Digital Insights

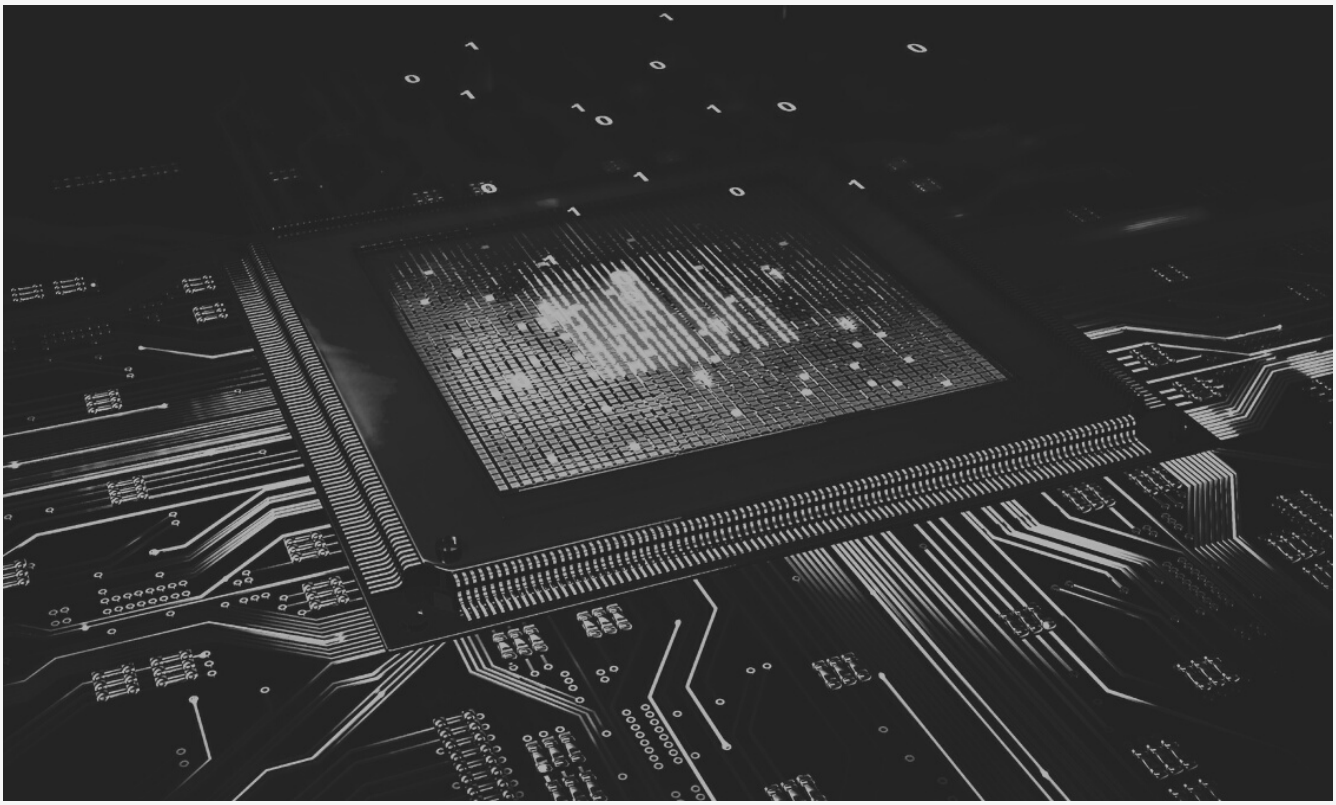
TRIAGE INVESTIGATE REPORT

SOC AS A SERVICE

BE AWARE. BE SECURE

WATCHTOWER365

SECURITY



UNIQUE SAAS MODEL

- Security Information and Event Management
- Network Monitoring
- Incident Response & Remediation
- Vulnerability Assessment & Penetration Testing

KEY BENEFITS

- 24/7/365 Security Monitoring
- Threat Detection
- Incident Response
- Threat Intelligence Analysis
- Compliance Management
- Security Testing

A COMPLETE CYBERSECURITY PACKAGE!

ONE UNIFIED SOLUTION

WatchTower 365 (SOC as-a-Service) helps support compliance with a rule by providing multiple essential security capabilities in a single solution, enabling you to satisfy many of the ‘reasonable steps’ outlined by the rule to accelerate investigations into suspected breaches to meet the 30 calendar - day window.

- Asset Discovery
- Vulnerability Assessment
- Intrusion Detection
- Incident Response
- Behavioural Monitoring
- Integrated Threat Intelligence
- Network Traffic Analysis
- Endpoint Detection & Response
- Compliance Reporting
- Penetration Testing

SIEM

SECURITY INFORMATION & EVENT MANAGEMENT

SIEM (AlienVault USM) is a component that includes integrated asset discovery & inventory via passive & active scanning tools and allows for the assignment of asset criticality. We conduct vulnerability scanning, reporting, and management of vulnerability stats, to assist customers in addressing the most critical items.

This is performed both internally (authenticated) from AlienVault USM, and externally (unauthenticated) from the WatchTower 365 Managed Security Services. This information, integrated with SIEM, feeds to refine threat detection and analysis and reduce false positives.

The Threat Detection and Alerting abilities of AlienVault USM solution provides:-

- A fully-managed network and host-based IDS technology with leading industry threat feeds and rule-sets.
- Integrated proprietary and crowd-sourced threat intelligence.
- Ability to deploy additional integrated security controls.
- File integrity and privileged-user monitoring, etc.
- Automated real-time "unified" log correlation.
- Integration of all available security data (IDS, security device inputs, asset value database, vulnerability scan data).
- Application of 3,200+ correlation rules to asset, vulnerability, network traffic, and threat data.
- 24 x 7 x 365 alerting with "full threat context".
- Linkage to all log data related to the threat.
- Evaluation and elimination of systemic "false positives".

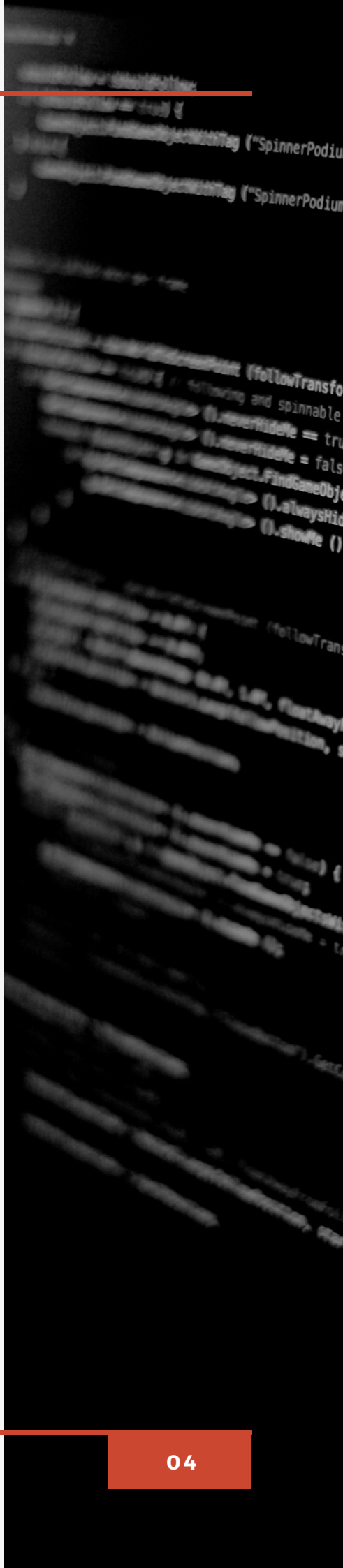
The Archival Log Storage and Search Functionality of WatchTower 365 Managed Security Services solution provides:-

- All collected security logs and forensically "stamped" and sent to a separate onboard "logger" database.
- Provides for long-term archival log storage to address compliance requirements.
- Enables efficient historical log search functionally for security forensics, event analysis, and reporting.

NETWORK TRAFFIC ANALYSIS

Network Monitoring is a component of WatchTower365 SoC-in-a-Box solution that provides web-based network traffic analysis and network flow collection.

- Sort network traffic according to many criteria including IP address, port, protocol, throughout, Autonomous Systems (AS)
- Show real-time network traffic and active hosts
- Produce long-term reports for several network metrics including throughput and application protocols
- Monitor and report live throughput, network and application latencies, Round Trip Time (RTT), TCP statistics (retransmissions, out of order packets, packet lost), and bytes and packets transmitted
- Store on disk persistent traffic statistics to allow future explorations and post-mortem analysis
- Geolocate and overlay hosts in a geographical map
- Alerts engine to capture anomalous and suspicious hosts
- SNMP to v2c/v3 support and continuous monitoring of SNMP devices



RAPID RESPONSE TO INCIDENTS

As we implement our Business Continuity plans and reset our corporate priorities to deal with the pandemic, it is important to keep cybersecurity in the forefront. We will be relying more heavily than ever on our IT systems to keep our businesses moving forward and cybersecurity plays a critical role in keeping those systems up and running.

It's important to understand the one defining reality of cyber security today. Defences fail. You can't prevent all attacks. The layering of numerous defensive solutions has been publicly proven to fail in protecting enterprises from being breached.

You must change your mindset. Security should be approached with the acceptance that adversaries have breached your defences. Therefore, the goals should be to reduce the dwell time of adversaries inside your network, to find them as quickly and effectively as possible, and to take the appropriate actions to protect your environment - now and in the future.

Once deployed on your network the threat hunting tool inspects each endpoint, hunting threats that have evaded real-time prevention technologies. Both the agentless and agent-based options communicate with the central console and offer enterprises the flexibility of permanent agent-based access to endpoints or deploying a scanner to inspect agentless endpoints in sensitive network segments. The threat hunting platform consists of a central hosted console, a forward deployable scanner and/or endpoint agents, dissolvable surveys, and an advanced cloud-based threat intelligence & analysis engine.

Threat Hunting with the tool involves 5 steps:

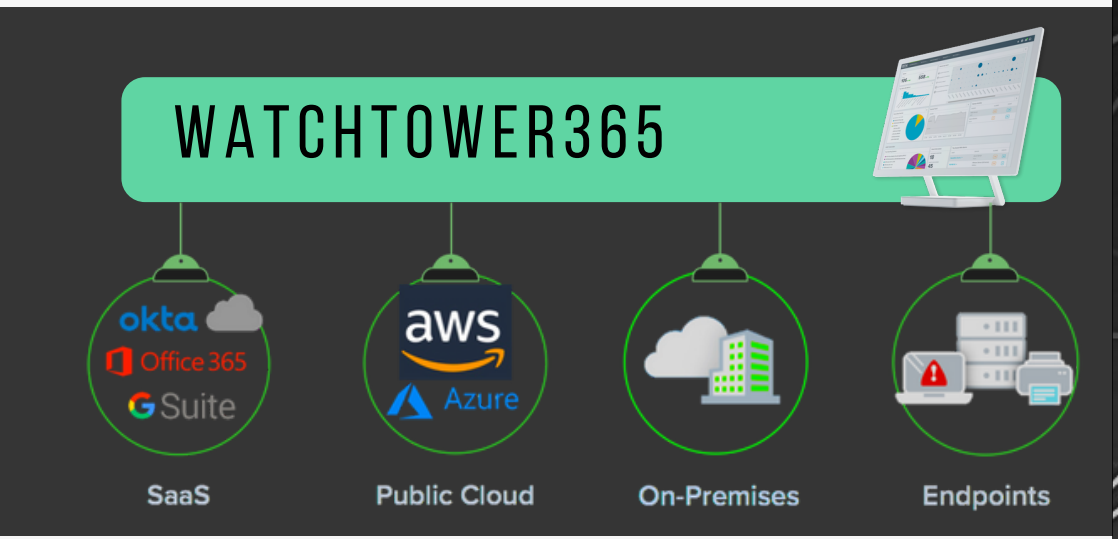
- Collect: Endpoint surveys periodically collect forensic data and inspect volatile memory for changes to the state of each system

- Enrich: The collected data is sent to the console which enriches, analyses, and scores the data with threat intelligence and reputation

- Triage: Advanced threat hunting specific workflows such as data stacking, pivoting, and hunt-specific machine learning algorithms score the data

- Investigate: Analyse suspicious malware samples, commands in memory, and other activities to find what signatures and intelligence fail to classify

- Respond: Killing malware and locking down compromised accounts



COMPLIANCE REPORTING:

HIPAA COMPLIANT · AICPA SOC · PCI DSS COMPLIANT · ISO 27001 Certified · amazon web services Partner Network ADVANCED TECHNOLOGY PARTNER SECURITY COMPETENCY · Microsoft Azure Certified

USER ENTITY BEHAVIOR ANALYTICS (UEBA)

U - More user-centric security monitoring, and less user-related.

E - Analyses entities in addition to Users, including, but not limited to: virtual instances, devices, data repositories, and more.

B - Focuses more on user behaviours and activities, and less on static parameters.

A - Advanced analytics rather than simple rule-based matching.

What does UEBA do?

UEBA monitors the behaviour of users who have access to entities, which includes various user accounts and endpoints. It then analyses this data against a baseline to determine if a particular activity is anomalous or suspicious.

- Simplifies investigations while including a human component
- Directs security practitioners to a starting point
- Reduces alert fatigue and adds context

Adding UEBA to USM Anywhere adds additional context to Alarms, making it faster and easier to detect threats across environments.

USM Anywhere UEBA Focus on Cloud:

- USM Anywhere's cross-cloud, out-of-the-box security presence remains a leader
- Our Alien Labs team is currently focusing on cloud analytics and cloud security
- Traditional SIEMs with UEBA solutions primarily track on-premise UEBA

Google Cloud aws Microsoft Azure

AT&T Cybersecurity areas of UEBA coverage:

- **PLATFORM: Cloud and Application:**
  - Monitor cloud user accounts and identifies restricted application areas.
  - Identify areas lacking expected security rules and configurations.

- **SYSTEMS: Endpoint and Network:**
  - Endpoint activity logs can help match identity and access anomalies to user accounts.
  - Login anomalies, persistent SSH sessions, unusual traffic times, and the sharing of credentials.

- **IDENTITIES: Access and Authentication:**
  - User access from unusual devices, unexpected user access to critical servers, and dormant user accounts suddenly active.

WATCHTOWER365

Digital Insights

Triage Investigate Report

PAYBACK IN UNDER

3 MONTHS

80%

IMPROVEMENT IN THREAT DETECTION AND INCIDENT RESPONSE TIME

80%

IMPROVEMENT IN SECURITY OPERATIONS STAFF PRODUCTIVITY

2000

HOURS SAVED PER AUDIT

= 94% REDUCTION

£40,000+

ANNUAL SAVINGS IN THREAT INTELLIGENCE EXPENSE

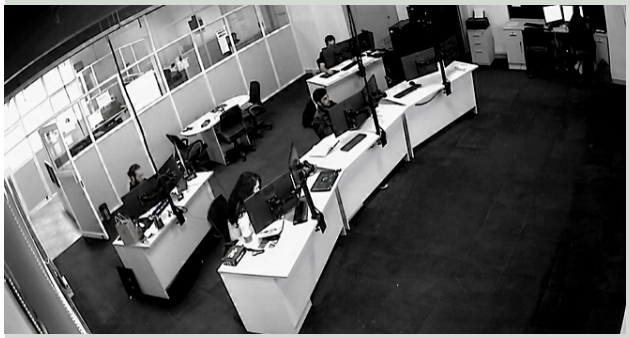
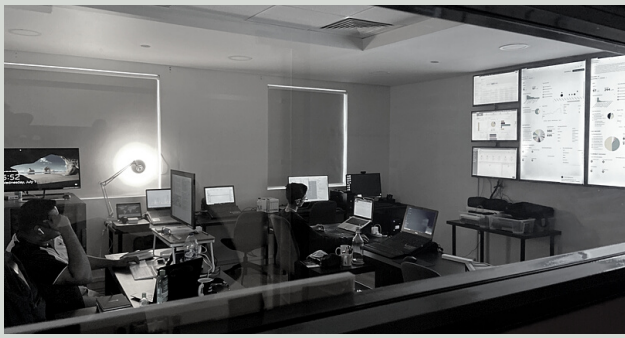
6x

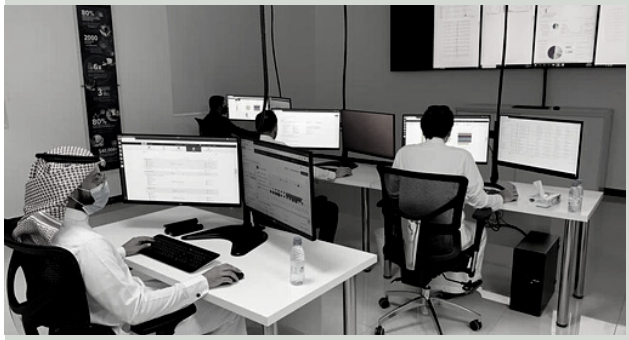
RETURN ON INVESTMENT

BE AWARE. BE SECURE

Digital Insights

TRIAGE INVESTIGATE REPORT


Suite 4-5 Acorn House, Midsummer Boulevard,
Milton Keynes, MK9 2UB, UK

Web: www.dic-uk.com
Email: lisanne@dic-uk.com | contact@dic-uk.com