BUI

INNOVATION
DELIVERY
RESULTS

CyberSOC

AFRICA'S NO 1 MICROSOFT CLOUD PARTNER

BUI INNOVATION DELIVERY RESULTS

Your Journey Today

- What is a Security operations Centre and Security information and event management (SIEM)
- Expanding Digital Estates and traditional SOC challenges
- Introducing The BUI Cyber Security Operations Centre
- Why BUI Cyber SOC?
- How is this service billed?
- BUI Cyber SOC Service Level Offerings

What is a Security operations Centre (SOC) and Security information and event management (SIEM)

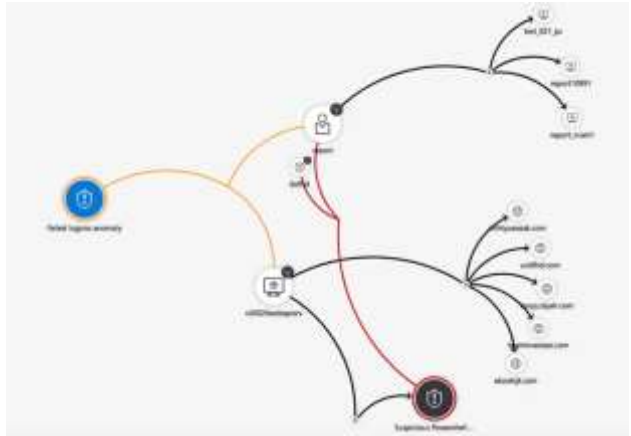
BUI INNOVATION DELIVERY RESULTS

What is a SOC (Security Operations Centre)

A security operations centre (**SOC**) is a facility that houses an information security team responsible for monitoring and analysing an organization's security posture on an ongoing basis.

Security operations centres monitor and analyse activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise.

The SOC team's goal is to detect, analyse, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.



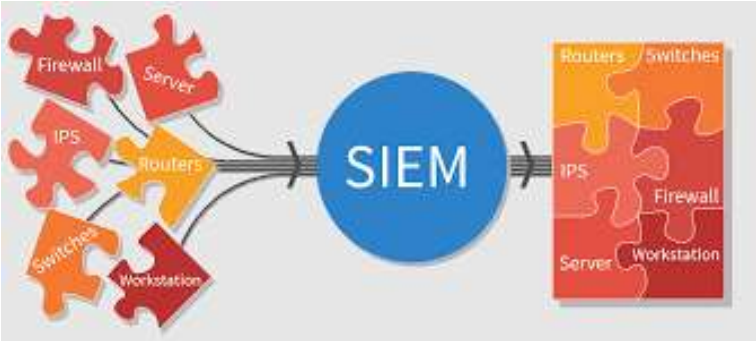
Security operations centres are typically staffed with security analysts and engineers as well as managers who oversee security operations.

SOC staff work close with organizational **incident response** teams to ensure

BUI INNOVATION DELIVERY RESULTS

What is SIEM (Security information and event management)

Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

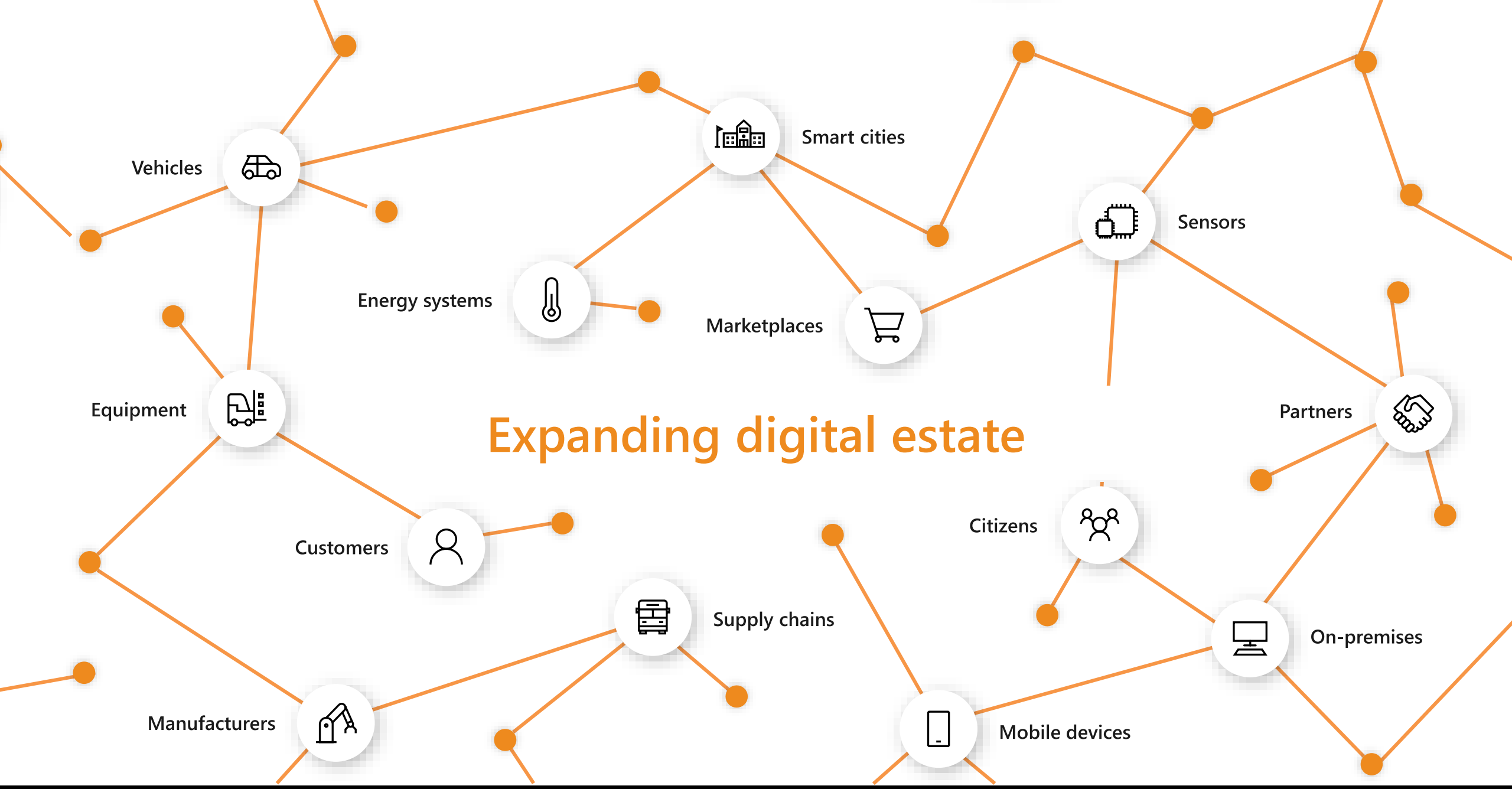


SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers and network equipment, as well as specialized security equipment, such as firewalls, antivirus or intrusion prevention systems (IPSes).

The collector's forward events to a centralized management console, where security analysts sift through the noise, connecting the dots and prioritizing security incidents.

SIEM software enables organizations to detect incidents that may otherwise go undetected. The software analyses the log entries to identify signs of malicious activity. In addition, since the system gathers events from different

Expanding Digital Estates and traditional SOC challenges



Expanding digital estate

Traditional SOC Challenges

- Sophistication of threats
- High volume of noisy alerts
- IT deployment & maintenance
- Rising infrastructure costs and upfront investment
- Too many disconnected products
- Lack of automation
- Security skills in short supply

Introducing
BUI's Cyber Security Operation Centre

BUI
INNOVATION
DELIVERY
RESULTS

SOUTH AFRICA'S NO 1 MICROSOFT CLOUD PARTNER

BUI INNOVATION DELIVERY RESULTS

What is BUI's Cyber SOC?

BUI Cyber SOC is backed by Microsoft Sentinel and is ideal for any organization that is looking to reduce security breaches and improve threat detection.

The BUI CyberSOC monitors your entire IT security landscape, including On-premise, Cloud, Devices, Applications, Networks, Infrastructure and Users.

The BUI CyberSOC provides a comprehensive and specialized Managed SOC service which runs on Microsoft Security technology, powered by modern Artificial Intelligence (AI) based infrastructure, which provides full security services around Compliance Reporting, Database, Infrastructure, Access Monitoring, Real-time Threat Monitoring and much more.

Managed and monitored by highly skilled cyber security professionals provided to you, as a service with near to no infrastructure requirements.

Providing a birds-eye view across your enterprise

- ✓ Highly secured physical facilities
- ✓ Cyber Security professionals
- ✓ 24/7 operation
- ✓ Flexible Usage based billing
- ✓ Custom and policy-based detection
- ✓ Infinitely scalable
- ✓ Ability to process billions of events per day
- ✓ Up to 90 days storage included

BUI INNOVATION DELIVERY RESULTS

Overview

BUI CyberSOC is ideal for any organization that is looking to reduce security breaches and improve threat detection.

Invest in security, not infrastructure

The BUI CyberSOC provides a proactive 24/7 managed security service backed up by powerful AI based Cloud Technology with dedicated skills focusing on real-time analysis security alerts.

With committed resources and highly scalable AI detection pattern matching to reduce noise and enhanced analysis for your unique security landscape.

Never again let a storage limit or a query limit prevent you from protecting your enterprise. The nature of our service allows your organization to eliminate infrastructure costs by automatically scaling your resources in a for-use consumption model, allowing you to scale as required.

BUI INNOVATION DELIVERY RESULTS

Features

Reduce infrastructure costs by automatically scaling resources and only paying for what you use.

Simplified SecOps for faster threat response

Our consultants are dedicated to the management of the BUI CyberSOC by providing highly skilled cybersecurity resources to manage our world class infrastructure, the BUI CyberSOC is backed-up and protected by globally available Microsoft Security Technology in your region.

Detection
Threat detection is smarter and faster

Reducing Noise
The focus is on finding real threats, daily, and minimizing false positives

Custom
Pre-built queries based on years of security experience

Patterns
Previously uncovered threats can be detected

Technology
Built-in machine learning backed by world-class Microsoft Technology

Analysis
BUI's SoC provides monitoring and alerting and, if enough data is collected, an analysis of the attack.

BUI INNOVATION DELIVERY RESULTS

Features

No storage or query limits: BUI CyberSOC offers scale to meet your organizational needs.

BUI CyberSOC is Technology agnostic

Azure Cloud Data Sources	On-premise ad other CSP Data Sources
Application	AWS
Azure Platform	GCP
PAAS	On-Premise
VM's / NVA	Other Clouds
Microsoft and Office 365	

Multiple data sources are used to monitor your environment and can integrate with existing tools (including business applications, other security products or even homegrown tools) to ensure robust security management.

Data can be stored in a data center near you.

Personal Identifiable Information (PII) and other evolving data privacy laws allows you to use local cloud services and provides the opportunity for your enterprise to store security related information in a region or country of your choosing. Data residency is a key benefit of our solution with built-in Redundancy and Disaster Recovery capabilities, so that your business which might be bound by

How is this service billed?

BUI INNOVATION DELIVERY RESULTS

How is this billed

The BUI Cyber SoC is billed based on each client's usage, lowering the barrier to entry and overall costs and allowing for virtually unlimited capacity.

Billing Model Example

Ingestion of logs. 152GB per Month (**5GB Per day) $633.10**

+

Service Level Agreement **Silver $1400.00**

+

Total $2033.10 Per Month

- Sold in four Versions Bronze, Silver, Gold and Platinum
- BUI uses its Tier One CSP – Clients and billed Monthly
- BUI uses Microsoft Sentinel as its SIEM to run its SoC

Note:

No Take on Costs

No Software Costs

Bronze	Silver	Gold	Platinum
Business hours	Extended Business Hours	24/7/365	24/7/365
Free 90 Day storage 8/5 monitoring	Free 90 Day Storage 12/5 monitoring Remote Monthly Review	Free 90 Day Storage 24/7 monitoring In person Monthly Review	Free 90 Day Storage 24/7 monitoring In person Monthly Review Additional Services
*Costs are based and calculated based on Data ingestion	*Costs are based and calculated based on Data ingestion	*Costs are based and calculated based on Data ingestion	*Costs are based and calculated based on Data ingestion

BUI Cyber SOC Service Level Offerings

	Bronze (Notification Service)	Silver	Gold	Platinum
PURPOSE OF THIS OFFERING	Basic entry level notification-based service for SME and small customer. Could also be used as a POC for one of the larger offerings	Primary SOC offering- For large customers who require intense security monitoring		Very focused SOC service for highly secured environments
* Consulting Support	Not included - but paid-for consulting will be available or customers can opt to use existing SLA (L2-L3 support)	4 hours of SLA security consulting support per month	Total of 8 hours of SLA security consulting support per month	Up to 24 hours of incident support per month. Security consultants to assist with incident response
Hours of Operation - Active Monitoring	Office hours - 08h00-17h00 (Mon - Fri)	Extended office hours (GMT+2) *** (Mon - Fri)	24x7x365	24x7x365
Notification Methods	Automated email from Sentinel	Automated email from Sentinel & SMS notifications	Automated email from Sentinel & Teams or SMS notifications Flow-based automated notifications Team site for reports and collaboration	Automated email from Sentinel & Teams or SMS notifications Flow-based automated notifications Team site for reports and collaboration
Hunting	1 hour hunting per week / systems maintenance	2 hours total hunting per week / sys maintenance	8 hours total hunting per week / sys maintenance	12 hours total hunting per week / sys maintenance
Meetings	Monthly Teams meeting (Exec overview - limited reporting)	Monthly Teams meeting & system generated reports	Onsite monthly meeting with reports	Onsite monthly meeting with reports
Log Ingestion per day	No minimum	Minimum 20 GB per day	Minimum 40 GB per day	Minimum 60 GB per day
Licensing	CSP-BUI (Min PAL) **	CSP-BUI (Min PAL) **	Must utilize BUI CSP	Must utilize BUI CSP
Additional Services			Guidance in handling breaches with security incident management	Assistance and guidance with security incident management
Advisory Services			Vulnerability assessment - yearly	Vulnerability assessment - quarterly One external penetration test per year
Incident Management	Not included but can be provided via consulting contract or existing SLA (if available)	Not included but can be provided via consulting contract or existing SLA (if available)	Assistance to remediate breaches *	Assistance to perform root cause analysis and remediation of breaches
Microsoft Secure Score	Reporting on	Reporting on	Advisory services to improve Secure Score	Advisory services to improve Secure Score as well as consulting assistance to implement Secure Score
Management Assistance			Account manager managed	Account manager managed
Forensic Services	Not included	Not included	Not included	Guidance and advice given to conclude Forensic analysis
BUI CyberSOC Management Fee	CSP Log Ingestion Costs Only	From US$ 1,400.00 per Month + Log Ingestion	From US$ 3,200.00 per Month + Log Ingestion	From US$ 4,600.00 per Month + Log Ingestion

Visit bui.co.za/soc for updated Terms and Conditions

* Consulting support for security-related SOC incidents or any customization relating to Sentinel. Any additional hours used will be charged for at preferential SLA rates

** Customers using EA licensing incur additional 5% monthly management fee

*** Extended office hours 06h00 until 19h00

Note : Minimum requirement is a new subscription for Sentinel (Silver, Gold and Platinum tiers)

LET'S TALK

WWW.BUI.CO.ZA

+27 (0)87 740 2400
info@bui.co.za

SOUTH AFRICA

JOHANNESBURG

Head Office
Second Floor, Microsoft Corporate Hill,
3012 William Nicol Drive, Bryanston

CAPE TOWN

Harbour Bridge, Roggebaai Canal,
Lower Long St,
Cape Town City Centre

DURBAN

Unit 13, Braehead Office Park,
1 Old Main Road, Kloof
Kwazulu-Natal

USA

CALIFORNIA

530 Technology Dr., Suite 100 & 200,
Irvine, California, 92618
United States of America