KUSTODIAN SECURITY OPERATIONS CENTRE

SIEM- “SIEMONSTER” HIGH LEVEL DESIGN

Document Version	1.7
Lead Designer	James Bycroft / Chris Rock
Author	Chris Rock
Last Change Date	Thursday, 19 May 2016

Contact information

For more information on this document please contact:

Name	Chris Rock
Position	CEO
Location	Level 50 /120 Collins Street
Telephone	+61 1800-HACKER +1 8447-HACKER
E-mail	chris@kustodian.com

The following people can also be contacted in relation to this document:

Name	Position	Email
Chris Rock	Solution Lead	chris@siemonster.com
James Bycroft	Lead Architect	james@siemonster.com
Ian Latter	Architect	ian@siemonster.com
Dez Rock	Solution Analyst	dez@siemonster.com

Document Reviewers

Name	Position	Signature	Date
Chris Rock	Solution Lead		24/4/16
James Bycroft	Lead Architect		24/4/16
Ian Latter	Architect		24/4/16

Revision history

Revision	Revision Description	Date	Changed By
1.0	Revision Version 1 – Pre Release	20/4/2016	CR
1.1	Re-Architecture of single Image Final Version 1.1	24/4/2016	JB
1.2	Cluster Amazon specs changed from R3 to M4.2 Xlarge based on latest performance testing done buy logz.io http://logz.io/blog/benchmark-elasticsearch/	4/5/2016	CR
1.3	Typo's and rearranging Roles in Hardware, and FIR put into Proteus.	5/5/2016	CR
1.4	Rewording of 3.2 (AWS roles)	6/5/2016	CR
1.5	Syslog-Ng removed confused installers	6/5/2016	CR
1.6	Agent Flow Diagrams added	7/5/2016	CR
1.7	Typos and Confidential→ Public Classification	19/5/2016	CR

Referenced documents

Reference	Document Name	Location
[1]		Kustodian

Glossary

The following terms and acronyms are used in this document:

Term	Definition
AD	Active Directory
ASA	Cisco ASA IPS / Firewall
Critical Stack	Real time threat analysis framework
Elastic	Providers of Elastic Search, Kibana, Logstash, SHIELD
ELK	ElasticSearch Logstash and Kibana Open Source Data analytics
Graylog	Open Source Log Management
Kustodian	Security company providing SIEMonster
IIS	Internet Information Services
OSINT	Open Source Threat Intelligence
OSSEC Wazuh	Open Source Host-based Intrusion Detection System Project Wazuh Fork
SLACK	Private Real time messaging system allowing group sharing of messengers
SIEM	Security Incident and Event Management
SOC	Security Operations Centre
Proteus	Cluster Node 1, Non-Data, Master Eligible, Logstash Server, Kibana Server, Rabbit MQ, Syslog-NG Server, Incident Response Server, OSINT
Kraken	Cluster Node 2, ElasticSearch Server, Data node
Tiamat	Cluster Node 3, ElasticSearch Server, Data node
Capricorn	OSSEC Server, Graylog Server - Alerts, Filebeat, Outputs for Future Alert Visualisation
Hydra	Optional Relay Server – Onsite. Logstash Server, RabbitMQ, Syslog-NG Server

Table of contents

1 AUTHORS PREFACE

As a security professional, protecting your company's assets from Cyber-attacks is a complex task. It is crucial you have visibility across your entire environment. It's like having a house alarm, there is no point having some rooms with motion sensors and others without it.

All systems that have the ability log or alert that something is happening but is there anyone listening. When you picture your environment, with Servers, workstation, network appliances, printers, SCADA and other equipment they all let out events and alerts. On top of this all your applications are sending out alerts, Web Servers, applications, Anti-Virus, Endpoint protection.

By using a Security Incident Events Management system (SIEM) you can capture all of these cries for help, separate the "Cry wolfs" from the real attacks and alert the operator that an attack maybe underway. Operators can be alerted via a Dashboard, an SMS, Slack or email for any suspect activity when an administrator creates a privileged account or alerted when an executive is using email from a destination that is different from their current location. The rules and alerts to suit your business are limitless.

What are the SIEM options? Of course there is a myriad of commercial products out there such as HP ArcSight and SPLUNK but these solutions come with node/GB limitations and can be quite expensive and of course the ongoing annual costs really stack up.

Of course you can go the open source route, and use Elastic Logstash and Kibana (Elastic Systems) system or Cisco OpenStack, but speaking from experience the time you have built the plugins, dashboards, parses to have a functioning SIEM you're looking at a years' worth of development. ELK is not a SIEM, its data analytics, you need other tools to make it a SIEM.

Kustodian have done this development for you and built a SIEM using the latest open source frameworks built on Elastic. We researched across all the open community projects including BlacktHat and DEFCON presentations, GitHub to make sure we had the best SIEM components available. The free open source version is called SIEMonster. SIEMonster is a free open source unlimited use version comes with all the OSINT, HIDS, dashboards, plugins, incident response tools including ticketing systems to make a functioning SIEM and Security Operation Centre (SOC). SIEMonster is a commercial grade enterprise SIEM with dashboard development and a suite of documentation (Standard Operating Procedures, Detailed Designs, DR fail over, Backups, installation guides etc.)

After the successful development and roll out of an Open source SOC into a multi-region stock listed company with over 20,000 seats it made sense to allow companies to use our system for their own environments.

The solution can be either onsite in a data centre or in the cloud such as AWS. This solution makes it simple for businesses to use open source SIEM technologies without the development headaches, documentation integration, and unlimited use and is affordable which all other products don't provide.

2 INTRODUCTION

Kustodian has spoken with a variety of its customer in a series of collaborated workshops on the problems with existing commercial SIEM solutions as well as Open source options. The biggest complaint about commercial SIEM's was the ongoing licence fees, high costs and sizing limitations. The complaints for open source was it required thousands of development hours, documentation integrations that it wasn't turnkey. Security professionals needed a working product not a framework and support options were just as expensive as the commercial products.

Kustodian has chosen Elastic's ELK for the SIEM's base. ELK by itself does not provide a SIEM but is a perfect base to build a SIEM using fantastic frameworks out there including OSINT, OSSEC Wazuh fork, Graylog UI, FIR (incident ticketing), community rulesets and dashboards, community and open source free plugins that make the SIEM.

Based on these workshops Kustodian have built and open source SIEM solution to meet companies Informational Assurance visions without the development or ongoing cost but support options are available to clients to need assistance or custom dashboards. SIEMonster can exist both in the cloud such as AWS or in the clients existing Data Centre. Some of our clients were restricted in housing data offshore, so we catered for both. SIEMonster has the following benefits.

- Fully Open Source SIEM
- No License restrictions such as node or data limitations
- Open Community for additional features
- Completely free unless you require Enterprise Support (custom dashes etc)
- On premise hosted Security Analytics and SIEM Open SOC or Cloud Hosted
- Instant Incident Alerting via email or SMS or Console view via a secure portal and integration with "Slack"/"Hipchat" using Graylog Streams.
- Provide continuous Cyber Security monitoring identify, mitigate & respond to internal and external risks in real time
- Full ISMS suite of documentation including Detailed Designs, Build Guides, Maintenance and Standard Operating Procedures etc.
- Full integration with OSSEC Wazuh fork for Host Intrusion Detection and PCIDSS ruleset incorporated into Elastic
- Threat Intelligence using open source OSINT Critical stack and Intelligence feeds
- Incorporate your existing Vulnerability Scans into the Dashboard, (OpenVas,McAfee, Nessus etc.)
- Open Source Incident Response Ticketing system for Incident recording, raising tickets to other operators or a whiteboard to show night shift analysts current issues

Organisations have a multitude of security and network appliances all logging security events. However due to their size and complexity these logs are not correlated together in one portal to analyse these events. These security events will provide a clear picture to your team on how the end user is using the network to detect

- User Activity, compliance including PCIDSS
- Users trying to access payroll or Intellectual Property.
- End point compliance
- Misuse of the environment including illegal file downloads
- Hackers accessing the network the network

2.1 HIGH LEVEL COMPONENTS

This solution includes the following high level components.

SIEM & SIM / SEM – Is built to provide 24x7 Security Event collection, correlation and Incident response. Risk Identification, visual alerting, analysis and secondary email/SMS/Slack alerts to the operator.

Software Components – All open source components that are included in SIEMonster.

Hardware Components – Virtual hardware requirements for Virtual environment

Configuration – SIEMonster configuration, rulesets, architecture, equipment requirements, backups and maintenance.

Dashboards – Visual representation of configured alerts and risks in the environment.

Rules and Search – How to configure rules and run searches using Elastic Search

Incident Response Alerting and Ticketing – Ticketing system to record Incident Response, and documentation for security analysts and Graylog for alerting and UI

Host Based Intrusion Detection Alerting – Integration with OSSEC Wazuh fork to allow HIDS alerting and pre-built rulesets including PCIDSS.

OSINT – Integration with Open Source Threat Intelligence for real time threats in the wild incorporating Critical Stack.

Vulnerability Scanning – Using your existing vulnerability scanning tool incorporated into a world view dashboard revealing hot spots in your network

Reporting – Reporting snapshots of your SIEM

Plugin Development – How to develop your own plugins for specific equipment like SCADA or custom equipment or how to get help from the community of Kustodian to monitor specific equipment like Blast Furnaces, paint guns, robotic arms or production lines.

.

2.2 SCOPE

This document covers all the software and hardware infrastructure components for the Security Operations Centre SIEMonster product. Separate documents such as build guides, standard operating procedures, troubleshooting and maintenance are in other documents included in the document suite. Training videos, and how to use guides are on the SIEMonster website. http://www.siemonster.com

2.3 AUDIENCE

This document is intended for technical representatives of companies, SOC owners as well security analysts and professionals. The audience of this document are expected to have a thorough level of knowledge of Security, Software and Server Architecture.

The relevant parts are included here for convenience, and may of course be subject to change. They will be updated when notification is received from the relevant owners.

3 FUNCTIONAL OVERVIEW

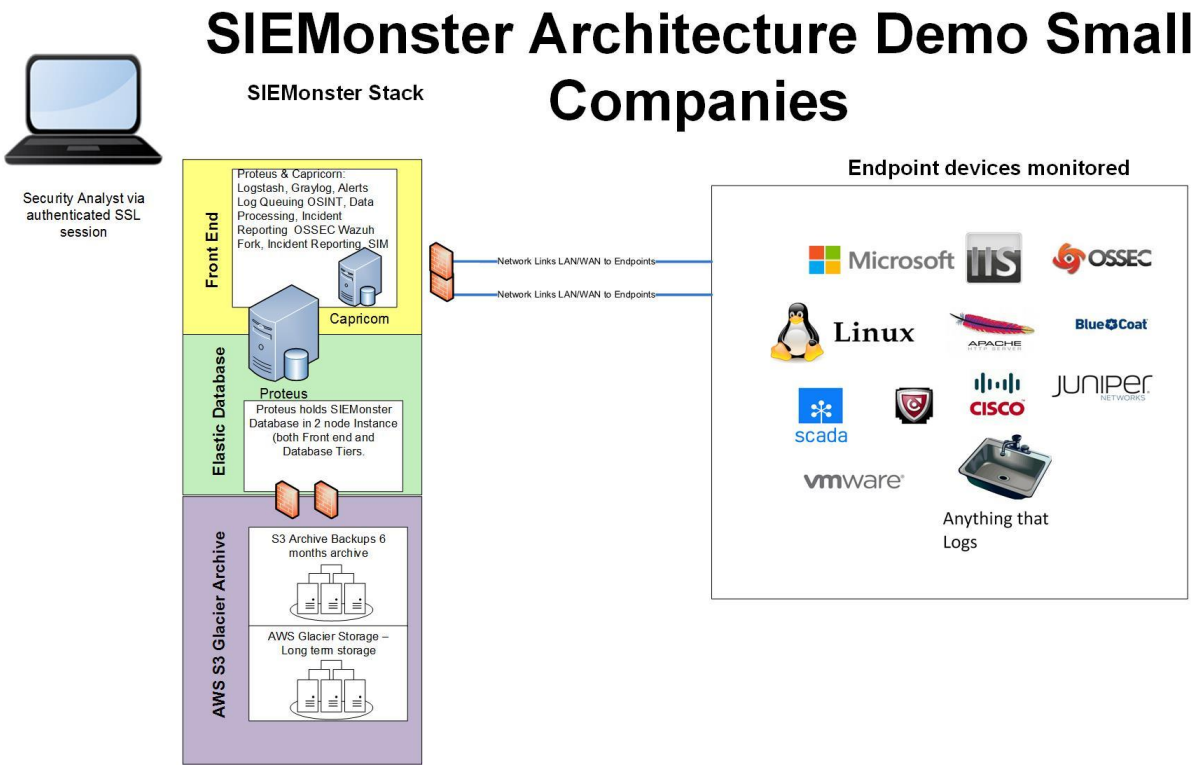
3.1 HIGH LEVEL OVERVIEW

The SIEMonster Architecture is based on events being shipped, queued, and processed from endpoints within the organisation. Alerts based on rules stored and then Visualised using open source products only. Data Sources can be any device. Anything that produces an alert, a syslog or agent can be captured, correctly formatted and sent into the SIEM for analysis. This includes Network Appliances, Windows/Linux Servers, Applications, Security Appliances and SCADA. The events are filtered and stored. OSINT will alert the operator to known attack IP's and patterns from around the world, Kustodian and OSSEC rules will identify any breaches or non-compliance and Alerts.

3.2 SIEMONSTER HIGH LEVEL ARCHITECTURE DEMO OR SMALLER COMPANIES

Endpoint logs data are sent to Proteus. HIDS data is sent to Capricorn. The Master node (Proteus) provides data filtering and queuing via RabbitMQ, Logstash, OSINT, and Syslog data pipelining. Proteus also provides the FIR incident response web application. In the 2 node Tier Proteus also acts as the ES server database server. The ES engine is for medium/long term data storage/analysis listed below in green. After data is processed and stored on Proteus, the data is forked to Capricorn. Capricorn provides a single Graylog node and OSSEC HIDS Server. Graylog provides a disposable 24-hour Index used primarily for Alerting (comparable to Watcher for Elasticsearch) and additional data analysis.

Node to node communications are over TLS 1.2 secured by SearchGuard SSL (similar properties to Elasticsearch Shield). Optional AWS integration in purple includes automated archiving 6 months or backups annually and maintenance.

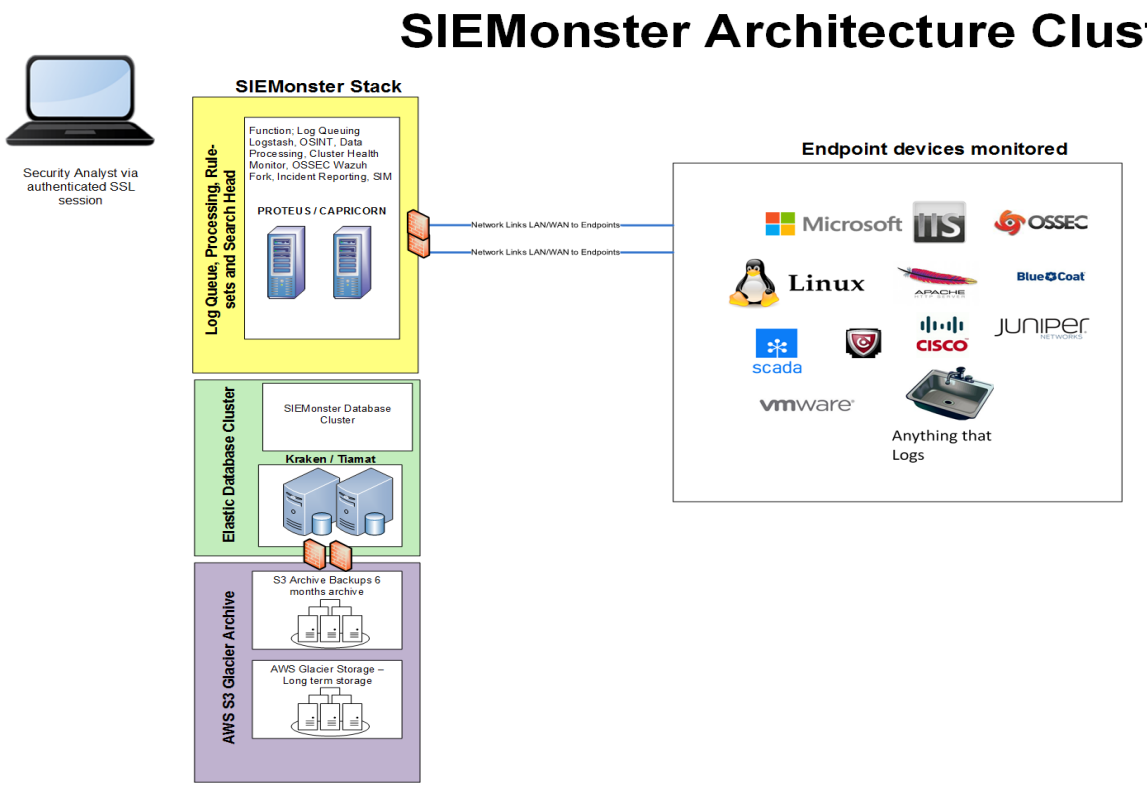


3.3 SIEMONSTER HIGH LEVEL ARCHITECTURE CLUSTER FOR MEDIUM TO LARGE ORGANIZATIONS

Proteus: Master Node high spec rated server in yellow below. Endpoint logs are sent to Proteus, HIDS data is sent to Capricorn. The Master node provides data filtering and queuing via RabbitMQ, Logstash, Cluster Health monitoring, OSINT, and Syslog data pipelining. Proteus also provides the FIR incident response web application. The data is then forked to both the ES cluster(green) and the Alerting Server – 'Capricorn'. The clustered High spec ES engine is for medium/long term data storage/analysis.

Capricorn: (yellow high spec rated server below) Provides a single Graylog node and OSSEC HIDS Server. Graylog provides a disposable 24-hour Index used primarily for Alerting (comparable to Watcher for Elasticsearch) SIM/SEM function and additional data analysis

Node to node communications are over TLS 1.2 secured by SearchGuard SSL (similar properties to Elasticsearch Shield). Optional AWS integration in purple includes automated archiving 6 months or backups annually and maintenance.



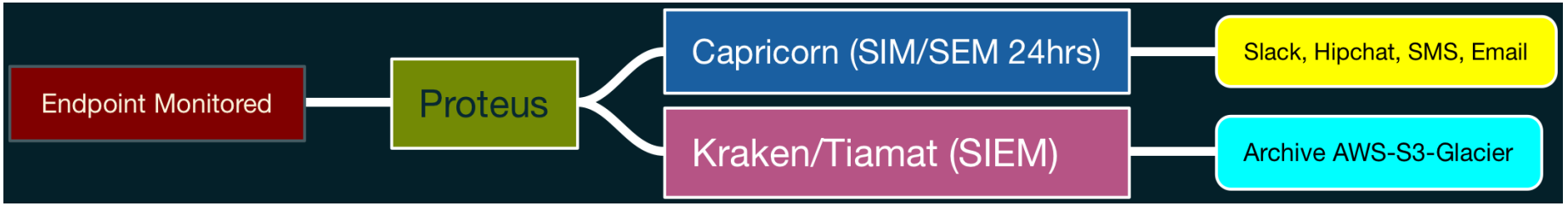
3.4 SIEMONSTER HIGH LEVEL ARCHITECTURE

TIER	Software and Role
End Nodes	Linux hosts: Sylog-ng, OSSEC (logs and HIDS) Windows hosts: Nxlog, OSSEC (logs and HIDS) Other: syslog's (logs) End nodes will send their logs, alerts to the Master Node encrypted.
Master Node – Linux (Proteus)	Master Node provides Logstash, Cluster Health for the Elasticsearch cluster below in green. Server also provides log queuing and filtering using RabbitMQ, rulesets and Kibana. The master node also provides the FIR incident response web application. Server also has OSINT installed using Critical Stack as well as light weight web server for vulnerability scanning integration and an Incident Response Management System. (High Spec)
Alerting/IR Server – Linux (Capricorn)	Alerting/Analysis server provide a single node Graylog instance for alerting via email, Slack, Hipchat etc. Server also provides OSSEC Wazuh fork HIDS and Filebeat. (High Spec)
Cluster Nodes – Linux (Kraken/Tiamat)	Server Cluster running Elastic stores all your data logs in a data base. The servers are High Spec with 32GB RAM. When a user performs a search for example using the Master Node above. "All users who used the word confidential in an email sending to an external email domain" Elastic Search database will locate the entries and present the lookup to the user in Kibana (yellow)
Amazon AWS	Using Amazon AWS, the Master Node Scripts will archive your Cluster Node database entries to Amazon S3 for archival storage. This scripts can be changed to any value i.e. archive all data after 6 months or a year. Scripts automatically backup your data to Amazon Glacier for 1-7 years or whatever your compliance requirements.

3.5 SIM / SEM / SIEM

Without the over complications of multi security terms that often overlay each with any SOC monitoring, there is always two types of monitoring. There is the instant alert, an Administrator is being added to the systems, a hacker probing an external router and there is also the long term correlation rule trigger events, for example a user that normally logs on between 8-9am from California is now logging on from both California and China at the same time. In some outsourced environments the Instant alert, trigger events are done by a 24/7 SOC and the SIEM correlation events are done in house as they are in the best situation to know their business heuristics. SIEMonster provides both functions. The instant alerts, events viruses via Proteus/Capricorn and the longer SIEM function for searches on staff sending emails external over a 6-month period via the Kraken/Tiamat. Although Capricorn is designed as a 24 hr volatile memory state it can be increased for longer durations but remember all events are forked into the SIEM anyway, so we found 24hrs was ideal.

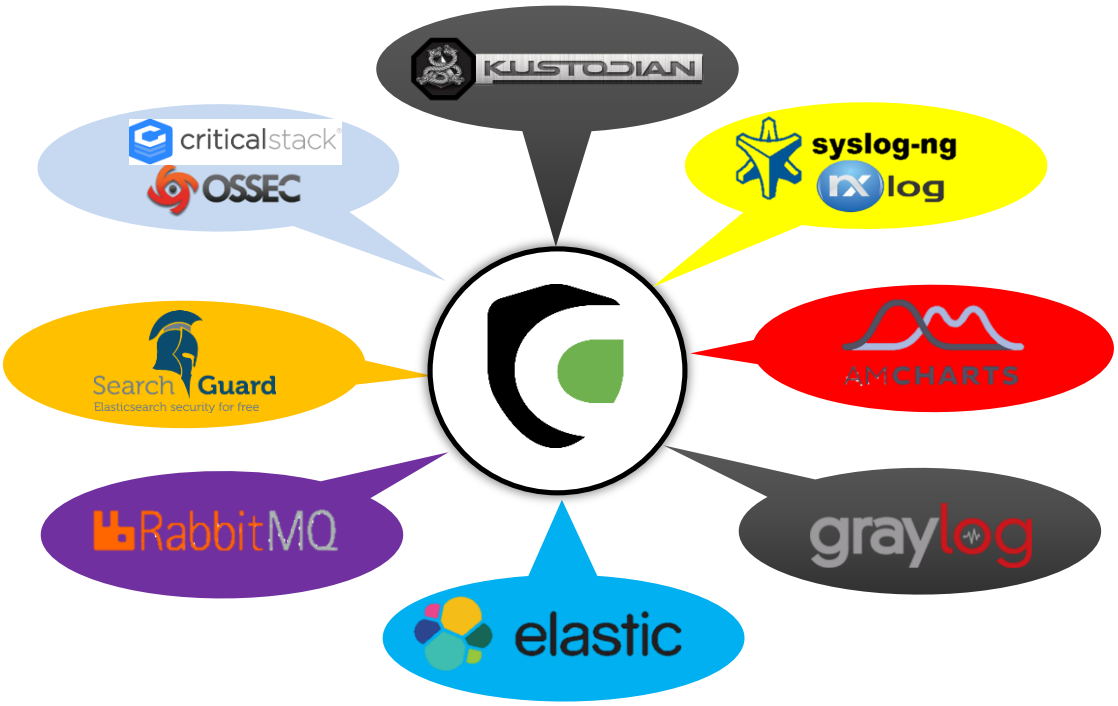
Most SOC'S run the traditional Dashboards, which work well but we wanted a more modernised approach for those organisations who didn't want to be tied to a console and have incorporated, Slack, Hipchat SMS and email support or you can run both Dashboard and the other services for alerts. The events are configurable, so you can send out management alerts or alerts to an outsourced 3rd party without the client details in them for example, no client name or IP or distinguishable details. Just enough to raise the alarm.



3.6 FUNCTIONAL ARCHITECTURE OVERVIEW – SOFTWARE STACK

The solution had to be completely scalable, open source and completely free without exception. Using SIEMonster you can use it for free and as many nodes/clusters as you need without data restrictions.

Purpose	Description
Log Retrieval	Filebeats, Syslogs, NXlog, Ossec
Process	RabbitMQ, Logstash, Kustodian
Intrusion Detection	OSSEC with Wazuh fork
Rules, Storage, Alerting	Logstash, Elasticsearch, Graylog, Kustodian. OSSEC Wazuh fork
Security	SearchGuard, Firewalls & Lockdowns
Threat Intelligence	Critical Stack, open source feeds
Visualize	Kibana, Slack, emails, AMcharts
Backup scripts, Maintenance	Kustodian scripted AWS Glacier backup, archiving and restoring
Vulnerability Scanning	Use OpenVAS or use your own commercial scanner.
Ticketing	FIR – Fast Incident Response



3.7 RULESETS

Pre-configured alerting rule sets have been created for your use and well as integrated rules from the community are included. For example, if you want to know when a user is added to the Domain admin group, an alert will be issued or a PCIDSS environment has detected open telnet in a Card Holder Data's environment.

Sample Rule-sets to get the idea.

Rule Name	Description
Logon	A user fails to login 10 times or more within a 60-minute period
Trojan	A Trojan virus outbreak spikes at more than x events per hour
DDOS	A webserver experiences a denial of service attack when the rate of events spikes beyond a set limit
User Lockout	The rate of user lockouts spikes beyond a set limit, indicating a brute force attack
User privilege uplift	A user adds another user to a Domain Admin or administrators group.
Weird network activity	Anomalous network activity detection outside of expected patterns
Email box compromised	A user logs on to OWA from multiple IP's in different countries
Redundant Staff	A redundant staff member group for catching IP leaving your Enterprise "4 Weeks' Notice period"
Custom Alerts	Anything can be made into an alert to an email, a Dashboard alert or an SMS
Email	User using the word Confidential, Top Secret, private to a sender to an outside organisation or their own personal Hotmail/Gmail account against company policy

3.8 SIEMONSTER FUNCTIONAL TECH / METRICS OVERVIEW

Two VM Instance (Proteus & Capricorn)

The following metrics if for a demo or small company running up to 100 monitored endpoints as a baseline of what you archive monitoring an array of equipment from around the organisation can. This node is flexible, and is scalable to a multi node cluster at any time

Equipment:

2 Servers comprising of

- M4.2Xlarge AWS spec - Data Node / Logstash/Syslog/RabbitMQ, OSINT and Incident Response Management – Server Proteus
- M4.2Xlarge AWS spec – OSSEC/ Graylog/Filebeat - Server name Capricorn

Enterprise Sample metrics:

Event Rate: ~ 50,000 events per hour scalable upwards
30-day time frame for open indices
6 months' data maintained onsite / Weekly snapshots
Data archive to AWS Glacier/S3

Multi Node Cluster (Proteus-Capricorn-Kraken-Tiamat)

The following metrics is the typical Enterprise size of a 10,000-20,000 seats with 1000 monitored endpoints as a baseline of what you archive monitoring an array of equipment from around the organisation can. These cluster nodes are flexible, and can be scalable to a Quad node cluster at any time to suit any company size. If your organisation has WAN LINK of 256k-2MG and you are concerned about WAN overload, the event collectors can be configured to a 32-64k feed to not flood your links.

Equipment:

4 Server instances Redundant ES Cluster and Single Node Graylog/FIR Server comprising of

- M4.2Xlarge AWS spec Non Data cluster health / Logstash/Syslog/RabbitMQ, OSINT and Incident Response– Server name Proteus
- M4.2Xlarge AWS spec Alerting incorporating Graylog and OSSEC HIDS – Server name Capricorn
- 2 X M4.2Xlarge AWS spec End DATA Elastic Cluster (redundant pair) Server name Kraken and Tiamat

Enterprise Sample metrics:

Event Rate: ~ 350,000 events per hour scalable upwards
30-day time frame for open indices
6 months' data maintained onsite / Weekly snapshots
Data archive to AWS Glacier/S3

Monitoring aspects Sample:

- Multiple Domain Controllers Security Event Logs
- External Websites IIS & Apache
- Exchange OWA and Message Tracking
- Multiple Cisco Devices
- IPS devices
- VPN Concentrators
- Internal Asset Vulnerability Analysis Data
- Bluecoat Proxy
- Ironport Firewalls
- McAfee ePO Orchestrator
- OSSEC HIDS Data
- Any device that's produce a log, syslog snmp or agent installed.

Alerting – Events and Metrics Sample:

- Administrator Actions
- Logon Failures
- Anomalous Activity – Spikes/Flatlines
- Brute force attacks
- Multiple Logon Source IPs
- Email phishing and virus attacks
- Denial of Service Attacks
- Web Application Hacking Attempts
- Honeypot activity
- HIDS
- Virus Outbreaks
- Heartbeat

Visualisation: Dashboards for event visualisation Sample

- SOC Dashboard with breakdowns of relevant DC security Events
- 2007, 2010-2013 Microsoft Exchange Dashboards for Tracking Logs
- Exchange OWA Activity
- External Website Dashboards for IIS and Apache
- Cisco
- Threat Intelligence OSINT
- IPS
- Antivirus
- OSSEC HIDS
- Bluecoat Proxy
- Syslog
- Vulnerability Data
- Anything that logs, you can visualize

4 VIRTUAL HARDWARE

4.1 SIEMONSTER AWS VIRTUAL SERVERS DUAL NODE - SMALL

Whether you decide to go bare metal, VM in your datacentre or AWS the important thing to note is RAM and I/O on SSD is more important than CPU cores. We have tested on a variety of specs and found the 8/32 Front End and 8/32 for the Cluster is the ideal number for solution without headaches.

Total Servers: 2

Server 1: Proteus (Contains Elastic DB in 2 node instance)

SIEMonster Recommended Server Specifications – Front End	
Build	Cloud AWS M4.2XLarge
CPU	8 Cores
Memory	32 GB RAM
Storage	1 X 80 SSD
Operating System	Standard 64-bit Ubuntu 14.04

Server 2: Capricorn

SIEMonster Recommended Server Specifications	
Build	Cloud AWS M4.2Xlarge
CPU	8 Cores
Memory	32 GB RAM
Storage	1 X 80 SSD
Operating System	Standard 64-bit Linux Ubuntu 14.04

4.2 SIEMONSTER AWS VIRTUAL SERVERS - CORPORATE

Total Servers: 4

Server 1: Proteus (Cluster Health / Logstash/CriticalStack Client/FIR/Kibana)

SIEMonser Recommended Server Specifications – Front End	
Build	Cloud AWS M4.2XLarge
CPU	8 Cores
Memory	32 GB RAM
Storage	1 X 80 SSD
Operating System	Standard 64-bit Ubuntu 14.04

Server 2: Capricorn (Graylog/OSSEC/Filebeat)

SIEMonser Recommended Server Specifications – Front End	
Build	Cloud AWS M4.2XLarge
CPU	8 Cores
Memory	32 GB RAM
Storage	1 X 80 SSD
Operating System	Standard 64-bit Ubuntu 14.04

Server 3: Kraken Data Cluster Node 1

SIEMonster Recommended Server Specifications Data Cluster 1 and 2	
Build	Cloud AWS M4.2Xlarge
CPU	8 Cores
Memory	32 GB RAM
Storage	1 X 80 SSD
Operating System	Standard 64-bit Linux Ubuntu 14.04

Server 4: Tiamat Data Cluster Node 2

SIEMonster Recommended Server Specifications Data Cluster 1 and 2	
Build	Cloud AWS M4.2.Xlarge
CPU	8 Cores
Memory	32 GB RAM
Storage	1 X 80 SSD
Operating System	Standard 64-bit Linux Ubuntu 14.04

4.3 STORAGE RECOMMENDATIONS

Using Amazon AWS storage or local storage the costs are negligible. Data volumes of course will vary from client to client depending on how many agents your data is being transmitted but as a guide, here is a good way of managing your data requirements. Based on premise that the SIEM will store 100 GB per month and increase by 100 GB per month that's approximately 1.2 TB per year at AWS S3 storage costs of less than $500 per year. You will notice that at any stage at 6 months, 1 year, 2 years you can move your data from fast S3 storage to Amazon Glacier storage at no cost. This means you can archive your data whenever you like. You can still access the data (for a fee) but you remove the load from the Elastic Database. You might grow at 1 TB per month, even so the costs are very small for backed up storage. Of course if your data is 10-100 times this in size, just multiply it out to give yourself a guide.

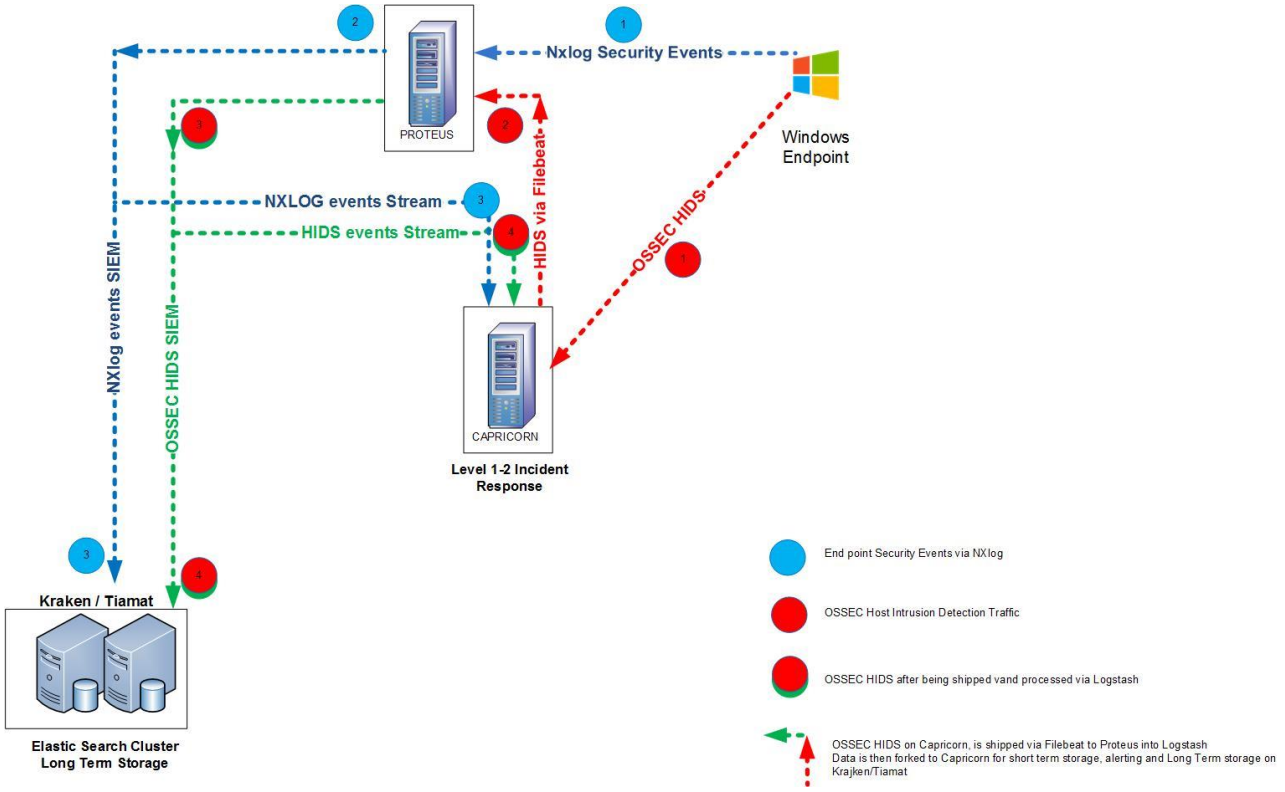
	S3 Storage	S3 Cost	Glacier Storage	Glacier Cost	**Total month**
Month 1	100	3.30	0.00	0	3.30
Month 2	200	6.60	0.00	0	6.60
Month 3	300	9.90	0.00	0	9.90
Month 4	400	13.20	0.00	0	13.20
Month 5	500	16.50	0.00	0	16.50
Month 6	600	19.80	0.00	0	19.80
Month 7	700	23.10	0.00	0	23.10
Month 8	800	26.40	0.00	0	26.40
Month 9	900	29.70	0.00	0	29.70
Month 10	1000	33.00	0.00	0	33.00
Month 11	1100	36.30	0.00	0	36.30
Month 12	1200	39.60	0.00	0	39.60

5 SOFTWARE STACK DETAILS

5.1 END USER AGENTS

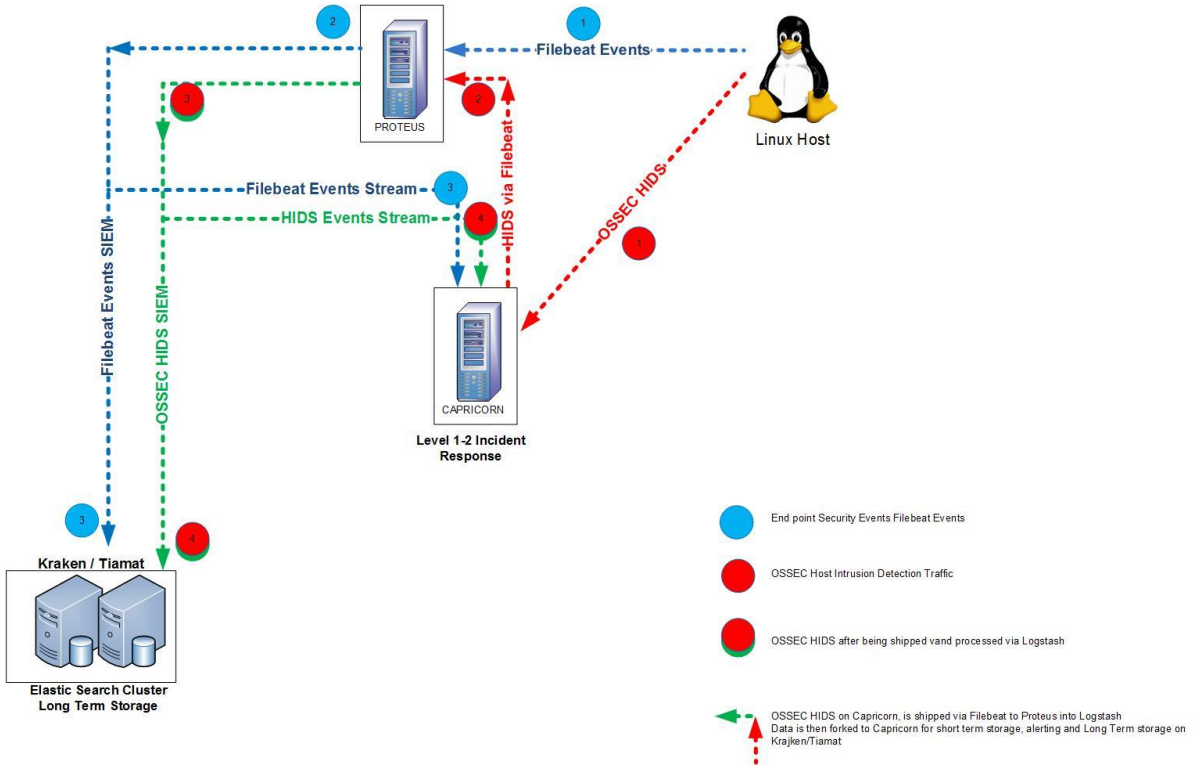
Windows Endpoint Host: On a Microsoft host, NX-Log is to be installed. This will collect event logs and send them to Proteus via SSL for Logstash analysis. The data then will be forked to Capricorn for Alerting/Analysis short term storage as well as the ElasticSearch database on Kraken/Tiamat. OSSEC agents are also recommended to be installed on Windows hosts to provide Host Intrusion Detection analysis as well.

Once OSSEC agents are installed these events will be sent to Capricorn (not Proteus) to the OSSEC sever. Capricorn will then send these events via Filebeat to Proteus to enter the fork stream to both short term analysis and Long term SIEM storage.

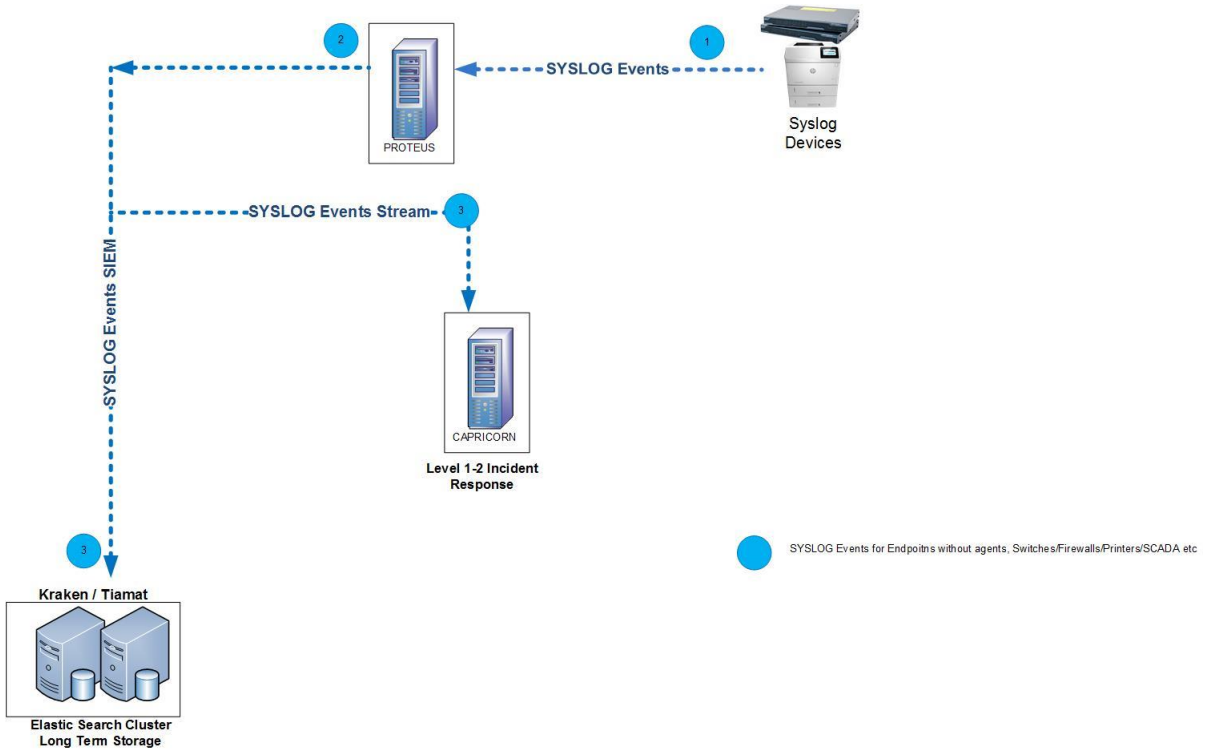


Linux Endpoint Host: On a Linux host, Filebeat is to be installed. This will collect event logs and send them to Proteus via SSL for Logstash analysis. The data then will be forked to Capricorn for Alerting/Analysis short term storage as well as the ElasticSearch database on Kraken/Tiamat. OSSEC agents are also recommended to be installed on Linux hosts to provide Host Intrusion Detection analysis as well.

Once OSSEC agents are installed these events will be sent to Capricorn (not Proteus) to the OSSEC sever. Capricorn will then send these events via Filebeat to Proteus to enter the fork stream to both short term analysis and Long term SIEM storage.



Agentless Endpoint Hosts (SYSLOG): On a network appliance/printer/SCADA device that does not have an agent point the hosts SYSLOG configuration to Proteus. Proteus is running Syslog-ng and will capture all syslogs and insert them into the Logstash stream fork procedure. The data then will be forked to Capricorn for Alerting/Analysis short term storage as well as the ElasticSearch database on Kraken/Tiamat.



5.1.1 Log Forwarding (Filebeat / NXlog / OSSEC)

Secure log forwarding offering deployments for UNIX and Windows environments. Secured against intrusion by TLS/SSL encryption using purchased certificates or in-house self-signed or propriety certs. By using this encryption and other methods there is no need for the Elastic Shield product which means support is free.

- OSSEC Wazuh agents install on Windows and Linux hosts to collect and send HIDS data to Capricorn
- Preconfigured Nxlog agent with SSL certificates is used for Windows hosts is used for log collecting and sending to Proteus
- Hosts that don't support an agent such as Network appliances can be configured to send all alerts SYSLOGS (0,1,2,3,4+) Port 514/1514 TCP/UDP to Proteus.

5.2 PROTEUS SERVER

Proteus function in SIEMonster is to queue, filter and process incoming endpoint data, apply rulesets and send the data to both Capricorn for instant alerting and Kraken/Tiamat for long term database storage. Proteus providers cluster health monitoring for Kraken/Tiamat. Proteus also runs Fast Incident Response (FIR) for Incident ticketing and Kibana. Kibana provides the dashboard view for the events captured in the database on the cluster. Proteus has Open Source threat intelligence OSINT installed using Critical Stack.

In the 4 node instance Proteus is the master node running Elastic Search non data.
In the 2 node instance Proteus is the master node running Elastic Search with data.

5.2.1 Software Overview Function Table

Proteus	Function
Logstash	Log retrieval, processing
RabbitMq	Messaging queuing
Critical Stack / OSINT	Open Source Threat Intelligence
FIR Fast Incident Response	Ticketing system for incidents and investigations
Elastic Search	Open source, distributed, real-time search and analytics engine
Kibana	Visualization tool through a Browser (Dashboards)
AMCharts	Geo Location charting
Elastalert	Alerting system for integration into SMS/Email/Slack etc

5.3 CAPRICORN SERVER

Capricorn's primary function is to provide security professionals with real time alert, analysis, triage of events as they come into the organisation. In SIEMonster Capricorn provides a single instance for alerting via email, SNS, Slack and Hipchat. Graylog has produced a virtual appliance as an open source product as an extension to Elastic Stack to the community and it is included in SIEMonster design.

Capricorn receives a volatile (short life) stream of data 12/24hrs (configurable up or down) from Proteus for instant alerting on rules within your organisation. The security operations staff will respond to these alerts. The other stream for long term storage goes to Kraken and Tiamat for Elastic Search traditional SIEM correlation searches over long periods of time.

Capricorn also provides OSSEC Wazuh fork Host Intrusion Detection (HIDS), optional Slack Alerting options. Filebeat is required to ship OSSEC logs received and send them to Proteus to enter the FORK data stream both back to Capricorn and long term storage in Kraken and Tiamat

5.3.1 Software Overview Function Table

Capricorn	Function
Graylog	Event Management Stream/Alerting Real Time alerts
OSSEC Wazuh Fork	Rulesets, PCIDSS, CIS benchmarks, Forensic analysis
Filebeat	Linux log shipper into Elastic Search
Slack	Optional Alerting to Mobile Devices for groups of Sec pros privately
Elastic Search	Open source, distributed, real-time search and analytics engine

5.4 KRAKEN AND TIAMAT CLUSTER

Kraken's primary function is Cluster Node 1 Elastic storing all your long term SIEM data in the database. When a user performs a Kibana search on. "All users who used the word confidential in an email sending to an external email domain" Elastic Search database will locate the entries and present the lookup to the user in Kibana. Cluster Node 2 called Tiamat is identical and provides redundancy for Kraken. The health and controlling of the cluster is done by Proteus. In the event of hardware failure, a cluster node can be bought offline and another replaced.

5.4.1 Software Overview Function Table

Kraken/Tiamat	Function
Elastic Search	Open source, distributed, real-time search and analytics engine

6 SECURITY

The SIEM servers must reside in a secure subnet protected by a Firewall blocking all but the required ports. The SIEM contains the most sensitive logs and must be protected from the other network equipment. Administration access should be restricted via ACLS and SIEMonster is configured for user/password access. Some of the technologies are listed below.

- Flexible REST layer access control (User/Role based; on aliases, indices and types)
- Flexible transport layer access control (User/Role based; on aliases, indices and types)
- Document level security (DLS): Retrieve only documents matching criteria
- Field level security (FLS): Filter out fields/source parts from a search response
- HTTP authentication (SPNEGO/Kerberos, Mutual SSL/CLIENT-CERT)
- HTTP session support through cookies
- Authentication backends (LDAP(s)/Active Directory)
- Node-to-node encryption through SSL/TLS (Transport layer)
- Secure REST layer through HTTPS (SSL/TLS)
- X-Forwarded-For (XFF) support
- Audit logging
- LUKS Disk encryption at rest (bare metal installs only recommended)

6.1 FIREWALL SETTINGS IF ISOLATED SIEM MULTI NODE CLUSTER

Source (End Points)	Destination	Port & Transport
NxLog Agent	Proteus	3520-3525 TCP
OSSEC Wazuh Fork Agent	Capricorn	1514 UDP
Syslog (Network Appliances)	Proteus	514,1514 UDP/TCP
Source	**Destination**	**Port**
Proteus	Kraken/Tiamat	9300-9400 TCP
Kraken/Tiamat	Proteus	9300-9400 TCP
Proteus	Capricorn	12201-12205 TCP/UDP 80, 443, 12900 (Graylog)
Capricorn	Proteus	3520 TCP (Filebeat) 3526-3530 (Graylog Outputs)
Source (Admin Desktop)	**Destination**	**Port**
Security Administrators	Proteus / Capricorn	22 TCP (SSH) 443 TCP (Kibana) 80 TCP (Kibana) 8080 TCP (Graylog) 443 TCP (Kibana) 8443 TCP (FIR) 15672 TCP (RabbitMQ) 55000 TCP (Graylog)
Security Administrators	Kraken	22 TCP (SSH)
Security Administrators	Tiamat	22 TCP (SSH)

Note: Internet access for Proteus, Capricorn Kraken, Tiamat is required for daily rule updates via secure Internet gateway. These are just recommendations to protect your SIEM

6.2 FIREWALL SETTINGS FOR CLOUD SIEM AS A SERVICE

Source (End Points)	Destination	Port & Transport
NxLog Agent	Hydra	3520-3525 TCP
OSSEC Wazuh Fork Agent	Hydra	1514 UDP
Syslog (Network Appliances)	Hydra	514, 1514 UDP, TCP
Source (Admin Desktop)	**Destination**	**Port**
Security Administrators	Hydra	22 TCP
Kustodian via VPN or SSH	Hydra	VM Security updates

VPC connection to AWS is required for Hydra to connect to SIEMONSTER