FUJITSU
shaping tomorrow with you

User Entity & Behaviour Analytics Services

Insider threats are a growing concern for defence organizations around the world, especially in the wake of high-profile insider breaches like the infamous data theft by Edward Snowden. A number of governments are going so far as to act on the insider threat vector through policy or regulation. However, effectively fighting insider threats is complex and difficult. Fujitsu's User Entity & Behaviour Analytics Service provides organisations a key differentiator in their security posture and ability to mitigate these ever growing threats that are increasingly getting more prevalent and malicious.

With Fujitsu's User Entity & Behaviour Analytics (UEBA) Platform & Services, we provide you with the core components for the speedy, detection, intelligence and alerts to enable fast response and remediation of security incidents in addition to enabling retrospective analysis to support security investigations and compliance requirements.

User Behaviour Intelligence Platform

- **User Visibility:** A lightweight collector captures complete audit trails in real-time. It is scalable, privacy-conscious, and provides online and offline visibility
- **User Behaviour Intelligence:** Advanced intelligence pinpoints suspicious user behaviour as well as both "known-bad" behaviour patterns and baselines normal behaviour to detect anomalies
- **Analytics:** Machine learning baselines individuals' normal user behaviour and alerts on suspicious anomalies or red flags
- **Actionable Alerts:** Produces alerts based on an entity's risk score. This "alert stacking" means that analysts only receive an alert when the user's total risk score reaches a pre-defined threshold, reducing noise and false positives.

The traditional approach to cyber security has been to use a prevention centric strategy focused on blocking attacks. This approach has had limited success in recent years especially as threat actors techniques, tactics and processes have evolved to evade these less agile strategies.

Detecting and stopping insider threat attacks as early as possible in the cyber-attack life cycle is a key deliverable of any threat lifecycle management programme where an integrated detect and response strategy is being deployed.

Business-affecting incidents and data breaches can be largely avoided if businesses detect threats early in the threat management lifecycle and respond quickly, reducing costly damage clean-up exercises.

Monitor Privileged Users

Fujitsu's UEBA Services allows organizations to monitor privileged users without limiting their productivity.

Privileged and administrative users are often be the most difficult to catch, as they cannot be restricted by lock-and block policies. Our approach however is to catch privileged malicious actors because it relies on visibility and analytics at the user-level, not broad rules or blocking. Unlike log-based

monitoring tools, our UEBA platform collects data straight from the endpoint – so it captures the data you need in order to catch advanced data theft, including every application used, every window open, all file and folder activity, all web activity, and more.

It then establishes a baseline of normal behaviour for every user. There is no need to develop special rules, which means that privileged users are covered the same as every other employee. When a privileged user behaves suspiciously, they will be alerted immediately.

Achieve Security Off the Network

Fujitsu's UEBA Services provides endpoint-based visibility that does not go dark when the user leaves the network.

With the rise of remote work and portable technology, organizations can no longer rely on perimeter security to protect extremely sensitive data. Our UEBA platform provides user behaviour visibility directly from the endpoint itself, giving you visibility into devices even when they are off network (like at home or a coffee shop).

Stop Phishing and Infiltration

Fujitsu's UEBA Services monitors and baselines behaviour patterns that immediately alert on signs of external infiltration.

Our UEBA platform's ability to detect and alert on suspicious anomalous behaviour also allows it to detect when an outside attacker has compromised a user's account. When a user exhibits wildly unusual behaviour, combined with red flags like privilege escalation or lateral movement, it alerts on compromised credentials for immediate remediation.

Fujitsu UEBA Services offer

- A managed CRC Service for triaging and incident management
- 24/7 monitoring
- Secure UEBA Management services
- UEBA as a Service - supply, integration and management
- Optional advanced remediation actions

Fujitsu's Comprehensive UEBA Services

Our service offers the ability to detect Insider Threats at every stage of the cyber kill chain

- **Reconnaissance** – The attacker does research in preparation to steal data
- **Circumvention -** The attacker circumvents security to exfiltrate data
- **Aggregation -** The attacker collects the data that they intend to steal
- **Obfuscation –** The attacker covers their tracks
- **Exfiltration –** The data leaves your organization
- **End-to-end monitoring and response** on a 24 x 7 basis, backed by Service Level Agreements

- **Typical Engagement profile**
  - Platform is installed on your network or cloud
  - First day – Platform begins baselining & identifying high risk user activities
  - Three Months – The platform gets better at identifying anomalies as it learns your user baselines through machine learning
  - Ongoing – Expert analysis helps with ongoing tuning, investigations & alert triage

Summary of features:

User Entity & Behaviour Analytics (UEBA) as a Service	Standard	Optional
Install: Install Server & Endpoint agents	✓	
Scan: Scan endpoint behaviour & begin baseline formulation	✓	
Remediation Report: Report on identified threats & score based on client priorities as well as threat severity	✓	
Advanced Remediation Action: In conjunction with Client, remediate identified threats for managed service, triage, investigation, classification and reporting of events and incidents; including standard SLA's		✓
Integration into SIEM tool		✓

Service Levels

In today's business world, security is a 24*7 requirement; Fujitsu provides around the clock service availability with a number of service level options designed to meet specific business needs.

Fujitsu's Cyber Resilience Centre (CRC)

Fujitsu's state of the art CRC provides a focal point for:

- The co-ordination of security monitoring and security incident management
- Providing situational awareness through the broad view of the security threat landscape due to the breadth of the Fujitsu Client base and the links with Cyber Security agencies and strategic technology partners
- The ongoing support and tuning of the technology platforms to enable the service to retain current against the emerging security threat
- Security event and incident related information to better enable risk mitigation
- Expert security advice and reporting
- Compliance assessment and support of associated reports and remedial actions
- Fujitsu's Advanced Remediation includes options such as - Incident response, Incident Management, End-User blocking, Endpoint re-imaging, end-user education etc...
- Fujitsu's Automation & Orchestration Services allow for full policy based control for clients with the ability to monitor, remediate and quarantine suspicious activity 24*7 seamlessly at machine speed

Benefits

Efficiency

- Reduction in time to detect threats
- Accelerate the speed to respond to threats
- Proactive services that can mitigate threats as they arise

Cost Savings

- Reduces the cost of hiring, training and retaining high quality security professionals
- Flexible aaS model can reduce capex expenditure
- Directs spend to appropriate controls and activities

Security

- Details difficult to detect insider threats
- Enables breaches to be detected or avoided and improves incident handling and containment
- Monitors the effectiveness of security controls
- Streamlines the auditing and reporting of compliance obligations
- Provides information to better inform risk management decisions

CONTACT FUJITSU
Email: cybersecurity@au.fujitsu.com

Address:
Lvl 3,4 National Cct
Barton, ACT 2600
Australia
Tel: +61-2-6250-9600