OSM Coursework 2

Security Report

Student ID: 2136685

Table of Contents

Table of Figures

Assumptions

1. Assuming that the insider is technically knowledgeable.
2. Assuming that the insider is present on the premises.
3. Assuming that the insider can access the client's physical resources.
4. For section 3, assuming that the client has an existing SIEM in place, as the brief states that "(…) deploying a **separate** solution for **insider** threat detection and automated response", implying that there is an existing solution for a more general use-case.
5. For section 3, assuming that attaching USB flash drives during out-of-office-hours is against the client's security policy, unless authorised to do so.
6. For section 3, assuming that the suspicious activity was unauthorised activity.
7. Assuming that the office has working CCTV cameras.
8. Assuming that the client operates in and from the United Kingdom and needs to comply only with the UK's legislation and regulations.

1. Detecting Reconnaissance

An insider is any one person that has authorised access to the client's resources. An insider threat is the potential risk that an insider may use their authorised access to harm the client. The threat can be unintentional – from negligence or accidental – or intentional – malicious (CISA, 2023; Imperva, 2019).

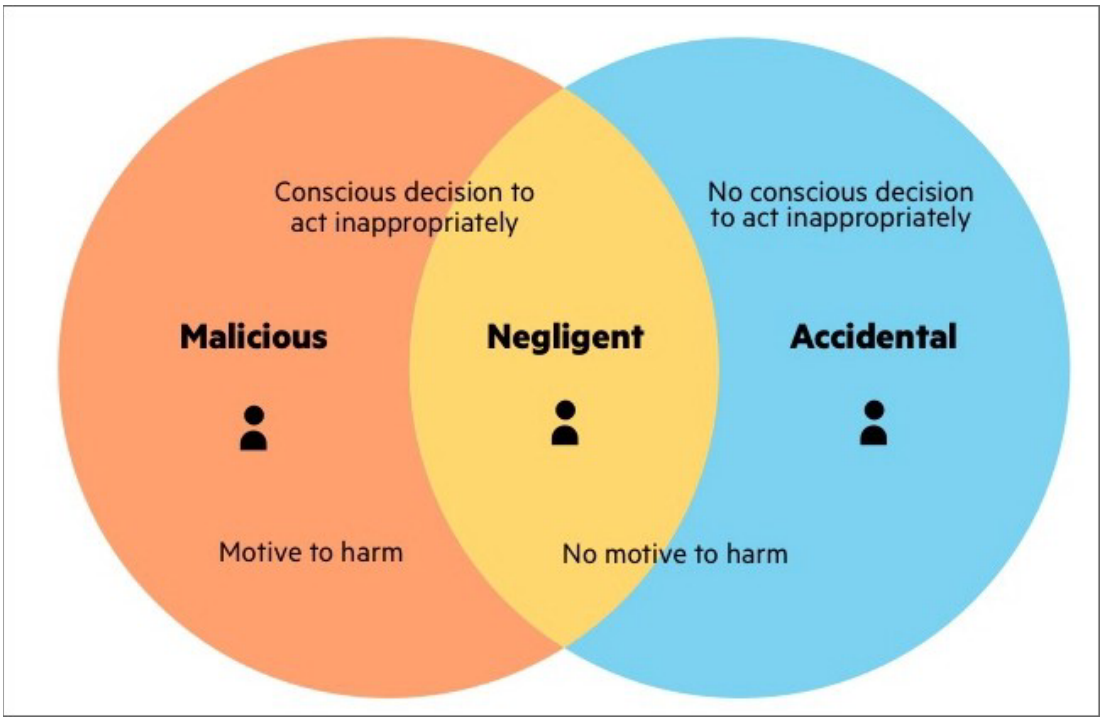

Figure 1: Types of Insider Threat (Imperva, 2019)

1.1 Insider Threat Reconnaissance

Before computers are involved, an insider can gather intelligence of the client's office space and physical resources. An insider may attempt to gather human intelligence by asking specific questions that may seem inconspicuous to an untrained employee. On the premises, the insider may be able to access important rooms that contain crucial resources, such as files or server rooms, through social engineering, or with their own access level, or a combination of both, posing a great threat to security.

On the network, an insider can gather information about the client by performing reconnaissance on the client's network to discover machines and create a network topology diagram, allowing an insider to choose the easiest and least noisy path towards a machine they want to sabotage. The insider can use well-known tools for network discovery such as nmap, or netdiscover for local discovery, if they are on-premises.

An insider can then gather information about the services on the machines using "*nmap -sV*". The command outputs the services and their respective versions that run on the machine, allowing an insider to check for vulnerabilities using a database such as CVE. The insider can exploit the vulnerabilities using a framework such as metasploit, which has a large range of exploits available.

1.2 Systematic Data Collection

A systematic approach for data collection can begin with:

1. **Collecting network traffic data:**
    - i.e. packet captures on routers immediately before a cluster of machines
    - Capturing packets on routers immediately before a subnet allows for easier analysis of malicious activity as other subnets' traffic does not conceal our desired traffic. Moreover, this ensures that the packet captures are grouped per subnet, making the traffic collected more homogeneous and easier to analyse.
    - Packet captures must be done on nodes 3, 4 and 5, as part of the server farms network captures.
    - On nodes 8 through 13, as part of the client nodes captures.
    - On nodes 14 and 15, as part of the office's wireless APs captures.
2. **Collecting device metrics:**
    - i.e. memory usage, CPU usage, network interface usage, disk usage
    - Collecting device metrics should be done on all machines.
    - The device metrics can help detect malicious activity, such as unusually large amounts of read/writes on a disk; unusually large CPU usage; unusually high network interface usage.
3. **Collecting security logs:**
    - i.e. authentication logs, firewall logs, privilege escalation logs
    - Collecting security logs must be done on all routers on the network, 0 through 15.
    - For example, if an insider wants to change the firewall on a router, the security logs will allow an incident responder to see when and who logged into the machine, when did they use privilege escalation to access the firewall, and when and where did they change the firewall rules.

4. **Collecting user activity logs**
    - i.e. user authentication logs, user session logs, file access logs, privilege escalation logs
    - Collecting user activity logs should be captured on all machines, routers, servers and user machines.
    - Collecting these logs allows an incident responder in detecting malicious activity, such as unauthorised access, suspicious out-of-office-hours activity.

1.3 Tools for Data Collection

The tools that can be used for collecting the data discussed in the section above are as follows:

1. **Collecting network data:**
    - For collecting the data, tcpdump, a command line tool that is resource efficient and can be configured to run in the background, making it suited for a simple, automated solution as a Unix service.
    - The packet captures can be analysed in Wireshark. Wireshark's analysis features, such as deep inspection, display filters and colour rules, help identify anomalies efficiently. Wireshark can be configured to capture packets based on filters, so the client can filter for a specific IP address, port or protocol (Wireshark, 2023).
    - Otherwise, the client may consider a comercial solution such as Cisco Secure Network Analytics. It employs real-time threat detection, allowing the client to improve unknown threat detection, insider threat detection, encrypted malware detection, policy violations and incident response and forensics (Cisco, 2024).
2. **Collecting device metrics:**
    - Collecting device metrics can be done using Nagios XI or Zabbix, however Nagios has a paid enterprise plan, as seen in Figure 3, whereas Zabbix is free and can be used for unlimited nodes, but their customer support is paid (Nagios, 2024; Zabbix, 2024a).
    - Zabbix has a public page of integrations and templates that shows how to integrate it with many other services, such as Elasticsearch or Splunk (Zabbix, 2024b).
    - Both can be configured to show all device metrics desired, such as CPU usage, memory usage and network interface usage and display them all in a convenient web UI.
3. **Collecting security logs:**
    - For collecting and centralising security logs, the client can implement either Splunk or Elastic Stack as their SIEM. These solutions will be analysed in depth in Chapter 2.

- Both solutions allow the client to create custom dashboards to place the most crucial information at the forefront, such as failed login attempts, security policy violations and unusual network traffic patterns.

4. **Collecting user activity logs:**
    - Logstash can be used to collect logs from user activity, just as collecting security logs, as Logstash is part of the Elastic Stack SIEM, therefore the SIEM solutions above can be configured to collect and analyse user activity logs as well.

1.4 The Problem of Scale

Due to the volume of the network network traffic, comprehensive data collection may not be feasible, especially as the network increases in scale. To overcome this problem, the client may reconsider what network traffic data they collect. Instead of collecting all traffic, the client may configure a filter to only collect specific packets, such as specific protocols, IP addresses or ports.

The client may consider prioritising important traffic, while deprioritising or excluding non-essential traffic. The client can implement a quality of service mechanism to create different traffic queues and give each a different priority. This ensures that high priority traffic does not get overlooked during high volume periods of traffic (EtherWAN, 2024; F5, 2023).

The client may consider reducing the dimensionality of the data by removing redundant or unimportant features, such as dropping duplicate packets, or dropping repeated protocol information within the same conversation. Moreover, non-essential metadata such as packet numbers, or interface identifiers can be dropped, however they may be important if, for example, a machine has multiple interfaces (Geeks for Geeks, 2020).

2. Splunk or Elastic Stack

Splunk and Elastic are reputable companies in the world of SIEMs. They offer highly robust SIEM solutions with Splunk Enterprise Security and Elastic Stack, although there are a few differences:

1. **Splunk:**
    - Splunk offers a powerful SIEM solution, as Splunk Enterprise Security, an addon to Splunk Enterprise, with advanced SIEM features (BlueVoyant, 2024; Shoard, Davies and Schneider, 2023).
    - Splunk ES offers real-time threat detection, pre-built detection rules for common security uses, threat intelligence integration, incident response workflows and compliance monintoring. These tools provide views that can be customised in the dashboard according to the client's needs. (BlueVoyant, 2024; Shoard, Davies and Schneider, 2023; Splunk, 2023a; Splunk, 2023b).

- The tools that Splunk ES provides on an initial setup allows the SIEM to be up and running very quickly, although trained expertise is required to set Splunk up. Moreover, the client must be able to retain the trained experts, as other organisations may make more attractive offers.
- Splunk ES can integrate with other tools to enhance the SIEM's capabilities, such as a SOAR for automated incident response workloads or a UEBA for identifying anomalous user behaviour and insider threats. Splunk offers both SOAR and UEBA solutions, making integration with Splunk ES less daunting (BlueVoyant, 2024; Shoard, Davies and Schneider, 2023; Splunk, 2023b).
- Splunk is popular due to its advanced search language, allowing for efficient data analysis. Moreover, Splunk delivers a friendly user experience and IT observability to non-security users, while providing advanced security operations to security teams, providing an enriched view of the client's environment (Shoard, Davies and Schneider, 2023).
- Splunk is offered using workload pricing or ingest pricing, whichever fits the client's needs best. However, there are also hidden costs in terms of data ingestion and storage, as Splunk pushes complete log collection. Moreover, the client must consider the prices of the Splunk addons as well (BlueVoyant, 2024; Shoard, Davies and Schneider, 2023).

2. **Elastic Stack:**
   - The Elastic (ELK) Stack, made of Elasticsearch, Logstash, Kibana and Beats can be configured to behave as a SIEM with similar features to Splunk ES, however ultimately, the ELK stack is a collection of separate tools. (Bunting, 2023; Miller, 2021; Shoard, Davies and Schneider, 2023).
   - The Elastic Stack is popular due to its high customisability, allowing the client to create preferential views of data for analysis. Moreover, it allows the client to choose the components they require, without having to pay for services they might not need (Shoard, Davies and Schneider, 2023; Tymoshyk, 2022)
   - The Elastic stack is attractive due to its initial low cost, although there are hidden costs, such as high costs of log ingestion and retention, and training and retention of experts. Moreover, configuration complexity and resource intensity of the stack may affect the overall performance and effectiveness of the workflow (Horovits, 2022).
   - For example, to ensure availability and scalability, the ELK stack must be able to handle sudden spikes in traffic, requiring a queueing system in front of Elasticsearch, such as Redis or Kafka, increasing complexity and configuration times (Horovits, 2022).

- Upgrading ELK stack is daunting, as upgrades may lead to Kibana breaking plugins and visualisations, sometimes needing complete code rewrites. Moreover, it may have problems communicating within components, like Kibana and Elasticsearch, slowing down the workflow (Horovits, 2022).
- The Elastic Stack used to be composed of open-source components, meaning that updates and new features may come more frequently and a professional user may change the code as they see fit. However, in 2021, the open source projects Elasticsearch and Kibana moved to a non-open-source dual license, questioning the benefits of running open-source. The client modifying the code may now pose a legal risk due to these licensing changes (Elastic, 2021; Horovits, 2022).

In conclusion:

- There are no more benefits to the ELK stack being open-source.
- The ELK stack requires additional expertise due to the separate configurations of the stack, whereas Splunk comes as a fully fledged solution and more easily integrates with additions.
- The ELK stack requires a larger downtime when upgrading or reconfiguring compared to Splunk.
- The prices of the SIEM solutions eventually balance out for reasons mentioned above, therefore the client should choose **the Splunk ES SIEM**.

3. Incident Response

Based on the advice from Sections 1 and 2, the data that needs to be collected is:

- Network traffic packet captures from gateways 10, 9 and 5.
- System logs from the identified machines connected to gateways 10, 9 and 5 (user authentication logs, USB Event logs, file access logs, process logs).
- Database server logs from the database server connected to gateway 5 (database authentication logs, database access logs).

Should the client need to use the data collected in the court of law, the evidence must be collected, preserved and examined in a forensically sound manner. The client must ensure the authenticity and integrity of the data collected as evidence by systematically applying an evidence acquisition process and filling out supporting information, to substantiate and authenticate the evidence.

The evidence that is expected to be derived from the analysis of the data above:

- **Evidence of unauthorised access during out-of-office hours:**
  - Evidence can be gathered to prove the unauthorised out-of-office-hours access by analysing the user authentication logs from the machine on gateway 10, to determine the account and as a result, the owner of the account.
- **Evidence of unauthorised external flash drive attachment:**
  - Evidence can be gathered by analysing the USB event logs on the machine on gateway 10, to verify what device was inserted, confirming the presence of an external flash drive.
- **Evidence of unauthorised data access:**
  - Evidence can be gathered by analysing the file access logs on the machine on gateway 9. Analysing the logs will tell the client what data has been accessed and potentially exfiltrated.
- **Evidence of unauthorised data exfiltration:**
  - Evidence can be gathered by analysing the network traffic packet captures from gateways 10, 9, and 5, as data from each machine may be exfiltrated. Moreover, it is important to analyse the traffic from gateway 10 in order to verify where the data would be exfiltrated to, as that is the machine that the insider is using.
- **Evidence of unauthorised database data access:**
  - Evidence can be gathered by analysing the database authentication and access logs on the database server on gateway 5. The logs will show the database user that the insider is connecting to the database service with and what database they accessed.
- **Evidence of unauthorised database data exfiltration:**
  - Evidence can be gathered by analysing the database access logs on the database server on gateway 5. The analysis of these logs will show if the insider accessed and exported any databases or tables.
- **Evidence of unauthorised database data modification:**
  - Evidence can be gathered by analysing the database access logs. The analysis of these logs will show if the insider has added, deleted or modified any tables on any database.

Additional data that may be collected:

- **Security alerts from SIEM:**
  - The security alerts can put into perspective the timeline of the insider breach, allowing for a more efficient analysis of the incident.

- **User Event and Behaviour Activity Data:**
    - Using a UEBA system enables machine-learning behaviour-based alerts, helping identify insider threats by discerning it from usual during-office hours activity.
- **Forensic image of identified workstation, the targeted file machine and the database server:**
    - Forensic images are saved states of machines right after an incident has occurred, allowing for a comprehensive and forensically sound analysis of the incident.
- Due to the physical nature of the breach, the client should collect **CCTV footage** from the internal cameras to analyse the physical access to the machine on gateway 10.

4. Advanced Persistent Threats (APTs)

To determine whether the solution proposed is appropriate, it must be tested against the use case. The solution should be tested by the same team that has implemented it, as they are trained experts and have the knowledge of the client's specific implemented layout. The following tests can be used to come to a conclusion:

1. **Functional testing:**
    - Functional testing entails testing the SIEM system in a way that verifies the functionality of the system, not the quality. The integration testing is to be done before the SIEM is live so as to ensure that the SIEM behaves within the specified requirements and meets the client's needs. One such test is integration testing, where it ensures that all the components, such as SOAR or UEBA modules work as intended with the SIEM. (Bose, 2021).
2. **Performance testing:**
    - Performance testing must be done before deploying the SIEM. Performance testing ensures that the SIEM system does not encounter any bottlenecks, for example from high periods of traffic. The system must be tested in multiple scenarios, from standby to high-load. Should data ingestion be bottlenecked, the system engineers must implement a data queueing system such as Kafka (Gillis, 2023).
3. **Red team exercises:**
    - After passing the above tests, the system engineers should simulate advanced persistent threats against the SIEM. Emulating real APTs can validate the effectiveness of the SIEM, or help identify gaps in the monitoring, detection and mitigation abilities of the SIEM, allowing the engineers to patch those gaps.

The threat intelligence, machine learning and UEBA components of the solution would be the ones tackling APTs. The client may observe APT behaviour such as additional suspicious out-of-hours activity, or detect certain indicators of compromise, such as file hashes of known malicious payloads which would be identified from documented IoCs; or behavioural analysis using the UEBA component, which specialises in detecting abnormal user behavior and can detect insider activity, such as unauthorised data access and lateral movement by analysing the detected unauthorised access. These APTs will be detected and the SIEM will allow an incident responder to take action directly from the platform, such as halting the affected machine (Exabeam, 2024).

5. Cost Effectiveness

Security investments for insider threat detection may seem redundant, expensive and inconvenient, especially so when the client already has a general SIEM system in place, however the benefits outweigh the drawbacks.

The overarching benefits in investing in additional equipment, human expertise and accepting temporary disruptions to the workflow, are that the client strengthens their security defences through employing or training employees to become highly-skilled incident responders which ensure fast acting mitigation against infiltration attempts by using the new SIEM systems to their full potential.

The equipment, such as the SIEM and any add-on modules such as a SOAR or UEBA, and storage for the logs collected, may incur a large portion of the costs, however they are crucial for the security of the client and their assets. Moreover, holding logs for the client's machines will aid in any security audits for international standards or data laws.

Allocating human resources to tasks such as manual configuration and upkeep of the new solution, monitoring operations, training and retaining of expertise may incur costs in terms of salaries, the actual training, and potentially creating a separate security department, however these expertise are crucially required to retain a smooth workflow and short downtimes.

There may be moments of inconvenience in terms of disruption to normal operations, such as downtime during system upgrades, security audits or perhaps even training session, however through these moments of temporary inconvenience, the client reposes in the fact that their assets are more strongly protected against insider threats, and that their trust and reputation is enhanced among customers, stakeholders and partners.

Moreover, these security improvements tighten the client's abidance to the legislations and regulations of the United Kingdom, ensuring that no data breaches would occur, as that would result in fines in sums larger than the security investments.

References

BlueVoyant (2024). *Splunk SIEM with Splunk Enterprise, Cloud, and Splunk ES*. [online] BlueVoyant. Available at: https://www.bluevoyant.com/knowledge-center/splunk-siem-with-splunk-enterprise-cloud-and-splunk-es [Accessed 10 Mar. 2024].

Bose, S. (2021). *Functional Testing : Definition, Types & Examples | BrowserStack*. [online] BrowserStack. Available at: https://www.browserstack.com/guide/functional-testing [Accessed 13 Mar. 2024].

Bunting, D. (2023). *Can You Use the ELK Stack as a SIEM? A Fresh Take*. [online] www.chaossearch.io. Available at: https://www.chaossearch.io/blog/elk-stack-siem [Accessed 10 Mar. 2024].

CISA (2023). *Defining Insider Threats*. [online] Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats [Accessed 5 Mar. 2024].

Cisco (2024). *Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet*. [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.html [Accessed 9 Mar. 2024].

Elastic (2021). *FAQ on 2021 License Change*. [online] www.elastic.co. Available at: https://www.elastic.co/pricing/faq/licensing [Accessed 10 Mar. 2024].

EtherWAN (2024). *Implementing Quality of Service for Prioritizing Network Traffic | EtherWAN*. [online] EtherWAN.com. Available at: https://www.etherwan.com/support/featured-articles/implementing-quality-service-prioritizing-network-traffic [Accessed 9 Mar. 2024].

Exabeam (2024). *What Is UEBA (User and Entity Behavior Analytics)?* [online] Exabeam. Available at: https://www.exabeam.com/explainers/ueba/what-ueba-stands-for-and-a-5-minute-ueba-primer/ [Accessed 13 Mar. 2024].

F5 (2023). *Overview: Traffic prioritization using quality of service (QoS)*. [online] techdocs.f5.com. Available at: https://techdocs.f5.com/en-us/velos-1-2-0/velos-systems-prioritizing-traffic-qos/overview-traffic-prioritization.html [Accessed 9 Mar. 2024].

Geeks for Geeks (2020). *Data Reduction in Data Mining*. [online] Geeks for Geeks. Available at: https://www.geeksforgeeks.org/data-reduction-in-data-mining/ [Accessed 9 Mar. 2024].

Gillis, A.S. (2023). *What is Performance Testing?* [online] SearchSoftwareQuality. Available at: https://www.techtarget.com/searchsoftwarequality/definition/performance-testing [Accessed 13 Mar. 2024].

Horovits, D. (2022). *Elk Stack Cost & Pricing (Time & Money)*. [online] Logz.io. Available at: https://logz.io/blog/the-cost-of-doing-elk-stack-on-your-own/ [Accessed 10 Mar. 2024].

Imperva (2019). *What Is an Insider Threat | Malicious Insider Attack Examples | Imperva*. [online] Learning Center. Available at: https://www.imperva.com/learn/application-security/insider-threats/ [Accessed 5 Mar. 2024].

Miller, J. (2021). *Is Elastic Stack (ELK) the Best SIEM Tool? | BitLyft Cybersecurity*. [online] www.bitlyft.com. Available at: https://www.bitlyft.com/resources/is-elastic-stack-elk-the-best-siem-tool [Accessed 10 Mar. 2024].

Nagios (2024). *Nagios XI - Easy Network, Server Monitoring and Alerting*. [online] Nagios. Available at: https://www.nagios.com/products/nagios-xi/ [Accessed 9 Mar. 2024].

Shoard, P., Davies, A. and Schneider, M. (2023). *Magic Quadrant for Security Information and Event Management*. [online] Gartner.com. Available at: https://www.gartner.com/doc/reprints?id=1-2BDC4CDW&ct=221010&st=sb [Accessed 10 Mar. 2024].

Splunk (2023a). *Splunk Enterprise*. [online] Splunk. Available at: https://www.splunk.com/en_us/products/splunk-enterprise.html [Accessed 11 Mar. 2024].

Splunk (2023b). *Splunk Enterprise Security SIEM*. [online] Splunk. Available at: https://www.splunk.com/en_us/products/enterprise-security.html.

Tymoshyk, N. (2022). *Splunk ES vs. Elastic (ELK) Stack: Comparison from the SOC Analyst*. [online] UnderDefense. Available at: https://underdefense.com/blog/splunk-es-vs-elastic-elk-stack-comparison-from-the-soc-analyst/ [Accessed 10 Mar. 2024].

Wireshark (2023). *Wireshark · About*. [online] www.wireshark.org. Available at: https://www.wireshark.org/about.html [Accessed 9 Mar. 2024].

Zabbix (2024a). *Technical Support Subscriptions - Zabbix*. [online] www.zabbix.com. Available at: https://www.zabbix.com/support [Accessed 9 Mar. 2024].

Zabbix (2024b). *Zabbix Integrations and Templates*. [online] www.zabbix.com. Available at: https://www.zabbix.com/integrations [Accessed 9 Mar. 2024].

Appendix

A.1 Figures

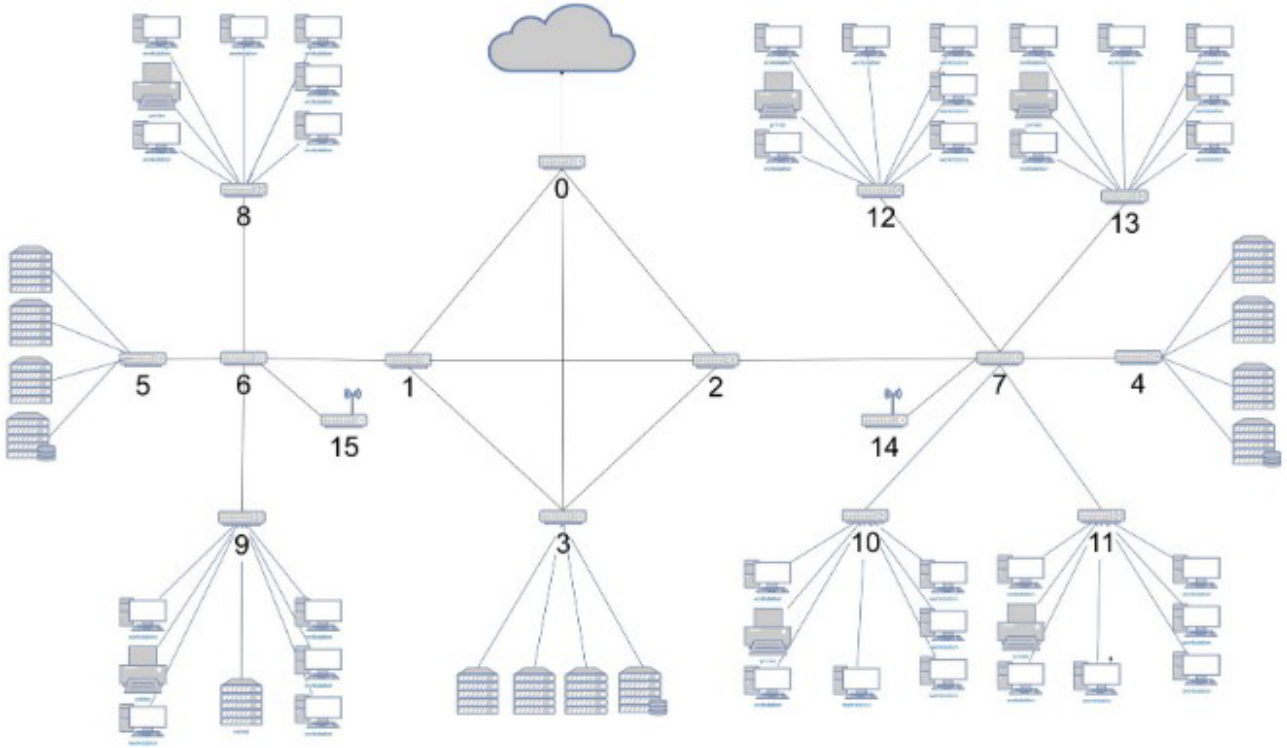

Figure 2: The Client's Network Topology Diagram

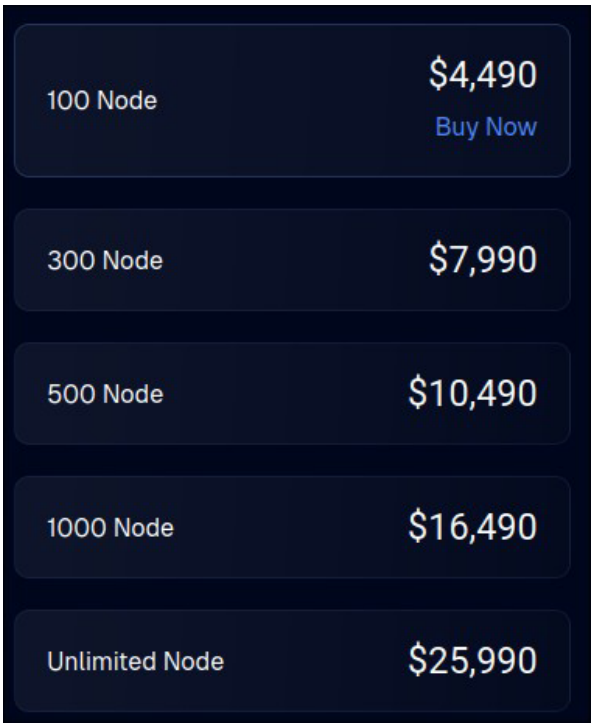

Figure 3: Nagios Enterprise Paid Plans