Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	**U2136249**

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	Tuesday 16th January 2024
Submission date (excluding extensions)	Friday 15th March 2024
Submission guidance	Tabula link
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

Module title & code	Operational Security Management (WM3B4)
Module owner	Christo Panchev
Module tutor	Christo Panchev
Assessment type	Coursework 2
Weighting of mark	60%

Word count	Total word count is 2800. There is a limit set for each question (see below) You will not be penalised for producing under length work, provided quality is not sacrificed to brevity. Learning to write to a limit is one of the skills the degree is designed to encourage you to cultivate.		
Does the word count allow +10%? **Select ONE**	Does the word count include tables? **Select ONE**	Does the word count include references? **Select ONE**	Does the word count include appendices? **Select ONE**
Yes	Yes	No	No
If appendices are included, will they be marked? No			

Submission format	PDF

Module learning outcomes (numbered)	• Anticipate cyber behaviors, both deliberately adversarial and unintentionally inept, that would undermine an organization's viability. • Critically evaluate the vulnerabilities of an organization through active probing of its systems. • Manage cyber resources to maintain an organization's viability in the face of adversarial or unintentional threats.
Learning outcomes assessed in this assessment (numbered)	As above
Marking guidelines	Generally indicated within specification
Academic guidance resources	You will have an opportunity to ask questions and get support on the assessment after it has been handed to you. You will be supported in this assessment through: 1. A special Moodle forum. 2. Through emails directed to the module tutor. **Notes to students:** If support is provided on a Teams Channel or a Moodle forum, please ensure you check previous questions posted on the channel. The Teams/Moodle channel will typically be closed one week before the submission date and no new questions will be addressed, please organise your time accordingly. Please be patient with module tutors. Please turn on your Teams Channel/Moodle notifications. If a tutor has not responded to a query within 5 working days, please email the module tutor.
Special instructions	Do not include the PMA specification in the submission. **Spelling/grammar.** Ensure that you spell check the submission, use a grammar checker and ensure that you proofread your work prior to submission. Spell/grammar checkers must be set to UK English, do not use 'Americanised' spellings. **References.** References are to be included at the end of the report (or do you want footnotes?) using the Harvard referencing system. You should not include a bibliography. Each reference must be connected to a citation within the main body of the report. Do not attempt to hide text within JPEGs, this will be construed as an attempt to mislead the assessor. **Coherence**. A poorly worded report will hide excellent content. The narrative should be easy to read, and arguments should be presented coherently and convincingly. **Presentation.** At this stage in your studies, there is no excuse for poor presentation. You will not receive marks for presentation; however, your submission will be penalised for poor presentation. **Formatting**. All figures and tables must be properly labelled and captioned. All pages must be numbered. Formatting must be consistently applied throughout the submission. Submissions that stray from this guidance may be penalised.

Contents

Assumptions

1. Throughout this document, an insider threat is defined as a malicious threat actor with intention to cause harm to the organisation for personal benefit or to act on a personal grievance, rather than non-malicious type, including negligent users, accidental mistake instances, or outsmarted users (CISA, 2023).

Q.1 Detecting Reconnaissance:

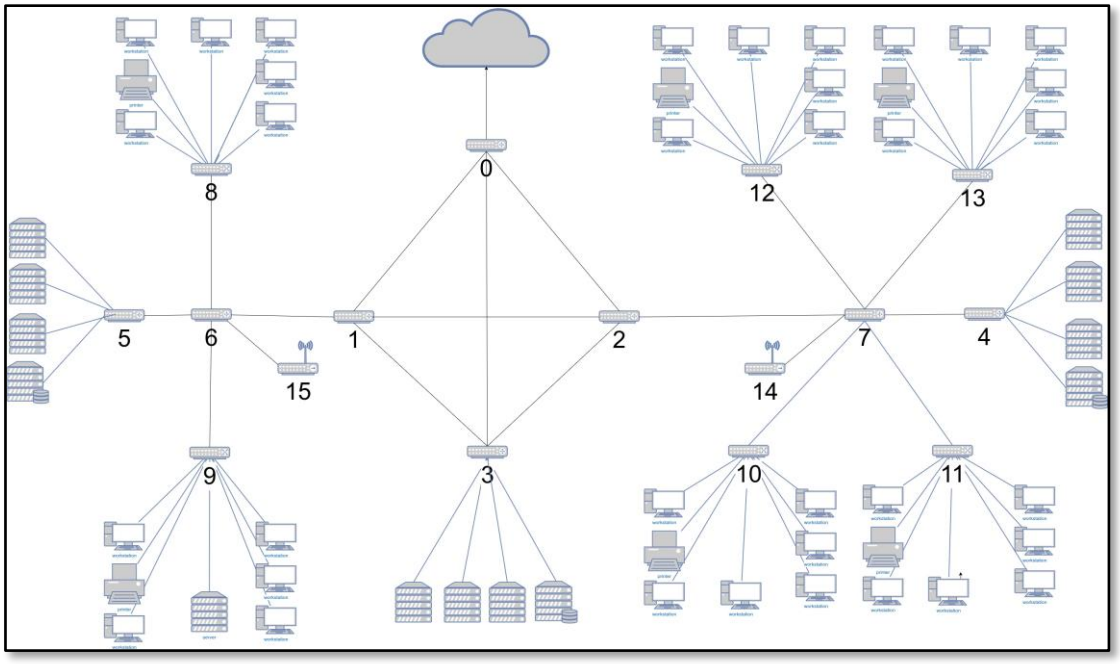


Figure 1 – Organisation's Network Infrastructure

Threat actors often follow a structured pattern to carry an attack (Stolfo et al., 2008), often following the Cyber Kill Chain Framework, which delineates the stages of an attack, including reconnaissance (Lockheed Martin, 2023). Insider threats have a distinct advantage compared to other threat actors, due to their legitimate access, permissions, and network knowledge (Liu et al., 2018). They can utilise the following techniques to cause potential damage to the organisation:

1. **Network Mapping**: map network topology, discover active hosts, ports, firewalls, and routing paths within the network infrastructure (MITRE, 2020b). These actions can reveal critical assets, e.g. database servers.

2. **Vulnerability Scanning**: use tools such as Nessus, to probe systems, compare software versions against extensive databases of known exploits. Proving the attacker vulnerable targets and maximize their chance of success (MITRE, 2020a).

3. **Port Scanning**: systematically probe target systems, revealing open ports and associated services accepting connections. This can allow the attacker to identify misconfigured services for potential initial access or pivot points for lateral movement (MITRE, 2020a).

4. **Service Enumeration**: probe open ports to fingerprint operating systems, internal application and identify their exact version. This enables the attacker to identify outdated or unpatched software giving the attack potential targets to exploit (MITRE, 2020a).

Figure 2, follows the Cyber Kill Chain attack methodology to demonstrate a systematic monitoring approach to prevent, contain, and eradicate potential insider threat reconnaissance activity within the organisation's network infrastructure, as shown in Figure 1. This approach establishes data collection points at strategic locations throughout the firm's network to detect the insider threat techniques outlined above.

Kill Chain	Collection Point	Insider Threat Activity
Reconnaissance	Gateway (Node 0)	• Outbound traffic (E.g. to file sharing platforms) • Establish remote connections. • Out-of-hours activity. • Remote activity (E.g. VPN)
	Access Points (AP) (Nodes 14, 15)	• Network scans to / from AP (internal network mapping). • Increased network traffic volumes or changes in protocol usage from devices on the AP. • Extensive use of network enumeration tools (E.g. Nmap)
Weaponisation	Core Switches (Nodes 1, 2, 6, 7)	• Suspicious process spawns on core switches (unlikely in normal operation) • Attempts to manipulate routing tables or firewall rules. • Configuration changes to network devices (E.g. From typical user).
Delivery	Client Workstations (Nodes 8, 9, 10, 11, 12, 13)	• File transfers or data staging activities. • Access or modification of systems or data (E.g. Outside of the user's area of responsibility or regular working hours). • Use of unauthorised devices (USB drives). • Deployment of unknown software.
Exploit	Client Workstations (Nodes 8, 9, 10, 11, 12, 13)	• Processes running with elevated privileges. • Unexpected access to other user accounts or systems. • Anomalous system / hardware resource usage (CPU, memory, network bandwidth)
Install	Client Workstations (Nodes 8, 9, 10, 11, 12, 13)	• Manipulation of legitimate tools (E.g. PowerShell) • Modifications of system settings, scheduled tasks, or registry entries • Creation of hidden user accounts.
Command & Control	Gateway (Node 0)	• Outbound connections to atypical protocols. • Increased outbound traffic volume or data obfuscation attempts. • Use of remote access tools (E.g. SSH) inside the network.
Actions on Objectives	Critical Servers (Nodes 3, 4, 5)	• Unauthorised access to sensitive files / databases (E.g. outside of typical usage). • Large data transfers. • Attempted deletion of logs or system files.

Figure 2 - Systematic Approach to Detect Insider Threat Reconnaissance Activity

To turn this strategy into practice, Figure 3 illustrates the tools and their respective configurations that the organisation can adopt to efficiently collect data, log activity, analyse data for detecting insider threat activity.

Tools	Configuration Guidance
Network Traffic Analysis (NTA): • **Open source: Suricata, Zeek** • **Commercial: StealthWatch SolarWinds, NPM**	• **Signature Development:** Define & maintain custom signatures on internal network, services running, and known vulnerabilities. • **Baseline Creation:** Establish and monitor baselines to analyse "normal" network traffic patterns over time such as protocol distribution, IP source/destination patterns, and typical bandwidth usage. (E.g. Port Scanning rules to detect excessive probes to a single host) • **DPI Configuration:** Enable DPI on critical network segments, (E.g. Examine payload content for protocol anomalies and sensitive data keywords).
Security Information and Event Management (SIEM): • **Splunk,** • **IMB QRadar** • **Elastic Stack**	• **Log Source Integration:** Specify log formats for various devices are parsed correctly (E.g. timestamp, user identifiers, event types). • **Normalisation:** Map similar event types from different devices to common fields names for consistent correlation. • **Threat Intelligence Feed Configuration:** Define connections to threat intelligence providers (E.g. CrowdStrike), indicating the types of data to ingest (IP reputation, malware hashes, attack patterns) to facilitate a threat analysis across the network. • **Correlation Rule Development:** Write rules using SIEM query language, such as: Multiple failed logins from IP X Followed by successful login AND access to resource Y within Z minutes, to enhance detection accuracy.
Deception Techniques (Honepots): • **Honeyd**	• **Honeypot Service Configuration:** Mimic common services (E.g. SMB, RDP, SSH, HTTP) with vulnerable configurations or software versions to detect attack scanning and exploitation attempts. • **Logging and Monitoring:** Configure logging on honeypot with alerts sent to the SIEM upon any interaction, proving high-level insights into attacker's methods. • **Strategy:** Place honeypots alongside legitimate assets (less critical) to increase attractiveness to reconnaissance.
User Behaviour Analytics (UBA): • **Exabeam,** • **Gurucul,** • **Securonix**	• **Baseline Scope:** Define baseline periods (Daily, weekly patterns) and the granularity needed (individual users vs groups). • **Data Source Selection:** Prioritise logs indicating logins, resource access, file transfers, application use, device geolocation. • **Risk Model Specification:** Use the UBA interface to weight the importance of different behaviours and assign conditions for triggering high-risk alerts.

Figure 3 - Tools & Configuration to Detect Insider Threat Activity

Monitoring a high-volume network presents key challenges for detecting insider threat such as invisibility in the network, attacker's knowledge of systems, and regular routines (Saxena et al., 2020). To address the problem of scale, the following strategies focusing on strategic data collection, efficient analysis, and optimisation should be applied:

1. **Strategic Network Segmentation**: divide client network into logical segments based on sensitivity levels, user groups and service type. By segmenting the network, it limits the scope of reconnaissance within a segment and reduces the overall volume of data requiring in-depth analysis. Enforcing segmentation using firewalls and access control lists (ACLs) to filter traffic and define strict communication rules between zones.

2. **Prioritised and Target Capture**: Instead of attempting to collect traffic from the entire network, target critical subnets (Nodes: 3, 4, 5, 9), using network prioritising techniques such as bandwidth throttling and traffic shaping to manage network resources more efficiently by targeting sensitive servers and user client groups with elevated risk profiles (Dilmegani, 2023). Implement pre-filtering on network devices using ACLs to capture only traffic matching patterns relevant to potential reconnaissance activity (e.g. port scans, unusual protocols). Leverage low-based analysis tools (E.g. NetFlow) to gain insight from network metadata without full packet capture (AWS, 2020).

3. **Caching and QoS Policies:** Employ content caching servers for frequently accessed data to reduce the load on internal servers and the network traffic. Implement Quality of Service (QoS) policies to prioritise traffic related to critical services and security monitoring tools, ensuring that reconnaissance detection is not hindered during peak times.

4. **Zero-Trust Implementation:** Adapt zero-trust principles to reduce the attack surface. Revoke implicit trust between network segments, requiring continuous authentication and authorisation (NCSC, 2021). Combined with granular ACL policies, will limit the scope for internal reconnaissance and lateral movement.

Q.2 Detecting Reconnaissance:

Figure 4 showcases the main capabilities differences between Splunk and Elastic Stack for detecting insider threat detection and automated response.

Feature	Splunk (Proprietary)	Elastic Stack (Open-Source)
Data Ingestion	• Supports semi-structured or unstructured of machine data in various formats incl. XML, JSON, CSV, TSV • Provides a centralised easy to use and user-friendly interface to correlate data logs into behaviour patterns. (Splunk, 2021)	• Excellent at ingesting large volumes of structured unstructured machine data sources incl. application, web servers and OS logs. • Capabilities can be extended through plugins and custom parsers for non-standard log formats.
Data Handling	• Offers normalisation from multiple data sources into a single data schema for intelligence management, by removing outdated or incorrect elements, ensuring consistent data representation, and making search and correlation very effective. (Splunk, 2023)	• Uses a schema-on-read approach – it stores data in JSON format. Provides flexibility for diverse data types but sacrifice on search performance compared to Splunk's pre-defined schemas.
Data Indexing	• Integrates search processing language (SPL), allowing complex queries to extract data from ingested logs, facilitating efficient threat hunting and investigation. (Splunk, 2017)	• Built using Kibana Query Language (KQL), offering similar SQL syntax, facilitating faster adoption and query building.
Insider Threat Detection	• Uses statistical analysis leveraging machine learning to identify deviation from establish baselines – vital to detect changes in user behaviour. • Provides pre-built UBA features for risk scoring based on user, entity, and behaviour (UEBA) analysis – allows prioritisation of suspicious events.	• KQL query language integration allows the creation of complex queries to search for specific user activities, anomalous data access patterns, or deviations from establish baselines. • UBA features can be integrated using advanced configuration to provide risk scoring and user behaviour analysis.
Threat Intelligence Integration	• Out-of-the box threat intelligence feeds to enrich investigations with contextual data on known threats and indicators of compromise (IOCs).	• Needs to be manually configured to support threat intelligence feeds, requires specialise knowledge to set-up.
Automated Response (SOAR)	• Phantom Integration: offers incident response orchestration, case management, and playbook automation to streamline investigation and containment workflows specific for insider threats. • Allows for third-party tools to extend existing capabilities for blocking accounts and isolating devices.	• Open-source options (E.g. TheHive, Cortex) can be integrated to provide varying levels of configuration automation for detecting insider threat behaviours.

Figure 4 - Splunk Vs Elastic Stack

Q.3 Incident Response:

The human factor is the weakest link in cybersecurity (Schneier, 2000), with insider threats responsible for over two-thirds of cyber-attacks (Verizon, 2023). Therefore, the organisation must monitor their environments for suspicious activity carried out by employees, contractors, and partners, and correlate the data into behavioural patterns to prevent data and financial loss in a timely manner (Ernst & Young, 2020). The challenge is that insiders act within the organisation or have legitimate access to the environment, making rule-base systems and alerts ineffective for detecting malicious behaviour (Liu et al., 2018). The solution is to implement a SIEM to collect data from normal users, devices, systems, and privilege accounts to identify anomalies in behaviour and flag potential malicious activity (CISA, 2020).

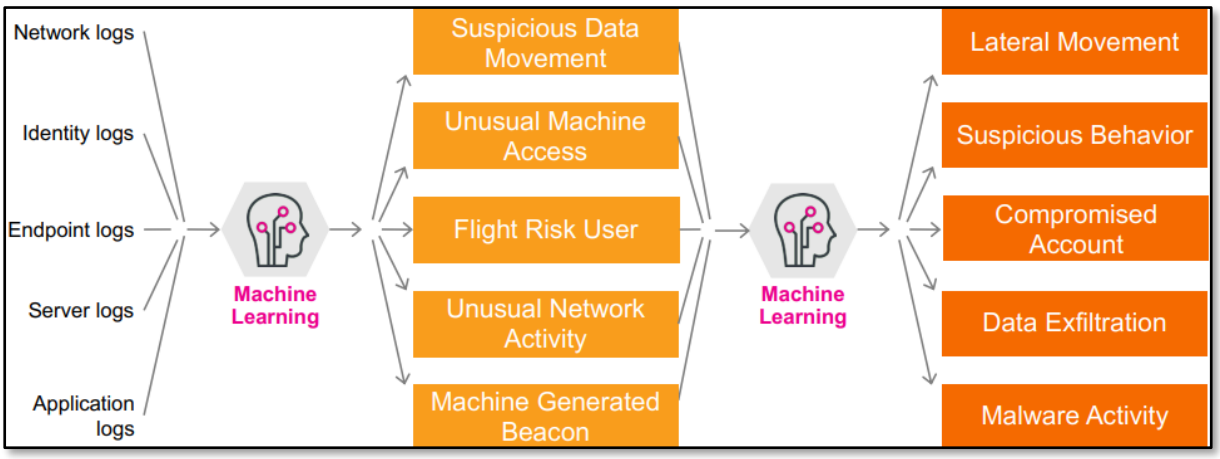


Figure 5 - Splunk's use of ML to detect Insider Threat

By analysing relevant data from Gateway 5, 9, and 10, as specified in Figure 2, Splunk can be used to correlate network and endpoint log data to detect: valid account abuse, privilege escalation, data exfiltration, unusual activity, and credential compromise using machine learning, as illustrated in Figure 5. Additionally, it can store this information a forensically sound manner (McKemmish, 2008), following legislation guidelines such as GDPR.

Using Splunk SPL, network traffic can be filtered by out-of-hours timestamps (See Appendix I for a list of specific syntax), focusing on the workstation, file server and database server to look for:

Gateway	Event Type	Expected Evidence
Workstations (Node 10)	Log Timestamps	• Collect network and login timestamps during out-of-hours timeframe
	Network Traffic	• Analyse traffic to / from suspicious workstation (atypical use of normal user) for: • unusual protocol or ports to indicate data exfiltrate attempts or abuse of valid account privileges. • Increased outbound traffic volume potentially indicating data transfers. • Remote access tools usage (E.g. SSH).
	Process Execution	• Destination IP addresses, ports used, and protocols involved in network communications. • Unusual data transfer volumes and timestamps compared to baseline network traffic. • Connections to known malicious domains or IP

		addresses. • Exfiltration attempts identified by analysing transferred data types and volumes.
	USB Device Usage	• OS Logs: Timestamps of USB device connection / disconnection (Device and User ID). • Filenames accessed on the media device. • File read / write operations associated with the USB device.
File Server (Node 9)	Network connection logs	• Destination IP addresses, ports used, and protocols involved in network communications (E.g. FTP, SMB), indicating data exfiltration. • Unusual data transfer volumes and timestamps compared to baseline network traffic. • Connections to known malicious domains or IP addresses. • Exfiltration attempts identified by analysing transferred data types and volumes.
	System & Security Logs	• Login Events with timestamps: including IP source (local/remote) • Successful / Failed attempts, and account used. • Detailed breakdown of user activity outside of normal working hours • Failed logins attempts exceeding a threshold (potential brute-force attack).
Database (Node 5)	Application logs	• Error messages related to unexpected application crashes or permission issues. • Entries indicating access to unauthorised applications or tools. • Logs with timestamps showing unusual application activity during outside of normal working hours.

Splunk's Advanced User Behaviour Analytics (UBA) have pre-built models which can alert on deviations from normal user behaviour (Node 10). These models are trained on historical user and entity behaviour data. The organisation should couple the data collected from Figure 2 and apply the following UBA models to efficiently mitigate insider threats:

- **Abnormal User Login**: aimed to identify unusual login attempts, such as from unexpected locations or times, failed login attempts exceeding average threshold, or logins from a dormant account. In this case, the out-of-hours login activity on the workstation would trigger an alert for further investigation [citation].
- **Unusual File Access / Transfers**: aimed to detect atypical file access patterns such as accessing a large volume of files in a short period, accessing sensitive files outside normal working hours, or accessing files from unauthorised location. This model can be used to flag unusual activity on the file server (Node 9).
- **Lateral Movement Detection**: aimed to identify suspicious attempts to move laterally within the network, such as accessing resources that a user does not normally access or pivoting from compromised accounts to other systems. If the threat actor used the compromised workstation (Node 10) to access the database server (Gateway 5) UBA could detect this activity as an anomaly.

Q.4 Advanced persistent threats (APTs):

Figure 6 details the APTs tactics, techniques, and procedures by following the MITRE ATT&CK Framework, and the corresponding Splunk's test configuration needed to detect insider threats, which must be carried out by the SOC team. (See Appendix II for a complete MITRE ATT&CK coverage).

Insider Threat TTPs	Splunk's Detection Mechanisms	SOC Testing & Configuration
Initial Access		**Functional Testing**
External Remote Services (T1133) **Trusted Relationship (T1078)**	• Monitor inbound traffic (E.g. SSH, FTP). • Track source IP addresses, connection duration, and data volume. • Identify connections from unusual location / outside of expected work hours. • Search unexpected remote service activity (E.g. spawned privileged processes) • Login event to identify successful / failed attempts (E.g. from unusual user) • Detect atypical login for specific users (non-working hours, unusual locations)	• Verify correct log ingestion (network traffic, endpoint, and application logs). • Test parsing accuracy against a variety of log formats (structured, semi-structured) • Evaluate Splunk's indexing speed, search query performance, and efficient execution of complex correlation rules. • Analyse query execution times for optimisation (E.g. Complex SPL searches)
Execution & Persistence		**Baselines & Thresholds**
Account Manipulation (T1098) **Create Account (T1546)** **Event Triggered Execution (T1133)**	• Monitor account creations, modifications, or deletions • Track process execution for administrative tools (E.g. PowerShell). • Detect Process spawns with unusual command-line arguments actions by regular users. • Alert on scheduled task creation / manipulation.	• Validate pre-define baselines for normal network traffic patterns, user login activity, application usage behaviour, and device activity (E.g. CPU, memory, disk). • Creating separate baselines for different network segments (E.g. Nodes: 5), user groups (E.g. Administrators), or time periods (E.g. Normal office hours Vs Out-office-hours).
Privilege Escalation & lateral Movement		**Detection Rules**
Abuse Elevation Control Mechanism (T1548) **Event triggered Execution (T1546)** **Exploitation of Remote Services (T1210)**	• Track processes initiated with elevated privileges or escalation attempts from modified accounts. • Look for tools known for privilege exploitation (E.g. Mimikatz) • Identify logins using elevated privileges outside typical patterns for the user, or access attempts to unusual	• Generate simulated attack patterns (E.g. Atomic-Red-Team Tool). • Inject activity samples across normal user activity, system updates and configuration changes. • Verify detection rules to identify true positives while minimizing false results. • Refine alerts, thresholds, and correlation logic based on test outcomes.

Data Exfiltration & Impact		Performance & Scalability
Exfiltration over network (T1011) **Data Destruction (T1485)** **Data Manipulation (T1565)** **Financial Theft (T1657)** **System Shutdown / Reboot (T1529)**	• Monitor outbound traffic (E.g. FTP, destination IP ranges, data volumes, and unusual port usage). • Alert on potentially obfuscated traffic, large, unexpected file transfers, DNS tunnelling attempts. • File operations from media devices (E.g. compression, encryption, or deletion) • Analyse logs and alerts indicating unexpected changes in file integrity, registry, deletion of critical data (E.g. attempts to disable backup systems) • Prevent full disk wipe activities.	• Simulate data volumes ranging from expected average loads to peak scenarios. • Monitor system performance metrics such as response times, resource utilisation (E.g. Disk I/O). • Conduct failure tests: simulate component crashes, network outages, or unexpected data bursts. • Evaluate the system's redundancy, automatic failover mechanisms, graceful degradation, and ability to recover from disruptions.

Figure 6 - APTs TTPs & Splunk's Monitoring Configuration

Q.5 Cost Effectiveness:

Figure 7 illustrates the equipment, human resources and inconvenient trade-offs and justifications for implementing security monitoring for detecting insider threats.

Cost Category	Description	Benefits
Equipment	Involves hardware, software, and training. Hardware includes buying or outsourcing servers for log storage, analysis, and virtualisation needs. Software costs include licensing for the SIEM (E.g. Splunk) and threat intelligence subscriptions.	• **Centralised Visibility**: having an SIEM such as Slunk provides a single platform to view logs and network data. • **Proactive Threat Identification**: enables historical log analysis, anomaly detection through threat intelligence subscriptions to reveal common and novel threats. • **Efficient Response**: Integrated tools and trained analysts allow for fast incident investigation and containment.
Human Resources	Security operations requires skilled personnel for initial setup, tailoring of detection rules, system maintenance and threat monitoring. This involves hiring new staff or upskilling existing employees and provide ongoing training to staying updated on threats, tools (E.g. Splunk) and attack techniques.	• **Proactive Defence:** Configure and optimise detections and prioritise threats. • **Risk Reduction:** having skilled staff provides expertise to anticipate vulnerabilities and hardening defence. • **Long-term Capability**: builds in-house security skills and awarenesses for future incident preparedness.
Inconvenience	Implementation and downtime for maintained might cause temporary business disruption. Enhanced security controls may also add minor overhead to user workflows (E.g. 2FA), impacting productivity until users adapt. Furthermore, industry regulations can impose extra compliance burdens, reporting requirements and audit overhead.	• **Minimised Outages:** proactive threat mitigation prevents major disruptions caused by breaches. • **Reputation & Trust:** Strong security protects customer data, enhances business reputation. • **Compliance Enablement:** simplifies meeting regulatory mandates and avoids potential penalties.

Figure 7 - Human, Equipment & Inconvenience Trade-offs for Security Monitoring

I. Appendix

Splunk's SPL Query Syntax (Splunk, 2023):

Common Search Commands	
Command	**Description**
chart/ timechart	Returns results in a tabular output for (time-series) charting.
dedup	Removes subsequent results that match a specified criterion.
eval	Calculates an expression. See COMMON EVAL FUNCTIONS.
fields	Removes fields from search results.
head/tail	Returns the first/last N results.
lookup	Adds field values from an external source.
rename	Renames a field. Use wildcards to specify multiple fields.
rex	Specifies regular expression named groups to extract fields.
search	Filters results to those that match the search expression.
sort	Sorts the search results by the specified fields.
stats	Provides statistics, grouped optionally by fields. See COMMON STATS FUNCTIONS.
mstats	Similar to stats but used on metrics instead of events.
table	Specifies fields to keep in the result set. Retains data in tabular format.
top/rare	Displays the most/least common values of a field.
transaction	Groups search results into transactions.
where	Filters search results using eval expressions. Used to compare two different fields.

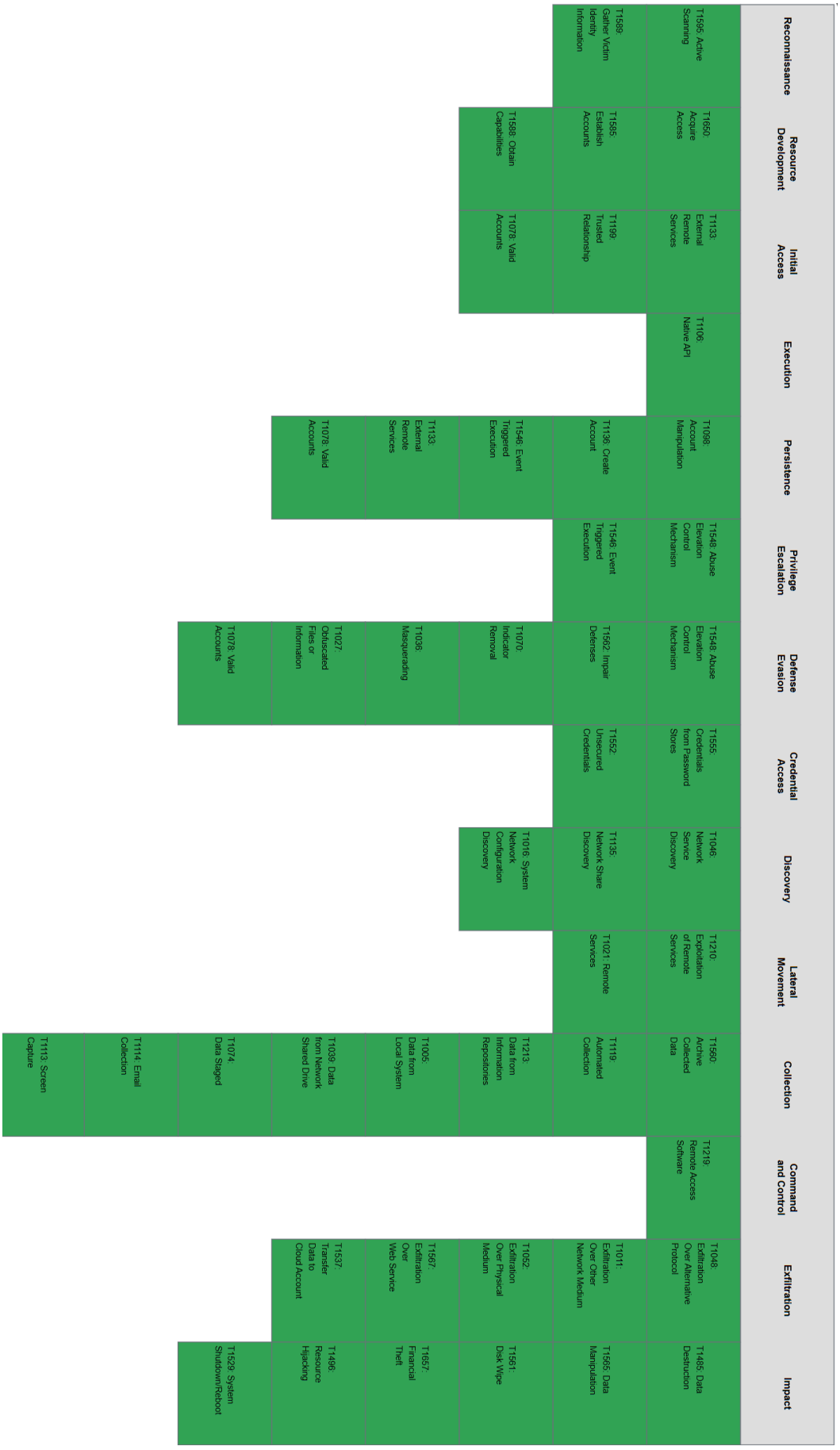
Common Eval Functions	The eval command calculates an expression and puts the resulting value into a field (e.g. "...| eval force = mass * acceleration"). The following table lists some of the functions used with the eval command. You can also use basic arithmetic operators (+ - * / %), string concatenation (e.g., "...| eval name = last . "," . first"), and Boolean operations (AND OR NOT XOR < > <= >= != = == LIKE).	
Function	**Description**	**Examples**
abs(X)	Returns the absolute value of X.	abs(number)
case(X,"Y",...)	Takes pairs of arguments X and Y, where X arguments are Boolean expressions. When evaluated to TRUE, the arguments return the corresponding Y argument.	case(error == 404, "Not found", error ==500,"Internal Server Error", error == 200, "OK")
ceil(X)	Ceiling of a number X.	ceil(1.9)
cidrmatch("X",Y)	Identifies IP addresses that belong to a particular subnet.	cidrmatch("123.132.32.0/25",ip)
coalesce(X,...)	Returns the first value that is not null.	coalesce(null(), "Returned val", null())
cos(X)	Calculates the cosine of X.	n=cos(0)
exact(X)	Evaluates an expression X using double precision floating point arithmetic.	exact(3.14*num)
exp(X)	Returns eX.	exp(3)
if(X,Y,Z)	If X evaluates to TRUE, the result is the second argument Y. If X evaluates to FALSE, the result evaluates to the third argument Z.	if(error==200, "OK", "Error")
in(field,valuelist)	Returns TRUE if a value in "value-list" matches a value in "field". You must use the "in" function inside the "if" function.	if(in(status, "404","500","503"),"true","false")
isbool(X)	Returns TRUE if X is Boolean.	isbool(field)

isint(X)	Returns TRUE if X is an integer.	isint(field)
isnull(X)	Returns TRUE if X is NULL.	isnull(field)
isstr()	Returns TRUE if X is a string.	isstr(field)
len(X)	This function returns the character length of a string X.	len(field)
like(X,"Y")	Returns TRUE if and only if X is like the SQLite pattern in Y.	like(field, "addr%")
log(X,Y)	Returns the log of the first argument X using the second argument Y as the base. Y defaults to 10.	log(number,2)
lower(X)	Returns the lowercase of X.	lower(username)
ltrim(X,Y)	Returns X with the characters in Y trimmed from the left side. Y defaults to spaces and tabs.	ltrim(" ZZZabcZZ ", " Z")
match(X,Y)	Returns if X matches the regex pattern Y.	match(field, "^\d{1,3}\.\d$")
max(X,...)	Returns the maximum.	max(delay, mydelay)
md5(X)	Returns the MD5 hash of a string value X.	md5(field)
min(X,...)	Returns the minimum.	min(delay, mydelay)
mvcount(X)	Returns the number of values of X.	mvcount(multifield)
mvfilter(X)	Filters a multi-valued field based on the Boolean expression X.	mvfilter(match(email, "net$"))
mvindex(X,Y,Z)	Returns a subset of the multivalued field X from start position (zero-based) Y to Z (optional).	mvindex(multifield, 2)
mvjoin(X,Y)	Given a multi-valued field X and string delimiter Y, and joins the individual values of X using Y.	mvjoin(address, ";")
now()	Returns the current time, represented in Unix time.	now()

null()	This function takes no arguments and returns NULL.	null()
nullif(X,Y)	Given two arguments, fields X and Y, and returns the X if the arguments are different. Otherwise returns NULL.	nullif(fieldA, fieldB)
random()	Returns a pseudo-random number ranging from 0 to 2147483647.	random()
relative_ time (X,Y)	Given epochtime time X and relative time specifier Y, returns the epochtime value of Y applied to X.	relative_time(now()," -1d@d")
replace(X,Y,Z)	Returns a string formed by substituting string Z for every occurrence of regex string Y in string X.	Returns date with the month and day numbers switched, so if the input was 4/30/2021 the return value would be 30/4/2021: replace(date,"^(\d{1,2})/(\d{1,2})/", "\2/\1/")
round(X,Y)	Returns X rounded to the amount of decimal places specified by Y. The default is to round to an integer.	round(3.5)
rtrim(X,Y)	Returns X with the characters in Y trimmed from the right side. If Y is not specified, spaces and tabs are trimmed.	rtrim(" ZZZZabcZZ ", " Z")
split(X,"Y")	Returns X as a multi-valued field, split by delimiter Y.	split(address, ";")
sqrt(X)	Returns the square root of X.	sqrt(9)
strftime(X,Y)	Returns epochtime value X rendered using the format specified by Y.	strftime(_time, "%H:%M")
strptime(X,Y)	Given a time represented by a string X, returns value parsed from format Y.	strptime(timeStr, "%H:%M")

substr(X,Y,Z)	Returns a substring field X from start position (1-based) Y for Z (optional) characters.	substr("string", 1, 3)
time()	Returns the wall-clock time with microsecond resolution.	time()
tonumber(X,Y)	Converts input string X to a number, where Y (optional, defaults to 10) defines the base of the number to convert to.	tonumber("0A4",16)
tostring(X,Y)	Returns a field value of X as a string. If the value of X is a number, it reformats it as a string. If X is a Boolean value„ reformats to "True" or "False". If X is a number, the second argument Y is optional and can either be "hex" (convert X to hexadecimal), "commas" (formats X with commas and 2 decimal places), or "duration" (converts seconds X to readable time format HH:MM:SS).	This example returns: foo=615 and foo2=00:10:15:… | eval foo=615 | eval foo2 = tostring(foo, “duration”)
typeof(X)	Returns a string representation of the field type.	This example returns: “NumberStringBooll nvalid”: typeof(12)+ typeof(“string”)+
urldecode(X)	Returns the URL X decoded.	urldecode("http%3A %2F%2Fwww.splun k.com%2Fdownload %3Fr%3Dheader")
validate| (X,Y,…)	Given pairs of arguments, Boolean expressions X and strings Y, returns the string Y corresponding to the first expression X that evaluates to False and defaults to NULL if all are True.	validate(isint(port), "ERROR: Port is not an integer", port >= 1 AND port <= 65535, "ERROR:Port is out of range")

II. Appendix


Reconnaissance
T1595: Active Scanning
T1589: Gather Victim Identity Information
Resource Development
T1650: Acquire Access
T1585: Establish Accounts
T1588: Obtain Capabilities
Initial Access
T1133: External Remote Services
T1199: Trusted Relationship
T1078: Valid Accounts
Execution
T1106: Native API
Persistence
T1098: Account Manipulation
T1136: Create Account
T1546: Event Triggered Execution
T1133: External Remote Services
T1078: Valid Accounts
Privilege Escalation
T1548: Abuse Elevation Control Mechanism
T1546: Event Triggered Execution
Defense Evasion
T1548: Abuse Elevation Control Mechanism
T1562: Impair Defenses
T1070: Indicator Removal
T1036: Masquerading
T1027: Obfuscated Files or Information
T1078: Valid Accounts
Credential Access
T1555: Credentials from Password Stores
T1552: Unsecured Credentials
Discovery
T1046: Network Service Discovery
T1135: Network Share Discovery
T1016: System Network Configuration Discovery
Lateral Movement
T1210: Exploitation of Remote Services
T1021 Remote Services
Collection
T1560: Archive Collected Data
T1119: Automated Collection
T1213: Data from Information Repositories
T1005: Data from Local System
T1039: Data from Network Shared Drive
T1074: Data Staged
T1114: Email Collection
T1113: Screen Capture
Command and Control
T1219: Remote Access Software
Exfiltration
T1048: Exfiltration Over Alternative Protocol
T1011: Exfiltration Over Other Network Medium
T1052: Exfiltration Over Physical Medium
T1567: Exfiltration Over Web Service
T1537: Transfer Data to Cloud Account
Impact
T1485 Data Destruction
T1565 Data Manipulation
T1561: Disk Wipe
T1657: Financial Theft
T1496: Resource Hijacking
T1529 System Shutdown/Reboot

References

CISA (2020). *Insider Threat Mitigation Guide*. [online] Available at: https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.

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

Ernst & Young (2020). *Managing Insider Threat: a Holistic Approach to Dealing with Risk from within*. [online] Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/EY-managing-insider-threat.pdf.

Liu, L., De Vel, O., Han, Q.-L., Zhang, J. and Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: a Survey. *IEEE Communications Surveys & Tutorials*, 20(2), pp.1397–1417. doi:https://doi.org/10.1109/comst.2018.2800740.

Lockheed Martin (2023). *Cyber Kill Chain*. [online] Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

McKemmish, R. (2008). When Is Digital Evidence Forensically Sound? *IFIP — The International Federation for Information Processing*, pp.3–15. doi:https://doi.org/10.1007/978-0-387-84927-0_1.

MITRE (2020a). *Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK®*. [online] attack.mitre.org. Available at: https://attack.mitre.org/techniques/T1595/.

MITRE (2020b). *Active Scanning: Vulnerability Scanning, Sub-technique T1595.002 - Enterprise | MITRE ATT&CK®*. [online] attack.mitre.org. Available at: https://attack.mitre.org/techniques/T1595/002/.

MITRE (2020c). *Gather Victim Network Information, Technique T1590 - Enterprise | MITRE ATT&CK®*. [online] attack.mitre.org. Available at: https://attack.mitre.org/techniques/T1590/.

MITRE (2020d). *Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®*. [online] attack.mitre.org. Available at: https://attack.mitre.org/tactics/TA0043/.

NCSC (2020). *8. Choose Services Which Have Been Designed for Zero Trust*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/zero-trust-architecture/choose-services-designed-for-zero-trust.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K.R. and Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics*, [online] 9(9), p.1460. doi:https://doi.org/10.3390/electronics9091460.

Schneier, B. (2000). *Secrets and Lies : Digital Security in a Networked World*. Indianapolis, Indiana: John Wiley & Sons, Inc.

SentinelOne (2021). *Elasticsearch vs Splunk: A Comparison and How to Choose | Scalyr*. [online] SentinelOne. Available at: https://www.sentinelone.com/blog/elasticsearch-vs-splunk-comparison/.

Splunk (2021). *Using Splunk UBA to Detect Insider Threats*. [online] Available at: https://www.splunk.com/en_us/pdfs/product-briefs/using-splunk-uba-to-detect-insider-threats.pdf.

Splunk (2023a). *Advanced Threat Detection*. [online] Splunk. Available at: https://www.splunk.com/en_us/solutions/advanced-threat-detection.html.

Splunk (2023b). *Splunk Cheat Sheet: Query, SPL, RegEx, & Commands*. [online] Splunk-Blogs. Available at: https://www.splunk.com/en_us/blog/learn/splunk-cheat-sheet-query-spl-regex-commands.html.

Splunk (2023c). *Splunk for Advanced Analytics and Threat Detection Powered by Splunk Enterprise Security and Splunk User Behavior Analytics*. [online] Available at: https://www.splunk.com/en_us/pdfs/tech-brief/splunk-for-advanced-analytics-and-threat-detection-tech-brief.pdf [Accessed 15 Mar. 2024].

Stolfo, S.J., Bellovin, S.M., Hershkop, S., Keromytis, A.D., Sinclair, S. and Smith, S.W. (2008). *Insider Attack and Cyber Security: beyond the Hacker*. [online] *Google Books*. Springer Science & Business Media. Available at: https://books.google.co.uk/books?hl=en&lr=lang_en&id=tW298SIeg4IC&oi=fnd&pg=PA1&ots=Ccj0fh8G0m&sig=DENu2QoF0YQ-3w75O2BRWdeWpV4&redir_esc=y#v=onepage&q&f=false [Accessed 13 Mar. 2024].

Verizon (2023). *2023 Data Breach Investigations Report*. [online] Verizon Business. Available at: https://www.verizon.com/business/resources/reports/dbir/.