity analyst roles.
2. To understand some of the technology used in a SOC well enough to be able to build out security solutions myself in my home cyber security laboratory.

In setting out to achieve my goals for the internship, the following objectives were set out to help provide some structure and metrics in their pursuit, and the steps undertaken to achieve each of the objectives:

1. *High-level understanding of a SOC:* As someone who has previously never had any professional experience with the cyber security field, my first objective was to learn the structure of a SOC in terms of the roles present in Datacom, the responsibilities of each role, and the types of services typically offered by a SOC. As much of this information could only be gained by interacting with Datacom staff, to achieve this objective, I had to make notes of the answers to my questions regarding the SOC structure as well as reading internal documentation which outlined the overall structure of the team. Notes were also taken during a presentation by the SOC manager and a SOC analyst providing an overview of the history of the organisation, their clients and services, the types of threats they faced, frameworks used in their processes, and the technology employed to achieve their goals. Being able to summarise the previously stated information in my own words into a formal document was the metric used to signify accomplishing this objective, and these words are presented in the Literature Review section of this report.
2. *Entry-level Analyst Tasks:* In order to be confident enough to apply for entry-level employment in a SOC, I had to understand what the expectations and main tasks of such a role would be. To accomplish this objective, I had frequent interaction and dialog with a graduate analyst from the SOC who provided insight into their progression over the first few months of their role. They also provided information regarding the most common tasks performed during that time, and I was able to shadow the analyst which provided even more context around the expectations of their role. I now have a clear understanding of what an entry-level SOC role entails.
3. *Create an EDR Demo in a Homelab:* I learn best when I can build something from scratch. Thus, I decided early on during my internship that my main goal was to create an EDR setup on a personal computer as EDR technology intrigued me the most. I managed to discover an EDR provider that had thorough documentation for me to be able to implement it myself. This EDR vendor is called LimaCharlie and they offer to host two EDR monitored devices for free. I outline in the Appendix section how I went about creating a virtual windows machine which I installed a sensor on (a data logger), which then monitored the windows environment for any rules that I had enabled.

- 
4. *Set Up Alerting to Mimic Ticketing Functionality:* My final objective in building out personal homelab experiments was to set up a way to send alerts if the EDR rule was triggered. After reading documentation from both LimaCharlie and Slack, I managed to set up a system where details of specific alerts I am interested in monitoring are sent to a Slack channel dedicated to EDR alerts. I outline my methodology in the Appendix of this report demonstrating the successful deployment of EDR-to-Slack real-time alerting.



## 1.5 LITERATURE REVIEW

### Security Operations Center

A SOC describes a collective body of cyber security professionals who work towards protecting an organisation, or multiple organisations, from the ever-increasing cyber threats posed by having an online presence in the modern world (Danquah, 2020; Mareels, 2021). Ganesh (2021) outlines how a SOC seeks to achieve such protections by continually refining not only their technological tools, but also their processes and staff expertise.

Figure 1



Note. A graphical representation of the basic building blocks of a SOC. From *SIEM Better Visibility for SOC Analyst to Handle an Incident with Event ID* by B. Ganesh, 2021 (<https://gbhackers.com/siem-for-better-visibility-for-an-analyst-to-handle-an-incident/>).

Figure 1 presents a model of a SOC which consists of three key areas, as previously mentioned. A brief discussion of each component of Figure 1 is presented below.





## People

Microsoft argues the most important leg of the security operations triad is people (Allen et al., 2021). The tools used by a SOC are only as effective as the team's ability to wield them. Similarly, the effectiveness of processes developed in a SOC are determined by the team's ability to innovate and adhere to them. Zhang (2020) interviewed a number of security professionals regarding the undertaking of building out a SOC, where a common theme emerged from her interviewees around the high technical aptitude and learning ability needed by SOC professionals to be able to respond to adversaries who also learn and modify their attacks, as well as analysts being able to quickly familiarize themselves with the multitude of software vendor solutions. SOC members must also be effective communicators as they are constantly working with various internal and external stakeholders, customers and vendors.

## Common SOC Roles

Each SOC consists of various roles, and while some are a staple across SOC teams (e.g. analysts and SOC managers), others are not as common (e.g. Director of Threat Intelligence) (Stern, 2021, "Additional Roles" section). Exabeam (n.d.-a, "Who Works in a SOC" section) provides a breakdown of some of the more common SOC roles previously mentioned and is presented in Table 1.

## Process

Zhang's interview with engineer Sam Bocetta highlighted the central role well-reviewed processes play in what he termed "quality SOC centers" (Zhang, 2020, "Sam Bocetta" section). In Sam's thirty years of experience working for US defense companies, he attributes repeatable methodologies for security functions such as incident management as critical when resolving alerts.

An example of a framework that provides guidance on security incident handling processes is the National Institute of Standards and Technology (NIST) 800-61 (Cichonski et al., 2012).

**Table 1**

	Role	Qualifications	Duties
	<b>Tier 1 Analyst</b> Alert Investigator	System administration skills, web programming languages such as Python, Ruby, PHP, scripting languages, security certifications such as CISSP or SANS SEC401	Monitors SIEM alerts, manages and configures security monitoring tools. Prioritizes alerts or issues and performs triage to confirm a real security incident is taking place.
	<b>Tier 2 Analyst</b> Incident Responder	Similar to Tier 1 analyst but with more experience including incident response. Advanced forensics, malware assessment, threat intelligence. White-hat hacker certification or training is a major advantage.	Receives incidents and performs deep analysis, correlates with threat intelligence to identify the threat actor, nature of the attack and systems or data affected. Decides on strategy for containment, remediation and recovery and acts on it.
	<b>Tier 3 Analyst</b> Subject Matter Expert / Threat Hunter	Similar to Tier 2 analyst but with even more experience including high-level incidents. Experience with penetration testing tools and cross-organization data visualization. Malware reverse engineering, experience identifying and developing responses to new threats and attack patterns.	Day-to-day, conducts vulnerability assessments and penetration tests, and reviews alerts, industry news, threat intelligence and security data. Actively hunts for threats that have found their way into the network, as well as unknown vulnerabilities and security gaps. When a major incident occurs, joins the Tier 2 Analyst in responding and containing it.
	<b>Tier 4 SOC Manager</b> Commander	Similar to Tier 3 analyst, including project management skills, incident response management training, strong communication skills.	Like the commander of a military unit, responsible for hiring and training SOC staff, in charge of defensive and offensive strategy, manages resources, priorities and projects, and manages the team directly when responding to business critical security incidents. Acts as point of contact for the business for security incidents, compliance and other security
	<b>Security Engineer</b> Support and Infrastructure	Degree in computer science, computer engineering or information assurance, typically combined with certifications like CISSP.	A software or hardware specialist who focuses on security aspects in the design of information systems. Creates solutions and tools that help organizations deal robustly with disruption of operations or malicious attack. Sometimes employed within the SOC and sometimes supporting the SOC as part of development or operations teams.



## Metrics to Optimize Through Process

Establishing an effective security process does not necessarily ensure it is an efficient one. Thus, certain metrics can be used to assess the efficiency of some SOC processes (Cooper, 2020, "MTTD and MTTR Explained" section), with two notable metrics being:

- Mean Time to Detect (MTTD)
  - This is the mean time taken to detect potential security incidents.
- Mean Time to Respond (MTTR)
  - The mean time to isolate and mitigate any found threats.

## Ticketing

A ticketing system has an important role to play in a SOC's processes. As noted by Cherwell (n.d.), ticketing systems allow for centralized security alert and incident management, which in turn helps analysts and engineers monitor investigative progress on all events logged through the system. Ticketing also keeps track of the severity of alerts and any amendments to their severity levels as well as some documentation for post-incident reviews.

Another critical role played by ticketing systems is a mechanism by which service-level agreements (SLAs) are tracked (Cherwell, n.d., "Why Is a Ticketing System Needed?" section). An SLA is a formal document between a vendor and a customer which makes explicit the level of service promised, with a satisfactory service level measured by some agreed-upon metric. Any penalties for not meeting a service level are also outlined in this document (Overby et al., 2017, "What is an SLA?" section).

Therefore, SLAs could be measured by a certain MTTD or MTTR, or could include both. For example, the UK based managed security service provider (MSSP), Wizard Cyber (Wizard Cyber, 2021) outlines on their website their SLA measures, as outlined in Figure 2 below (Wizard Cyber, 2020).

Figure 2

## SLA SOC

### Service Deliverables

This is the Service Level Agreement ("SLA") which applies to our Service as set out in our Contract with you.

#### SLA Measurement

The Service Level Agreements for the Security Operations Centre:

The Service is running and available to collect data from in scope sources. Availability will be measured by monitoring the critical application services running in the hosting platform from an alternative location.

The MSP must notify the customer via email of all cyber security incidents and detail the actions that will be taken. To meet the SLA, all security incidents must be actioned within the allotted response time according to the priority.

#### SLA Period

An SLA period, for the purpose of measuring the performance of the Service against the SLA, is 1 calendar month, commencing on the first day of each month.

#### Service Level Agreement

A list of use cases and the standard assigned priority levels will be agreed and issued to the Customer once on-boarding of Customer to the solution is completed and may be reviewed and amended during service review. In the event of an SLA breach customers will receive a Service Credit that can be used against future purchases, which will be applied to the account. The Customer is responsible for ensuring that they are applied when the SLA has been breached.

In the event that more than one service level within each specific SLA is breached during an SLA period then we will only be liable to payout against the highest value Service Credit. Multiple breaches within each will not be treated as cumulative.

Name	Description	SLA
<b>Individual Security Event Investigation SLA (TTD)</b>	Upon generation of an alert that creates an incident, the Wizard Cyber SOC will begin the investigation. The SLA timeframe in minutes is automatically calculated by the system and annotated in the audit log. This is measured by taking the difference between the creation of the incident as shown in the audit log and when the incident is either assigned to a SOC analyst or manually escalated.	60 minutes
<b>Weekly Average Time to Assign SLA</b>	ATTA measures the total amount of time to assign after an incident is created. This includes the delay to assign the Alert to a SOC analyst to begin an investigation.	60 minutes
<b>Weekly Average Time to Close SLA</b>	ATTC measure the total time from the alert being generated to the alert and ticket being closed. ATTC includes the delay between the alert creation time and the alert being assigned to a SOC analyst. Investigations vary greatly but all alerts should be closed on average within the specified SLA.	120 minutes
<b>Executive Summary Reports</b>	A monthly executive report will be delivered via email in PDF document format. This report will include all high-level summary information for the corresponding period.	Monthly

#### Service Hours

The Service Hours of the Service are 24 hours per day, 365 days per year. Maintenance shall be carried out outside of core business hours (GMT) and should not affect the availability of the Service.

Where we intend to cause scheduled downtime, Outages, or Service Interruptions we will use reasonable endeavours to schedule them so as to minimise the impact on the Services and will notify the Customer of the anticipated commencement time and the estimated duration.

Wizard Cyber makes no representation and gives no warranty that any scheduled downtime, Outages, or Service Interruptions will be resolved in accordance with this SLA.

FOLLOW US

Address:  
10 Buckingham

Telephone:  
UK:

WIZARDcyber





## Technology

Just as the finance industry witnessed an adoption of various technologies over the last two decades, with Artificial Intelligence (AI) systems guiding buy and sell transactions in many high-frequency trading firms (Salvage, 2019), so too have SOC's seen an adoption of AI powered next-gen tools with one survey reporting "93% of respondents saying that they employ AI and ML technologies" (Lewkowicz, 2020). Two of the most embedded technological tools in the modern-day SOC are Next-generation Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) systems, both of which are today commonly augmented with some degree of machine learning (ML) capability (Exabeam, n.d., "SOC Tools" section).

### SIEM

SIEMs are integral tools in the modern-day SOC as they are the location where a vast multitude of data sources send events to be correlated, providing greater context around alerts of possible threats (González-Granadillo et al., 2021). The term SIEM was created by Mark Nicolett and Amrit Williams in 2005 in a Gartner SIEM report, combining Security Information Management (SIM) and Security Event Management (SEM) (Exabeam, n.d.-b). A SIEM can have a wide range of capabilities, ranging from complex correlation rules and search processing languages, to real-time machine learning-powered data analytics, to advanced dashboards (González-Granadillo et al., 2021, p. SIEM Features and Capabilities). Reviews on TrustRadius (n.d.) reveal some of the top SIEM solutions on the market are AlienVault USM, Splunk Enterprise, and IBM QRadar. González-Granadillo et al. mention that the "... success of detecting an event by a SIEM relies on the power of the correlation rules." (2021, p. 6), and therefore warrants further discussion of the details of such rules.

#### *Correlation Rules*

##### *Correlations*


Correlations in the context of a SIEM refer to the associations between various data source streams where the associations identify a possible security incident that needs to be further investigated (AT&T Cybersecurity, n.d.). Therefore, a correlation rule is the linking together of specific sequences of events which trigger alerts for a potential security threat (Crawley, 2018).

##### *Indicators of Compromise*

The events that make up correlation rules are commonly referred to as indicators of compromise (IOCs). IOCs range from IP addresses, to a file hash, to domain names and email addresses. The advantage of defining IOCs for known malware or adversarial actions becomes clear when automated systems such as SIEMs are able to use them to find and link each IOC quickly in large datasets (Rowell, 2017, "SECURITY INFORMATION AND EVENT MANAGEMENT" section).

### EDR

The EDR solution has been a relatively newer development in a SOC's arsenal, with Gartner's Anton Chuvakin originally coining the term Endpoint Threat Detection and Response (ETDR)



in 2013 (Chuvakin, 2013), to refer to what is today known as EDR. At a high level, an EDR solution is installed on, and monitors endpoints, with some solutions having the capability of responding to detected threats (Kienzle, 2020, "EDR Solutions" section). A SIEM with an integrated EDR tool offers higher levels of visibility as they provide data streams at the user level, as well as providing additional security measures and monitoring such as user and entity behavioural analysis (UEBA) for detecting hard-to-uncover insider threats (Kienzle, 2020, "Summary" section; Correa, 2020). Currently, some of the top-of-the-line EDR solutions are CrowdStrike Falcon, SentinelOne and Check Point Sandblast (Shread, 2021).

## Measuring Priorities and Alerts

Alerts generated by SIEMs, EDRs, or customers are assigned a priority level so that analysts and engineers can quickly gauge the severity of the alert before understanding all the details (Trustwave, 2019, "Security Threat Investigation and Incident Identification" section). When investigating an alert, it may be discovered that the alert notified the SOC of an event that was in fact not malicious. There are various reasons for such instances to occur, and when they trigger, are called false positives. In this section, we go into detail about what constitutes the varying priority levels, the accuracy of alerts, and what methods are available to decrease false positives.

### *Priority Ratings*

In general, organisations assign a priority with a number between one and four, often denoted P1 - P4 respectively. P1s are the most critical alerts while P4s are the least urgent. Each organisation has a different set of assets, objectives and services to protect and monitor. Therefore, priority classifications will differ accordingly. To illustrate, we refer to two company SLAs and their definitions of P1 - P4 events. Table 2 is the breakdown of priorities for Vocus (Vocus, n.d.), a New Zealand technology company, while Table 3 presents priority level descriptions for Trustwave (Trustwave, n.d.), an international cybersecurity and MSSP.

**Table 2. Vocus**

Severity Level	Description
Priority 1	Severe business impact. Critical business services down.
Priority 2	High business impact. Non-critical services down. Service degradation
Priority 3	Minor service degradation, specific service functionality unavailable
Priority 4	A minor service issue

As can be seen in both SLAs, P1s relate to any incident which has substantial detrimental impacts to the business, and subsequent priority levels classify decreasing negative effects.

**Table 3. Trustwave**

Priority	Analyst Response	Priority Description
<b>Critical (P1)</b>	Phone call & Email	Incidents at this level are actionable, pose high risk, and signal active compromise, damage, or disruption of operations to high value assets in the Client environment. Investigations that result in this priority require immediate action to contain the threat or response and recovery actions to mitigate the bypass of multiple security controls.
<b>High (P2)</b>	Phone call & Email	Incidents at this level are actionable, pose high risk, and signal the potential compromise, severe damage, or disruption of operations to high value assets in the Client environment. Investigations that result in this priority require clients to take nearly immediate defensive actions to contain the threat.
<b>Medium (P3)</b>	Email	Incidents at this level are actionable, pose medium-risk, and signal the potential of limited damage or disruption to standard assets in the Client environment. Investigations that result in this priority require clients to take timely, yet not necessarily immediate action to contain a threat.
<b>Low (P4)</b>	Email	Incidents at this level are not immediately actionable and may require further investigation by the client to determine possible actions. Investigations that result in this priority require additional context or may signal known risks and deviations from security best practice

As was mentioned earlier, the responsiveness of a SOC to alerts are usually outlined in an SLA, and metrics like MTTD and MTTR are defined such that this responsiveness is measurable. The aforementioned priority levels provide a SOC and it's customers a natural framework to help outline in an SLA the promptness required for the investigation and remediation of alerts. Vocus provides a further breakdown of their priority levels in Table 4 with the corresponding time frames for various categories.



Table 4

Category	Priority	Period	Target
Rebate			
99.95%		24x7x365	≥ -
Service Availability		< 99.9% - ≥99.7%	5%
		< 99.7% - 99.5%	10%
		< 99.5%	20%
Incident Response Time	P1	24x7x365	15 mins -
	P2	24x7x365	30 mins -
	P3	BH	4 hours -
	P4	BH	12 hours -
Target Restoration Time	P1	24x7x365	4 hours -
	P2	24x7x365	8 hours -
	P3	BH	24 hours -
	P4	BH	48 hours -
Service Request Response Time <sup>+</sup>	P5	24x7x365	2 hours -
	P6	BH	4 hours -
	P7	BH	24 hours -
Service Request Fulfilment Time <sup>+</sup>	P5	24x7x365	12 hours -
	P6	BH	24 hours -
	P7	BH	5 Business Days -
Service Delivery	Off-Net	BH	40 - 60 Business Days -
	On-Net 20	BH	20 Business Days -
	On-Net 40	BH	40 Business Days -

### A Further Deep-dive into Alerts

*TP, FP, FN, and TN:*

Alerts that are fed through to a SOC can either reveal genuine malicious intent, or incorrectly diagnose an event as an attack. Each of these two outcomes can be further analysed using the following four classifications (v500 Systems, 2016):

- True positives: These are alerts that have correctly identified an event as a security concern or incident.
- False positives: If we investigate an alarm to discover that there was no need for concern as the behaviour discovered was a legitimate user perhaps forgetting their password, then we classify the alert as a false positive

- False negatives: Perhaps the most damaging of the four classifications is the false negative. Here, we do not receive an alarm, however a real attack has occurred and no alarm was raised.
- True negatives: Pertains to situations when there is no malicious behaviour on the network, and no alarms were triggered.

### *Tuning*

According to research by Infocyte (2021), false positives make up approximately 40% of daily cybersecurity alerts. Chickowski (2019) of Bitdefender reports a figure closer to 50% with the added insight that approximately 25% of an analyst's work is dedicated to "chasing false positives". Given the nature of the work of a SOC, time is an invaluable asset and any allocation of this asset towards the investigation of legitimate threats is well spent. SIEM tuning offers a methodology to review correlation rules and detection configurations with the goal of decreasing the number of false positives triggered. There are instances where a SIEM comes with out-of-the-box correlation rules that are too general and not fit for an organisation. Therefore, the tuning process could look like a thorough understanding of a customer's unique environment, which assets they care about the most, and other nuances that could be considered when creating rules (Itangata & Daniels, 2020).

## **Auxiliary Investigative Tools**

### *Virtual Machines & Sandboxes*

Part of an investigation in a SOC may include dealing with potentially malicious software, commonly known as malware. As the goal of malware is to exploit a computer system (Regan & Belcic, 2021), it is highly recommended that such investigations are performed in isolated environments such as virtual machines (GeeksforGeeks, 2020) and sandboxes (GoGuardian, 2020).

- *Cuckoo*
  - Cuckoo is an open source tool that utilizes sandboxing to provide an environment where analysts can safely analyse malware.
- *Browserling*
  - Browserling provides an application via the browser where a user may access a completely isolated virtual machine with options to select browser versions and a select number of operating systems (Bartlett, 2018).
- *Any.run*
  - Similar to Browserling, Any.Run provides an online tool where the sandboxed service provides users the ability to safely detonate malware via virtual machines that also allow you to interact with any malicious files in a dedicated environment (Abrams, 2020).

### *Scanners*

- *Virus Total*
  - VirusTotal (n.d.) is an online service which accepts files, URLs, IP addresses, and file hashes which it then sends through over 70 antivirus scanners and URL/domain blocklisting services.

- *URLscan*
  - URLscan (n.d.) offers another scanner which performs an automated process to retrieve various findings about the user's URL entry.

### *Decoders*

- *Cyberchef*
  - Cyberchef (n.d.) is a web application that has been referred to as "The Cyber Swiss Army Knife". As implied by the reference, it comes with many useful encoding and decoding capabilities.

### *Message Header Analyzers*

An often neglected part of reading emails is the header information. Email headers offer richer context around the true nature of an email (Gandhi, 2018), and if there are suspicions about an email's legitimacy, the following tools offer ways to utilize headers to determine if a phishing attempt is being carried out.

- *Message Header Analyzer (MHA) mail app*
  - MHA (Griffin, n.d.) displays header information in a readable format, offering Add-in functionality for Microsoft Outlook (Panagiotidis, 2020)
- *Google's Messageheader Tool*
  - Messageheader (Google, n.d.) uses email header information to calculate the delay between email servers with the logic that if there are notable delays in delivery, then there is potential of overloaded spam server usage (Gandhi, 2018).

## 1.6. PROJECT TASKS

---

### Ticketing

As mentioned in the literature review section, ticketing plays an important part in a SOC. As interns, we were shown how tickets were:

- Displayed in ticketing software
- How the corresponding alerts were summarized
- How to view the priority of a ticket
- Who was assigned a ticket
- What the status/progress of a ticket was
- How to use the filter functionality of ticketing software
- How to assign a team member a ticket

Once accustomed to the software, we were given the authority to assign tickets to the relevant SOC members best equipped to resolve them. In order to assign a ticket correctly, one must understand the context of the ticket, which is inferred by analysing the ticket metadata previously mentioned (status, team member, etc). The correctness of an assignment of a ticket is based on the following variables:


- Priority level - assign the ticket within the set SLA. The analyst should be mindful of the timeliness of a ticket, and prioritize more critical tickets (P1s and P2s).
- Technology - alerts can be triggered by a customer directly, or a number of SIEMs and EDRs. In a large SOC, there may be a number of such solutions, and thus, various team members may specialize in a certain product. The ticket issuer must be able to distinguish which tool triggered the alert
- Customer - depending on the SOC environment, analysts and engineers may have a portfolio of customers they serve. Therefore, the ticket should be assigned to the SOC member who has the customer in their portfolio
- Engineering Tasks vs Analyst Tasks - certain types of alerts pertain to engineers, while others, to analysts. Knowing how to establish one from the other was a fundamental skill for ticketing

As interns, we were able to quickly learn how to achieve ticket correctness due to a well-documented internal Wiki which outlined exactly which team members were engineers and which were analysts. The Wiki also outlined which team members had certain customers in their portfolios as well as the software products they specialized in for that customer. In a SANS Institute (2019, p. 7) survey, it was found that using a combination of ticketing systems like Jira with Wiki software such as Confluence was common amongst established SOC's, and the effectiveness of this type of knowledge management was immediately apparent when first learning how to ticket correctly.

### Alert Examples

#### Impossible Travel - Analyst Ticket

According to Roberts (2019), the Impossible Travel alert is raised when a situation occurs where a user's current logged IP location and their previous logged location is physically impossible based on the amount of time it would take to reasonably achieve such a commute.



However, as outlined by Stachura and Frederick (2020), complicating factors such as switching from a work ISP to a mobile ISP or the use of non-company owned VPNs can cause large variations in reported location, consequently producing false positives. The analyst must look for documentation of any travels planned by employees, or look up IP addresses on scanning websites to assess their reputation and nature, to make a decision on whether or not the alert is a false positive.

### **Data Source Availability - Engineer Ticket**

Just as the circulation of blood is vital for the organs of a human body, so is the flow of data from data sources being monitored in a customer's environment to a SOC. Without a consistent influx of logs, it is difficult to deliver on real time monitoring capabilities which may be needed as compliance. Some of the tickets I issued were of this nature, and as mentioned by McAfee (2021), there are many reasons for a data source to become unavailable. These range from:

- Misconfiguration errors
- Data parsing issues
- Blocked data logging traffic by a firewall

## **Shadowing**


There are many moving parts in a SOC, and the complexities that arise from such an environment require SOC team members to have a deep understanding of the nuances that come with specific tools, protocols, and processes. For a potential employee or intern, these very complexities can be difficult to grasp solely from reading material or verbal explanations. Job shadowing allows learners to experience another dimension of skill acquisition, where they see first hand an accurate representation of how tasks are performed, often leading to theoretical knowledge becoming more concrete (Heathfield, 2020, "When Is Job Shadowing Most Important and Effective?" section).

### **Phishing Investigations - Analyst Checks**

Phishing is the use of social engineering to craft a malicious message via email or another messaging technology and includes some method of stealing the victim's credentials (Fruhlinger, 2020). Many of the tools mentioned in the Auxiliary Investigative Tools section were used by the analyst to determine if the alerts were false positives, or warranted further investigation. There were two main considerations I noted when reviewing lessons learnt from shadowing a phishing investigation:

1. **System Isolation and De-Risking:** It is of paramount importance that any analysis of potential phishing attempts were conducted in an environment that could pose no risk to a customer's or Datacom's network. Thus, virtual machines and sandbox technology should be utilized to ensure that this level of security is achieved. Defanging was a term that was often used to refer to further de-risking phishing analysis (IBM, 2019). It describes the process of replacing/augmenting characters in URLs or IP addresses so that accidental clicks of malicious links were prevented.
2. **Context:** Much can be inferred from an analyst's understanding of their customer's environment. This understanding provides the context needed to signal any anomalous flags in an email. Some out-of-context signals should be fired when emails





are sent at unusual times, or personal emails are requesting wire transfers when usually conducted using a business email address.

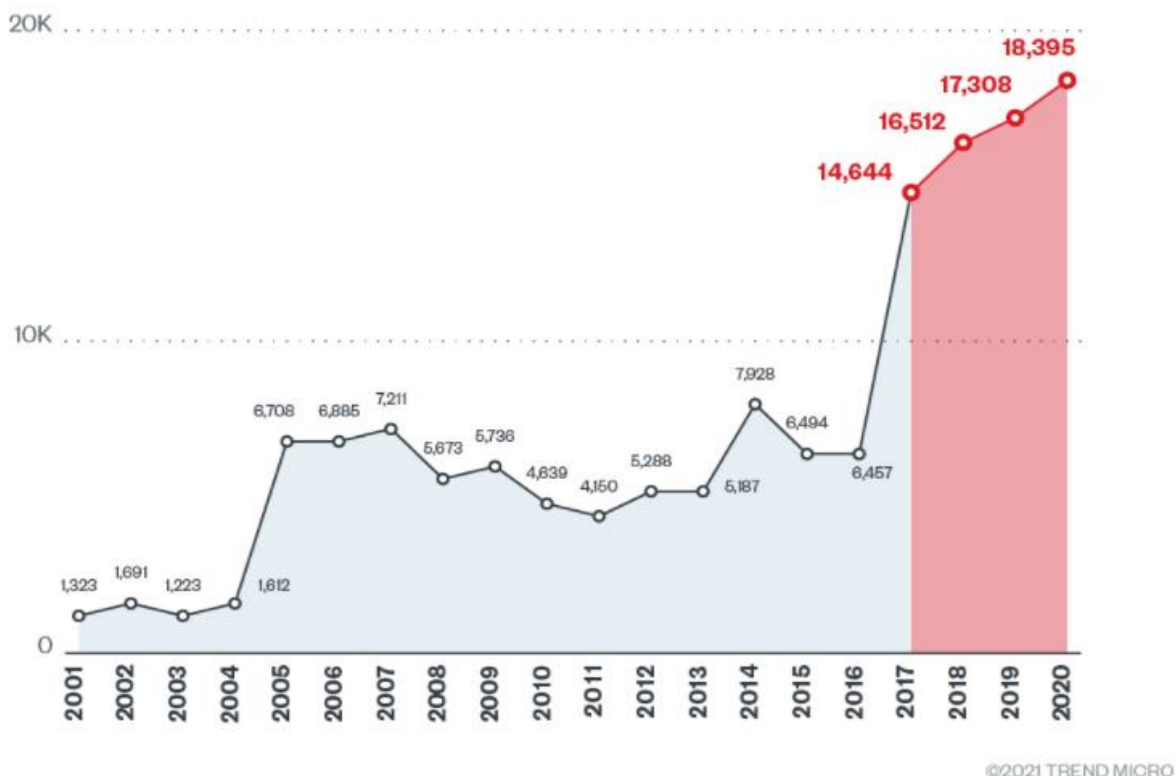
Each analyst will have their own methodology of analysing phishing attempts, but a rough outline of one that was performed at Datacom can be summarised by the following steps:

1. Ensure that any handling of the phishing material is performed in an isolated environment. Such an environment could be built using Cuckoo software.
2. With the email itself, encrypt and zip its content with a password such that only those who are purposefully looking to investigate it do so.
3. Analyse the email using the tools outlined in the Auxiliary Investigative Tools section of this report, looking for various IOCs such as:
  - a. Malicious IP addresses and URLs
  - b. Spam confidence levels
4. If need be, open links inside isolated services like Any.run or Browserling to gain further knowledge on the origins of the attack
5. If it turns out that the alert is indeed a True Positive alert, then the analyst must consider the following further checks:
  - a. Use the SIEM/EDR to assess if the person the email was sent to clicked on any links. If so, isolate their machine if possible, lock their accounts, and reset all user credentials. Direct the user towards resources that help educate them about how to detect a phishing attack
  - b. Check to see if any artifacts were downloaded by the user. If so, contain the device, run malware scans, and if necessary, rebuild the user's machine.
  - c. Perform a search to check that no other users in the organisation have received emails from the attacker, and that no other user has clicked on the same malicious link. Purge the malicious emails while also blocking the IP addresses and URLs associated with the attacker.

### Software Patching - Engineer Checks

The engineers responsible for the deployment of various software solutions for data collection, monitoring and alerting are also responsible for the maintenance of this software for both Datacom and the customers Datacom protects. As reported in the findings of Trend Micro (2021) and seen in Figure 3, there has been a notable surge in software vulnerabilities in recent years. Engineers must stay vigilant and constantly monitor the software systems they roll out to customers to ensure that vulnerabilities reported by vendors or other security authorities are patched as soon as possible.

Figure 3. The number of software vulnerabilities per year assigned CVE numbers



## Additional Training

Our internship experience also included some vendor specific training. As previously mentioned, Splunk Enterprise is a software solution which offers data collection, aggregation and visualisation tools, and in particular has many features that modernize a SOC. Considering this, part of the requirements of our internship was to complete some Splunk training provided by the company itself. Specifically, the training program is called Splunk Fundamentals 1, and is a free module which offers a certificate if the learner passes a final exam covering the main ideas. Some of the content included using the search language, creating reports, dashboards, and other fundamentals. I managed to successfully pass the training, and the corresponding certificate is provided in the Appendix section.





## 1.7. CONCLUSION AND LESSONS LEARNED

---

There have been many world-wide reports of the increase in cybercrime as hackers craft sophisticated attacks which exploit both technology and human trust. The results of these attacks are often millions of dollars in damages as well as public distrust of brand names who fall victim to the ploys of malicious actors.

The field of cybersecurity has evolved in parallel with the evolution of the cyber-criminal underworld as a direct response to hackers capitalising on the vulnerabilities of individuals and organisations. To be effective in securing the vulnerable from attacks, cybersecurity providers must have the adequate people, processes and tooling in place to combat against the growing advancements of cyber criminals.

My internship with Datacom demonstrated how the triad of people, process and technology are brought together synergistically to provide its customers a fighting chance in the online space. Datacom also highlighted how each of the three parts mentioned are equally crucial in order to provide thorough monitoring with time-sensitive alerting.

In hindsight, more proactivity on my part to understand tickets pertaining to the engineering team would have given me a more rounded picture of the pain points of the SOC as a whole. Having more of an analyst background, I was naturally drawn to the tickets of the analysts, however, if I could re-do the experience, I would have made sure to ask more questions about other engineering-based tickets I saw come through the ticketing system.


Nonetheless, I have learnt a lot and have seen great value in the internship with Datacom. I have a greater appreciation for the role of managers within a SOC, as there are many aspects to consider which have been explored in this report. Moving forward with my cybersecurity journey, I believe that my new-found knowledge of the role of people, processes, and technology will be directly and immediately applicable in both my Unitec studies and a future role within the industry.

I look forward to honing my analyst skills through acquiring cybersecurity certifications as well as an exploration of a mix of blue-team and red-team Capture the Flag (CTF) events. I will continually refine my engineering skills through updating and upgrading my home lab.

## REFERENCES

---

- Abrams, L. (2020, June 12). *Malware adds online sandbox detection to evade analysis*. BleepingComputer. <https://www.bleepingcomputer.com/news/security/malware-adds-online-sandbox-detection-to-evade-analysis/>
- Allen, D., Sharkey, K., & Buck, A. (2021, April 4). *Security operations - Cloud Adoption Framework*. Microsoft Docs. <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-operations>
- Armerding, T. (2019, July 16). *Why hackers are targeting your web apps (and how to stop them)*. Security Boulevard. <https://securityboulevard.com/2019/07/why-hackers-are-targeting-your-web-apps-and-how-to-stop-them/>
- AT&T Cybersecurity. (n.d.). *Correlation Rules*. Retrieved July 30, 2021, from <https://cybersecurity.att.com/documentation/usm-anywhere/user-guide/rules-management/correlation-rules.htm#:~:text=The%20logic%20to%20identify%20these,from%20the%20same%20data%20source..>
- Bartlett, J. (2018, August 17). *Browserling Tutorial for Beginners*. QA World. <https://qa.world/browserling-tutorial-for-beginners/>
- Cherwell. (n.d.). *Service Management for Better IT Outcomes*. Cherwell.Com. Retrieved July 29, 2021, from <https://www.ivantiv.com/solutions/service-management>
- Chickowski, E. (2019, September 2). *Every Hour SOCs Run, 15 Minutes Are Wasted on False Positives*. Bitdefender Business Insights Blog. <https://businessinsights.bitdefender.com/every-hour-socs-run-15-minutes-are-wasted-on-false-positives>
- Chuvakin, A. (2013, July 26). *Named: Endpoint Threat Detection & Response*. Blogs.Gartner.Com. <https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/>
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 6). *SP 800–61 Rev. 2, Computer Security Incident Handling Guide | CSRC*. Csrc.Nist.Gov. <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>



Cloudflare. (n.d.). *What is a DDoS booter/IP stresser? | DDoS attack tools*. Retrieved August 11, 2021, from <https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/#:%7E:te>

Cooper, P. (2020, January 28). *MTTD and MTTR: Two Metrics to Improve Your Cybersecurity*. Threatpost. <https://threatpost.com/mttd-and-mttr-two-metrics-to-improve-your-cybersecurity/152149/>

Correa, N. (2020, June 11). *EDR and UEBA for the Win: Uncovering the Insider Threat*. Micro Focus Community. <https://community.microfocus.com/cyberres/b/sws-22/posts/edr-and-ueba-for-the-win-uncovering-the-insider-threat>

Crawley, K. (2018, February 20). *How SIEM Correlation Rules Work*. AT&T Cybersecurity. <https://cybersecurity.att.com/blogs/security-essentials/how-siem-correlation-rules-work>

Cyber Chef. (n.d.). *GitHub - gchq/CyberChef: The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis*. GitHub. Retrieved August 1, 2021, from <https://github.com/gchq/CyberChef>

Danquah, P. (2020). Security Operations Center: A Framework for Automated Triage, Containment and Escalation. *Journal of Information Security*, 11(04), 225–240. <https://doi.org/10.4236/jis.2020.114015>

Datacom. (n.d.). *Security Operations – Monitor & Detect Cyber Threats |*. Retrieved August 11, 2021, from <https://datacom.com/au/en/solutions/security/security-operations>

Datacom Group Limited. (n.d.). *Datacom | Australasia's Largest Homegrown Tech Company*. Datacom. Retrieved August 11, 2021, from <https://datacom.com/nz/en>

Exabeam. (n.d.-a). *SOC, SecOps and SIEM: How They Work Together*. Retrieved July 21, 2021, from <https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/>

Exabeam. (n.d.-b). *What is SIEM? Complete Guide to the Future SOC*. Retrieved July 31, 2021, from <https://www.exabeam.com/siem-guide/what-is-siem/>

Fruhlinger, J. (2020, September 4). *What is phishing? How this cyber attack works and how to prevent it*. CSO Online. <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

- 
- Gandhi, R. (2018). *Phishing - Email Header Analysis* · nebraska-gencyber-modules. Mlhale.Github.io.  
<https://mlhale.github.io/nebraska-gencyber-modules/phishing/email-headeranalysis/>
- Ganesh, B. (2021, June 20). *SIEM Better Visibility for SOC Analyst to Handle an Incident with Event ID*. GBHackers On Security. <https://gbhackers.com/siem-for-better-visibility-for-an-analyst-to-handle-an-incident/>
- GeeksforGeeks. (2020, July 3). *Virtual Machine for Malware Analysis*.  
<https://www.geeksforgeeks.org/virtual-machine-for-malware-analysis/>
- GoGuardian. (2020, March 19). *What is Sandbox Security?*  
<https://www.goguardian.com/glossary/what-is-sandbox-security/>
- González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, 21(14), 4759. <https://doi.org/10.3390/s21144759>
- Google. (n.d.). *Messageheader*. Toolbox.Googleapps.Com. Retrieved August 1, 2021, from <https://toolbox.googleapps.com/apps/messageheader/>
- Government Communications Security Bureau. (n.d.). *New Zealand Information Security Manual*. Nzism.Gcsb.Govt.Nz. Retrieved July 21, 2021, from <https://www.nzism.gcsb.govt.nz/>
- Griffin, S. (n.d.). *Message Header Analyzer*. Message Header Analyzer. Retrieved August 1, 2021, from <https://mha.azurewebsites.net/>
- Harris, C. (2019). *Former Desjardins president falls victim to identity theft after data breach*. CBC. <https://www.cbc.ca/news/canada/montreal/desjardins-former-president-identity-theft-data-breach-1.5210717>
- Hays, C. (2020, January 29). *The Ultimate Guide to Data Breaches and Identity Theft*. Bloom Blog. <https://bloom.co/blog/ultimate-guide-to-data-breaches-and-identity-theft/#what-is-identity-theft>
- Heathfield, S. M. (2020, June 4). *Job Shadowing Is a Good Way to Do On-the-Job Training*. The Balance Careers. <https://www.thebalancecareers.com/job-shadowing-is-effective-on-the-job-training-1919285>
- Hubbard, R. (2015). *Impostors bilk Omaha's Scoular Co. out of \$17.2 million*. Omaha World-Herald. [https://omaha.com/business/impostors-bilk-omaha-s-scoular-co-out-of-million/article\\_25af3da5-d475-5f9d-92db-52493258d23d.htm](https://omaha.com/business/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.htm)



IBM. (2019). *Email Security – Defanging URLs*. © Copyright IBM Corporation 2018.

<https://www.ibm.com/docs/en/rsoa-and->

[rp/32.0?topic=SSBRUQ\\_32.0.0/com.ibm.resilient.doc/install/resilient\\_install\\_defangURLs.htm](https://www.ibm.com/docs/en/rsoa-and-rp/32.0?topic=SSBRUQ_32.0.0/com.ibm.resilient.doc/install/resilient_install_defangURLs.htm)

Infocyte. (2021, March 10). *Cybersecurity 101: What You Need To Know About False Positives and False Negatives*. <https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-and-false-negatives/>

Intersoft Consulting. (2019, September 3). *Recital 85 - Notification Obligation of Breaches to the Supervisory Authority*. General Data Protection Regulation (GDPR). <https://gdpr-info.eu/recitals/no-85/>

Itangata, E., & Daniels, M. (2020, August 20). *Are you in tune? Why SIEM tuning is important*. Binary Defense. <https://www.binarydefense.com/are-you-in-tune-why-siem-tuning-is-important/>

Kass, H. D. (2021, July 19). *IoT Hackers Target Millions of Devices in Pandemic, Report Says*. MSSP Alert. <https://www.msspalert.com/cybersecurity-research/iot-report-zscaler-findings/>

Kienzle, J. (2020, January 17). *The difference between SIEM and EDR*. LogPoint. <https://www.logpoint.com/en/blog/the-difference-between-siem-and-edr/>

Lewkowicz, J. (2020, October 20). *Report: Most SOCs are using AI and machine learning tools to detect advanced threats*. ITOps Times. <https://www.itopstimes.com/it-security/report-most-socs-are-using-ai-and-machine-learning-tools-to-detect-advanced-threats/>

Mareels, D. (2021, March 4). *What next for the Security Operations Center (SOC) in 2021?* ITProPortal. <https://www.itproportal.com/features/what-next-for-the-security-operations-center-soc-in-2021/>

McAfee. (2021, July 1). *How to troubleshoot when no events are received from a new data source*. <https://kc.mcafee.com/corporate/index?page=content&id=KB82387>

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39–53. <https://doi.org/10.1145/997150.997156>

Morgan, S. (2021, April 27). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*.

Cybercrime Magazine. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>





Netscout. (2021). *Netscout Threat Intelligence Report* (No. 6).

[https://www.netscout.com/sites/default/files/2021-04/ThreatReport\\_2H2020\\_FINAL\\_0.pdf](https://www.netscout.com/sites/default/files/2021-04/ThreatReport_2H2020_FINAL_0.pdf)

Overby, S., Greiner, L., & Paul, L. G. (2017, July 5). *What is an SLA? Best practices for service-level agreements*. CIO. <https://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html>

Palmer, D. (2020, November 11). *DDoS attacks are cheaper and easier to carry out than ever before*. ZDNet. <https://www.zdnet.com/article/ddos-attacks-are-cheaper-and-easier-to-carry-out-than-ever-before/>

Panagiotidis, P. (2020, July 27). *How To View Info about E-Mail Message Headers in Microsoft Outlook?* Smart Office. <https://officesmart.wordpress.com/2020/07/27/how-to-view-info-about-e-mail-message-headers-in-microsoft-outlook/>

Power, K. (2016, August 17). *The Evolution of Hacking*. The State of Security. <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/>

PwC. (2017). *Consumer Intelligence Series: Protect.me*. <https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf>


Regan, J., & Belcic, I. (2021, July 2). *What Is Malware? The Ultimate Guide to Malware*. Avg. <https://www.avg.com/en/signal/what-is-malware>

Rishi Iyengar and Clare Duffy, CNN Business. (2021, June 4). *Why hackers are going after physical infrastructure*. CNN. <https://edition.cnn.com/2021/06/03/tech/ransomware-cyberattack-jbs-colonial-pipeline/index.html>

Roberts, C. (2019, October 23). *Understanding Office 365 Impossible Travel*. Daymark. <https://www.daymarksi.com/information-technology-navigator-blog/understanding-office-365-impossible-travel>

Rowell, M. D. (2017, March). *Cyber Indicators of Compromise: A Domain Ontology for Security Information and Event Management* (Thesis). Naval Postgraduate School. <https://apps.dtic.mil/sti/pdfs/AD1046101.pdf>

Salvage, P. (2019, March). *Artificial Intelligence Sweeps Hedge Funds*. BNY Mellon. <https://www.bnymellon.com/us/en/insights/all-insights/artificial-intelligence-sweeps-hedge->



funds.html#:~:text=How%20Hedge%20Funds%20Use%20AI,different%20strategies%20and%20tailor%20allocations.

SANS Institute. (2019). *Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey*. <https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf>

Schwartz, M. (2021). *Data Breach Culprits: Phishing and Ransomware Dominate*. Bank Info Security. <https://www.bankinfosecurity.com/data-breach-culprits-phishing-ransomware-dominate-a-16775>

Shread, P. (2021, July 31). *Top Endpoint Detection & Response (EDR) Solutions for 2021*. ESecurityPlanet. <https://www.esecurityplanet.com/products/edr-solutions/>

Stachura, G., & Frederick, T. (2020, May 12). *Impossible Travel*. Security Risk Advisors. <https://sra.io/blog/impossible-travel/>

Stern, A. (2021, July 21). *Understanding The SOC Team Roles And Responsibilities*. Siemplify. <https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities/>

T-Mobile. (2021, February 24). *5 Reasons Hackers Target Mobile Devices And How To Stop Them*. Forbes. <https://www.forbes.com/sites/tmobile/2021/02/24/5-reasons-hackers-target-mobile-devices-and-how-to-stop-them/?sh=73d0db727b28>

Trend Micro. (2021, April 7). *The Nightmares of Patch Management: The Status Quo and Beyond* - Security News. <https://www.trendmicro.com/vinfo/nz/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond>


TrustRadius. (n.d.). *Top Rated Security Information and Event Management (SIEM) Products*. Retrieved August 1, 2021, from <https://www.trustradius.com/security-information-event-management-siem>

Trustwave. (n.d.). *Trustwave*. Retrieved July 31, 2021, from <https://www.trustwave.com/en-us/>

Trustwave. (2019). *Trustwave Service Description: Threat Detection & Response - Managed Detection*. <https://www.trustwave.com/media/17367/trustwave-tdr-managed-detection-password-protected-v15.pdf>

URLscan. (n.d.). *About - urlscan.io*. URLscan.io. Retrieved August 1, 2021, from <https://urlscan.io/about/>





v500 Systems. (2016, September 1). *False Positive, False Negative, True Positive and True Negative*. <https://www.v500.com/false-positive-false-negative-true-positive-and-true-negative/>

Virus Total. (n.d.). *How it works*. Retrieved August 1, 2021, from <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works>

Vocus. (n.d.). *Vocus*. Retrieved July 31, 2021, from <https://www.vocus.co.nz/home>

Vocus. (2020). *Vocus Service Level Agreement*. <https://www.vocus.co.nz/sites/default/files/2020-04/Vocus%20NZ%20-%20SLA.pdf>

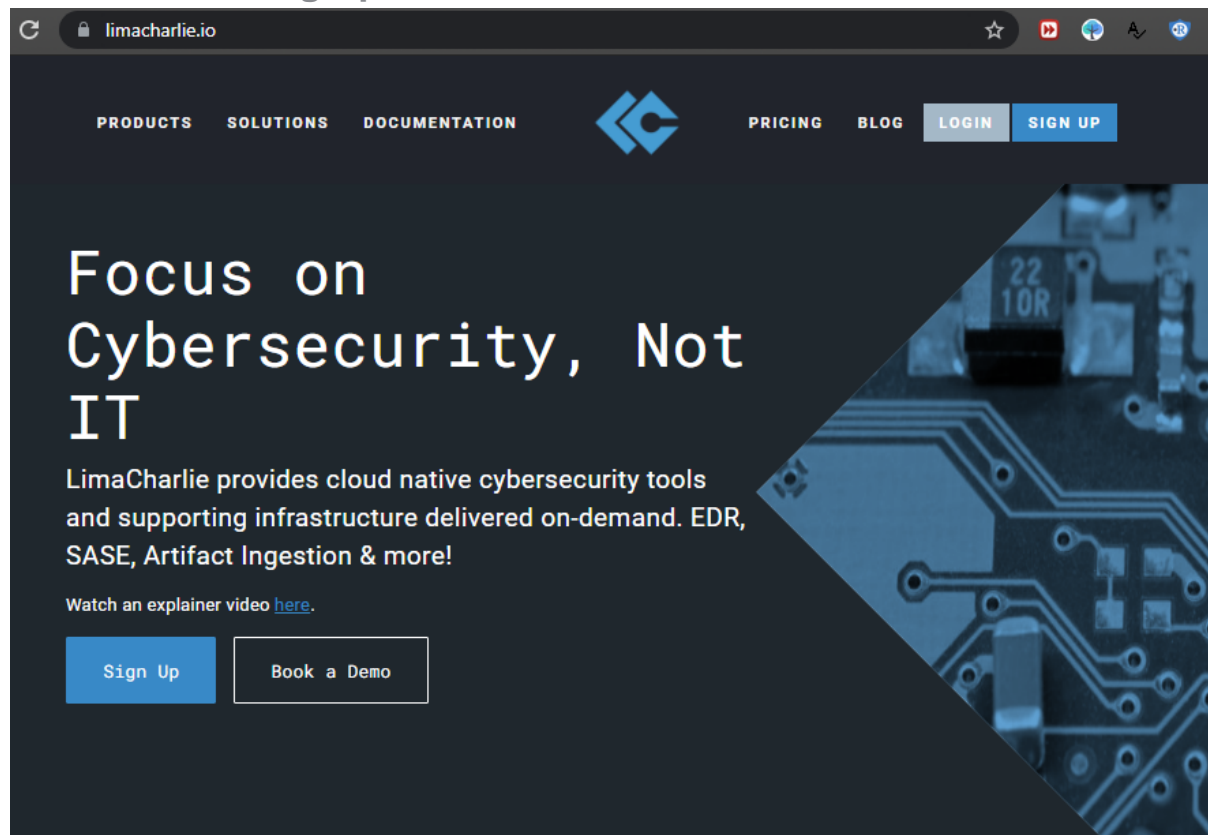
Wizard Cyber. (2020, October 30). *SLA SOC | WizardCyber*. <https://wizardcyber.com/sla-soc/#>

Wizard Cyber. (2021, June 10). *Cyber Security Experts for SMEs | Cyber Security Partner*. <https://wizardcyber.com/>

Zhang, E. (2020, December 1). *How to Build a Security Operations Center (SOC): Peoples, Processes, and Technologies*. Digital Guardian. <https://digitalguardian.com/blog/how-build-security-operations-center-soc-peoples-processes-and-technologies>

## APPENDICES

### Outline of Setting Up LimaCharlie EDR



### Trusted by Technological Leaders in Information Security

LimaCharlie is trusted by some of the fastest growing and most competent information security practitioners out there (and these are just the ones we are allowed to show you).

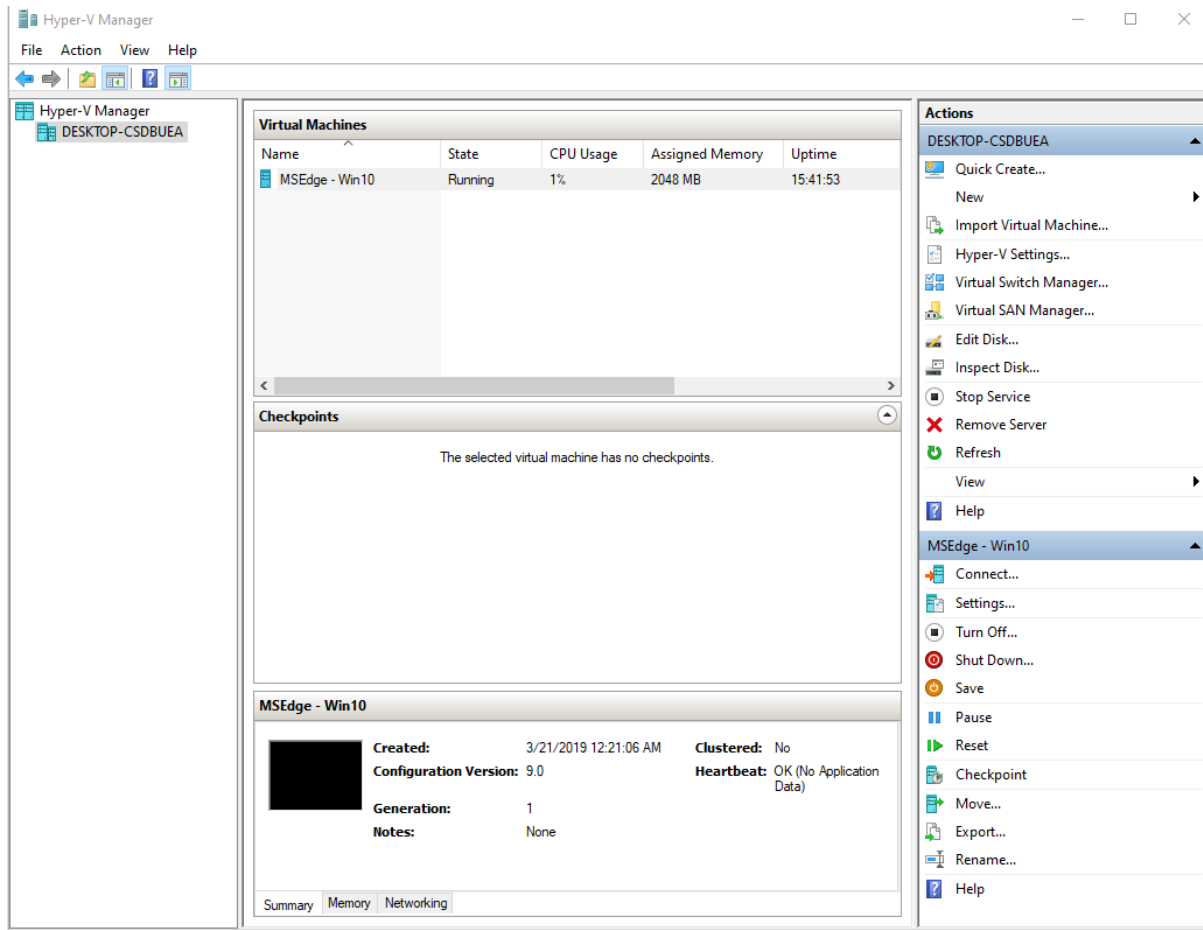


Cybersecurity tools and infrastructure delivered in a manner similar to AWS or any major cloud provider.

LimaCharlie is a cloud-native EDR and allows users to install what the company calls *sensors/agents* on two hosts for free. Sensors and agents essentially act as the mechanism which logs and sends data about its host back to LimaCharlie to evaluate. As this option was free, it lent well for experimentation purposes in my homelab.

## Virtual Machine Set Up

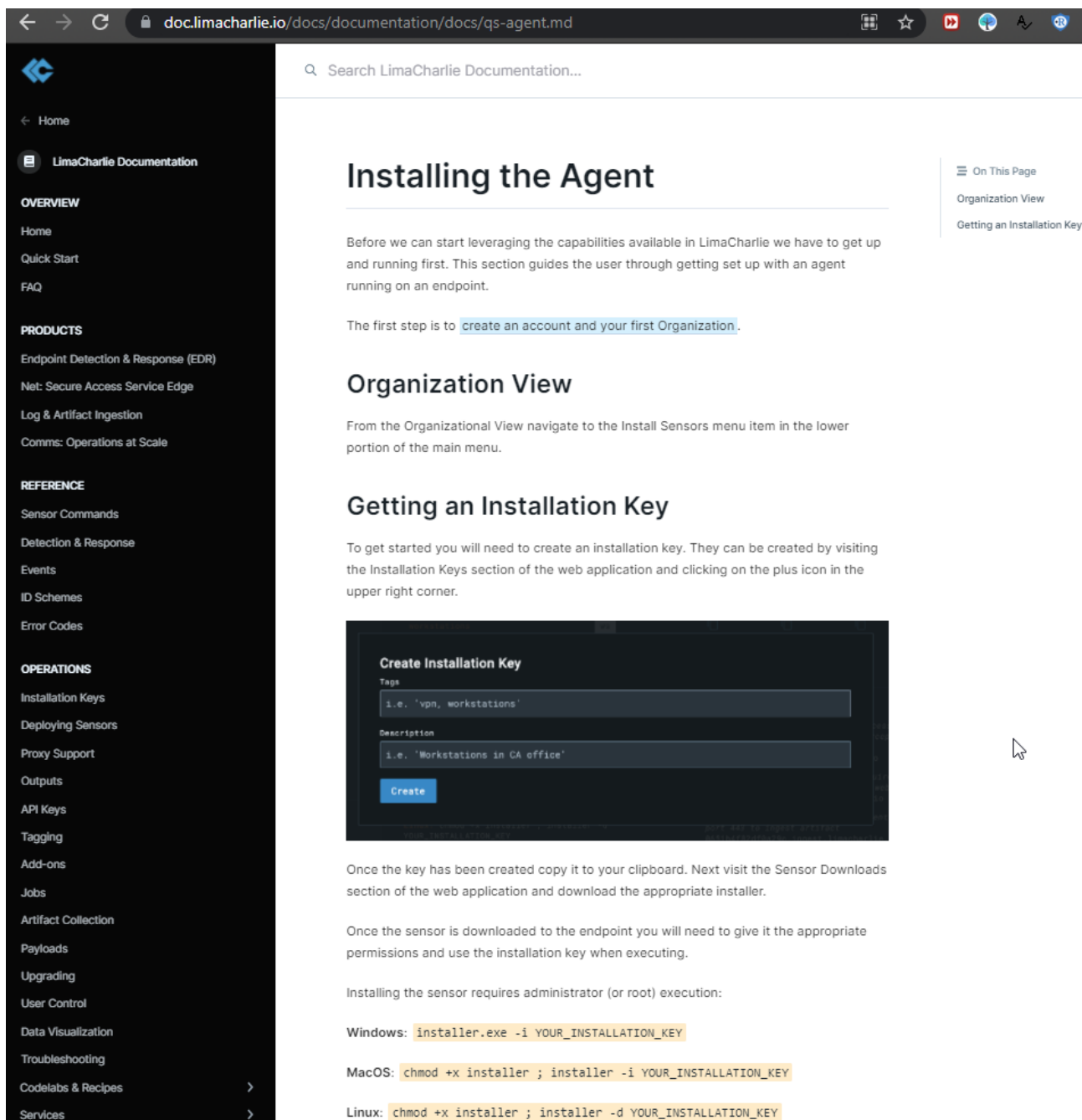
I decided to use a Windows 10 host running on Hyper-V Manager on my laptop as a test machine to install a LimaCharlie agent on.



Once the virtual machine was set up, all that was left to do was to install a LimaCharlie agent on it so that we can start sending data back to LimaCharlie.

## Installing LimaCharlie Agents and Setting Up EDR Rules

Following LimaCharlie's documentation on setting up an agent on an endpoint is clear and easy to follow. I was able to step through the process of creating an organisation and getting installation keys for my windows virtual machine by following the steps on the webpage at <https://doc.limacharlie.io/docs/documentation/docs/qs-agent.md>



The screenshot displays the LimaCharlie documentation website. The sidebar on the left contains navigation links for Home, Overview, Products, Reference, and Operations. The main content area features the title 'Installing the Agent' and a search bar. Below the title, there is a paragraph explaining the initial setup steps. A section titled 'Organization View' follows, detailing how to navigate to the Install Sensors menu. The 'Getting an Installation Key' section includes a screenshot of the 'Create Installation Key' form, which has fields for 'Tags' (e.g., 'vpn, workstations') and 'Description' (e.g., 'Workstations in CA office'). Below the form, instructions are provided for creating the key on Windows, MacOS, and Linux.

← → ↺ doc.limacharlie.io/docs/documentation/docs/qs-agent.md

Search LimaCharlie Documentation...

## Installing the Agent

Before we can start leveraging the capabilities available in LimaCharlie we have to get up and running first. This section guides the user through getting set up with an agent running on an endpoint.

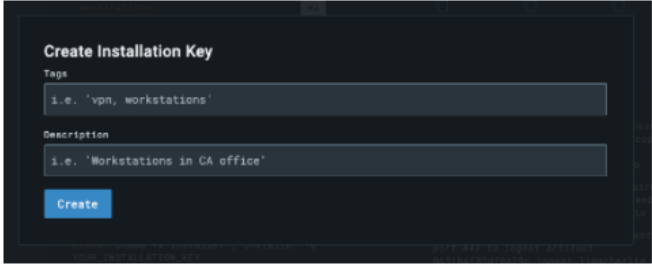
The first step is to [create an account and your first Organization](#).

## Organization View

From the Organizational View navigate to the Install Sensors menu item in the lower portion of the main menu.

## Getting an Installation Key

To get started you will need to create an installation key. They can be created by visiting the Installation Keys section of the web application and clicking on the plus icon in the upper right corner.



Once the key has been created copy it to your clipboard. Next visit the Sensor Downloads section of the web application and download the appropriate installer.

Once the sensor is downloaded to the endpoint you will need to give it the appropriate permissions and use the installation key when executing.

Installing the sensor requires administrator (or root) execution:

Windows: `installer.exe -i YOUR_INSTALLATION_KEY`

MacOS: `chmod +x installer ; installer -i YOUR_INSTALLATION_KEY`

Linux: `chmod +x installer ; installer -d YOUR_INSTALLATION_KEY`

The hostname of my virtual machine is [msedgewin10.mshome.net](#) and on the LimaCharlie web app, this virtual machine appears if the agent has been installed successfully on the endpoint as highlighted in the image below.

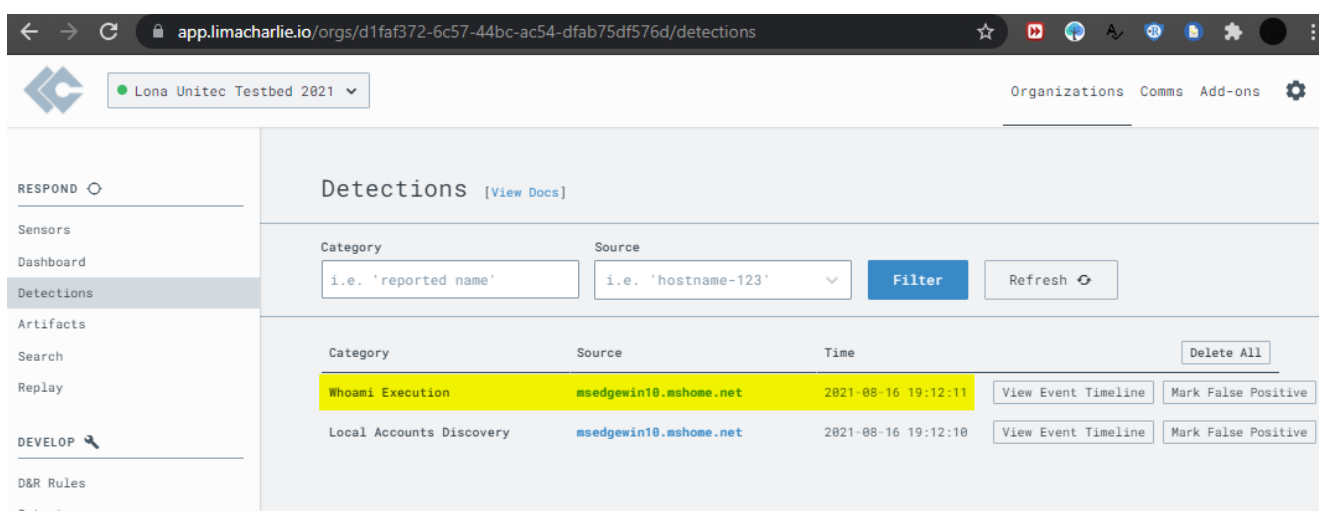
Next, I needed to set up some default rules to test whether or not LimaCharlie could successfully detect events that I wanted alerts for.

LimaCharlie allows users to create their own custom rules as well as use already-built rules such as Sigma rules. Having no prior knowledge of designing my own rules or signatures on an EDR platform before, I enable Sigma rules which provide hundreds of boiler-plate signatures which can be immediately deployed on my virtual machine for testing.

One of the rules that comes pre-packaged in Sigma is to trigger an alert when the command **whoami** is used in the command line on the endpoint. To test that we can successfully trigger this alert, I open up powershell on the virtual machine and execute **whoami** to see if the detection appears in the LimaCharlie web app.



We can confirm the hostname on the virtual machine is **msedgewin10** and we indeed see a detection come through on LimaCharlie of a **Whoami Execution** triggered.



Now that my virtual machine has successfully installed a working LimaCharlie agent, I want to set up an alerting system.

### Setting Up Alerting via Slack

LimaCharlie allows for alerting of detections on many platforms such as Amazon S3, SFTP, SMTP, Webhooks, Slack, and also integrates with Splunk.

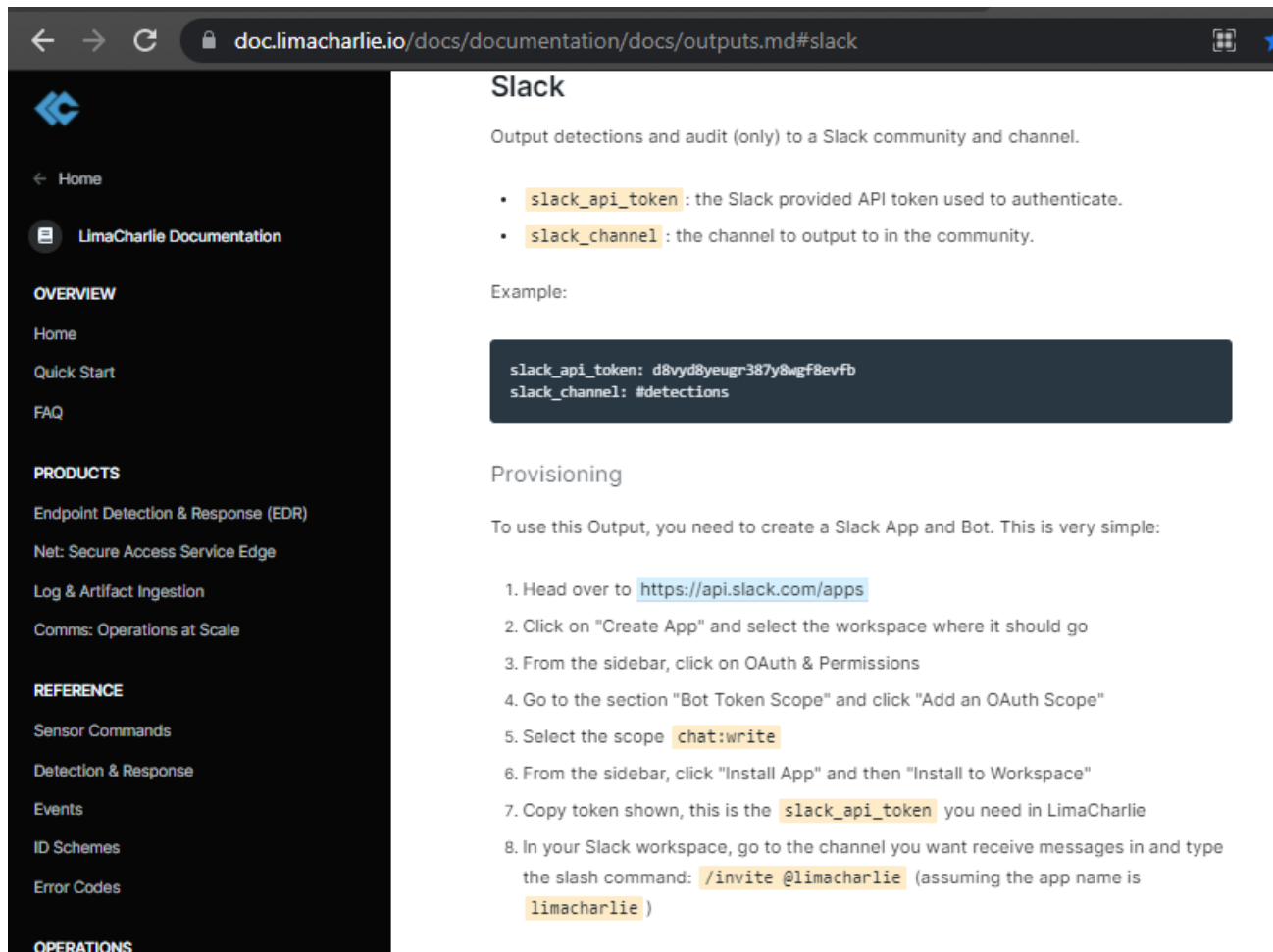
I wanted to see if I could begin with setting up alerts to Slack as I use this platform on a day-to-day basis, am familiar with its functions, and also have it installed on my mobile phone.

There is documentation on how to gain access to the Slack api token that will be needed for LimaCharlie. I had set up a Slack workspace especially for my homelab detection purposes and the Slack channel dedicated to alerts is called **#personal-cybersecurity-research**. The

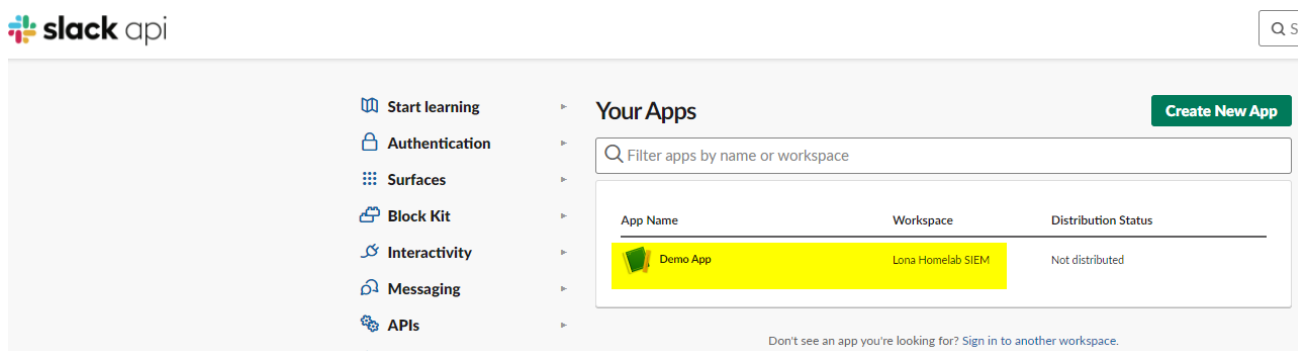


Slack app I created to alert me of LimaCharlie detections is called **Demo App**. The relevant LimaCharlie documentation can be found on

<https://doc.limacharlie.io/docs/documentation/docs/outputs.md#slack>.



The screenshot shows the LimaCharlie documentation page for Slack output configuration. The page has a dark sidebar with navigation links: Home, LimaCharlie Documentation, OVERVIEW (Home, Quick Start, FAQ), PRODUCTS (Endpoint Detection & Response (EDR), Net: Secure Access Service Edge, Log & Artifact Ingestion, Comms: Operations at Scale), REFERENCE (Sensor Commands, Detection & Response, Events, ID Schemes, Error Codes), and OPERATIONS. The main content area is titled "Slack" and describes outputting detections and audit (only) to a Slack community and channel. It lists two required variables: `slack_api_token` (the Slack provided API token used to authenticate) and `slack_channel` (the channel to output to in the community). An example configuration is shown in a dark box: `slack_api_token: d8vyd8yeugr387y8wgf8evfb` and `slack_channel: #detections`. Below this, the "Provisioning" section explains that to use this Output, you need to create a Slack App and Bot. It provides a 8-step guide: 1. Head over to <https://api.slack.com/apps>; 2. Click on "Create App" and select the workspace where it should go; 3. From the sidebar, click on OAuth & Permissions; 4. Go to the section "Bot Token Scope" and click "Add an OAuth Scope"; 5. Select the scope `chat:write`; 6. From the sidebar, click "Install App" and then "Install to Workspace"; 7. Copy token shown, this is the `slack_api_token` you need in LimaCharlie; 8. In your Slack workspace, go to the channel you want receive messages in and type the slash command: `/invite @limacharlie` (assuming the app name is `limacharlie`).



The screenshot shows the Slack API "Your Apps" page. On the left is a sidebar with links: Start learning, Authentication, Surfaces, Block Kit, Interactivity, Messaging, and APIs. The main content area is titled "Your Apps" and has a search bar "Filter apps by name or workspace". Below the search bar is a table with columns: App Name, Workspace, and Distribution Status. The table contains one entry: "Demo App" in the App Name column, "Lona Homelab SIEM" in the Workspace column, and "Not distributed" in the Distribution Status column. A green "Create New App" button is in the top right corner. At the bottom, there is a link: "Don't see an app you're looking for? Sign in to another workspace."

Now all that is left to do is to execute the **whoami** command on the virtual machine to check that we get an alert in Slack on the correct channel.

I am successfully alerted on both my desktop and mobile phone on the execution of a **whoami** command on my virtual machine, as seen in the images below.



app.slack.com/client/102AB3MQSQ4/C029Y5HNVHC

Search Lona Homelab SIEM

**Lona Homelab SIEM**

**Slack Connect** NEW

- Browse Slack
- Channels
  - # general
  - # personal-cybersecurity-research**
  - # random
  - + Add channels
- Direct messages
  - Lona mafaufau you
  - emfourfour
  - + Add teammates
- Apps
  - Demo App
  - + Add apps

**# personal-cybersecurity-research**

**Lona mafaufau** 9:15 PM  
joined #personal-cybersecurity-research.

**Lona mafaufau** 9:15 AM  
added an integration to this channel: [Demo App](#)

**Demo App** APP 9:18 AM  
was added to #personal-cybersecurity-research by Lona mafaufau.

**Demo App** APP 7:12 PM  
Detected **Local Accounts Discovery** on [MSEdgeWIN10.mshome.net](#):

Event:

```
{
  "cat": "Local Accounts Discovery",
  "source": "d1faf372-6c57-44bc-ac54-dfab75df576d.e0e6511b-b7ee-4a42-8f01-7ee81f9e4b03.df824c28-72c7-4908-b695-cc29786ea2b6.10000000.2",
  "routing": {
    "arch": 2,

```

[Show more](#)

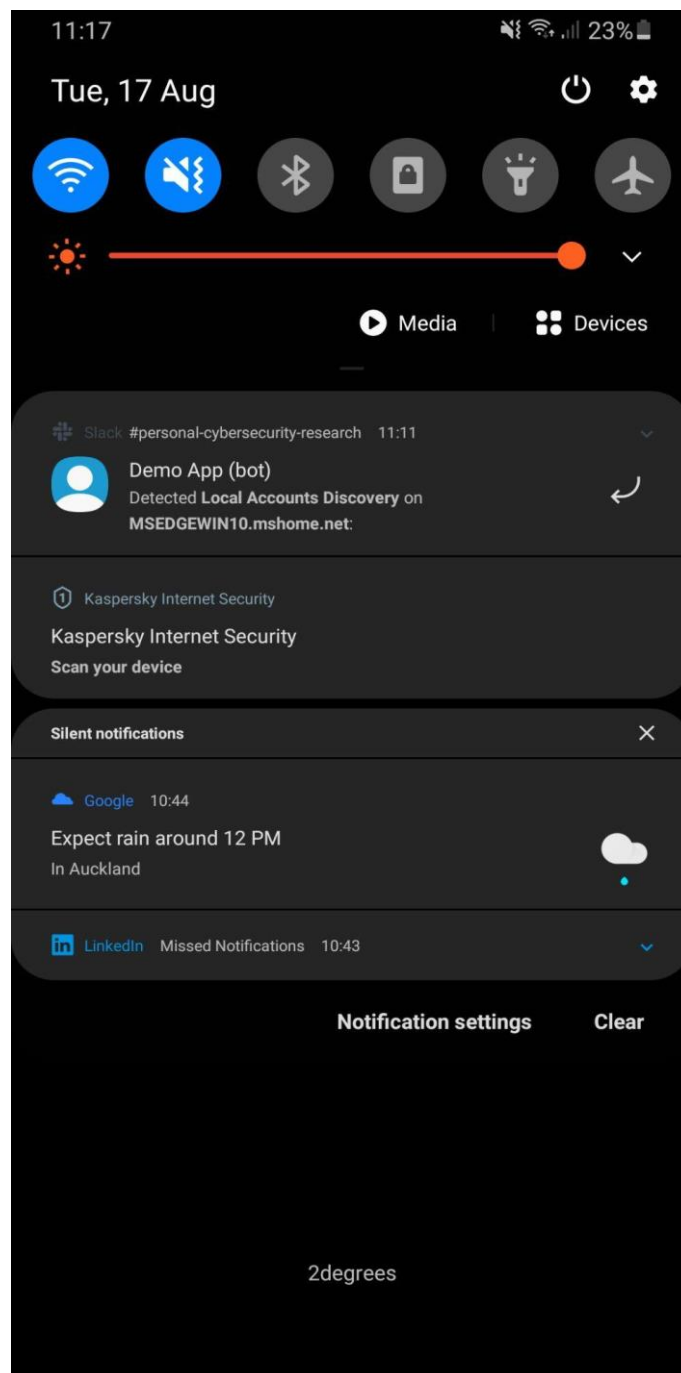
Detected **Whoami Execution** on [MSEdgeWIN10.mshome.net](#):

Event:

```
{
  "cat": "Whoami Execution",
  "source": "d1faf372-6c57-44bc-ac54-dfab75df576d.e0e6511b-b7ee-4a42-8f01-7ee81f9e4b03.df824c28-72c7-4908-b695-cc29786ea2b6.10000000.2",
  "routing": {
    "arch": 2,

```

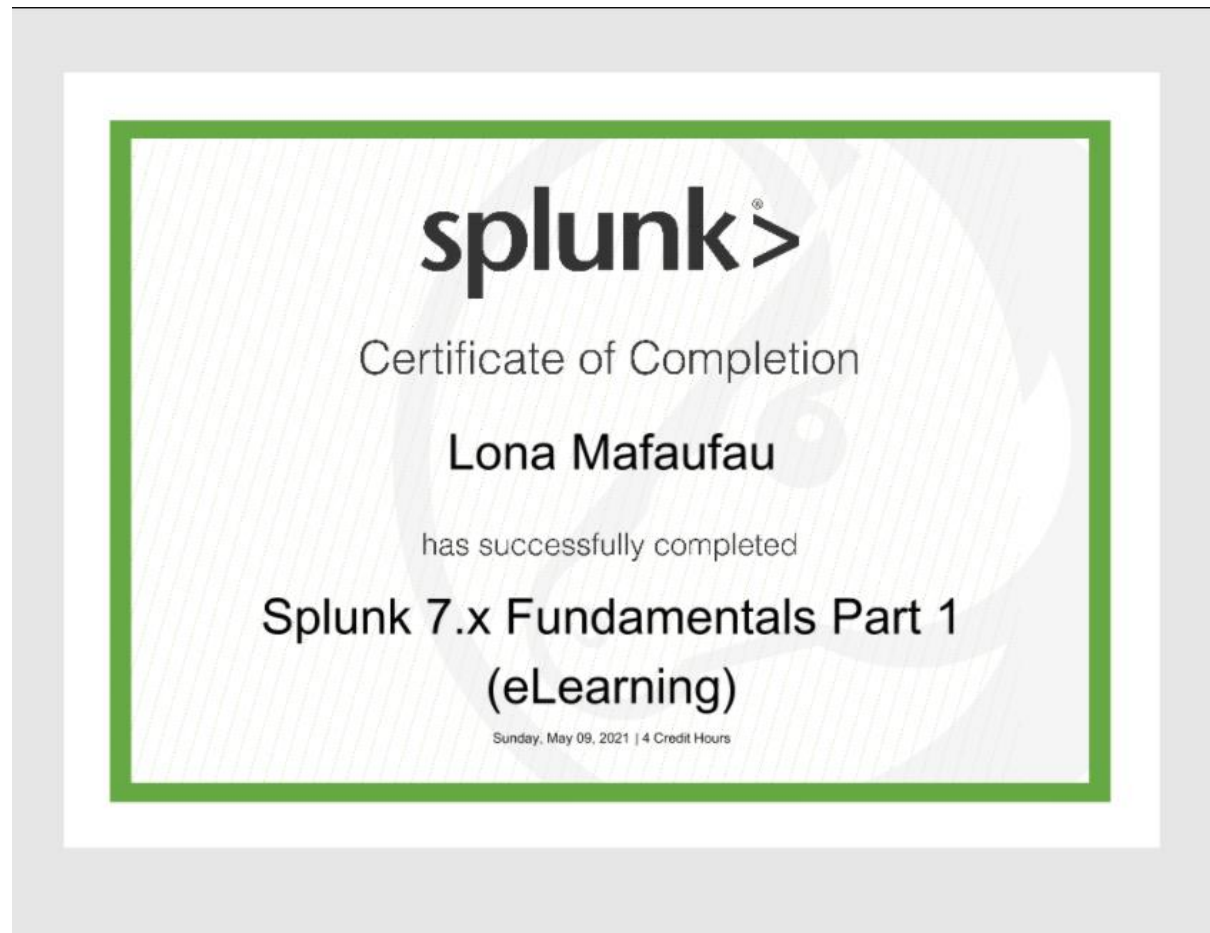
[Show more](#)



## Splunk Fundamentals Certificate of Completion

The link to view the official certificate can be found at the following link:

<https://education.splunk.com/award/completion/a2cde1a1-5d13-3b17-9901-8c2f97b6cf91/view-ext>

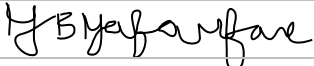


## ACKNOWLEDGEMENT AND APPROVAL

---


### Students Acknowledgment

The student acknowledged that all the information included in this document will not breach the confidentiality of the business and the business partner has been consulted about the contents

Student's Name	Signature	Date
Ma'alona Mafaufau		17/08/2021

### Industry Supervisor Approval

The approval indicates that the industry partner has confirmed that all the information included in this document will not breach the confidentiality of the business.

Name	Role	Signature	Date
Anirban Dey	Cybersecurity Operations and Intelligence Team Leader		27/08/2021