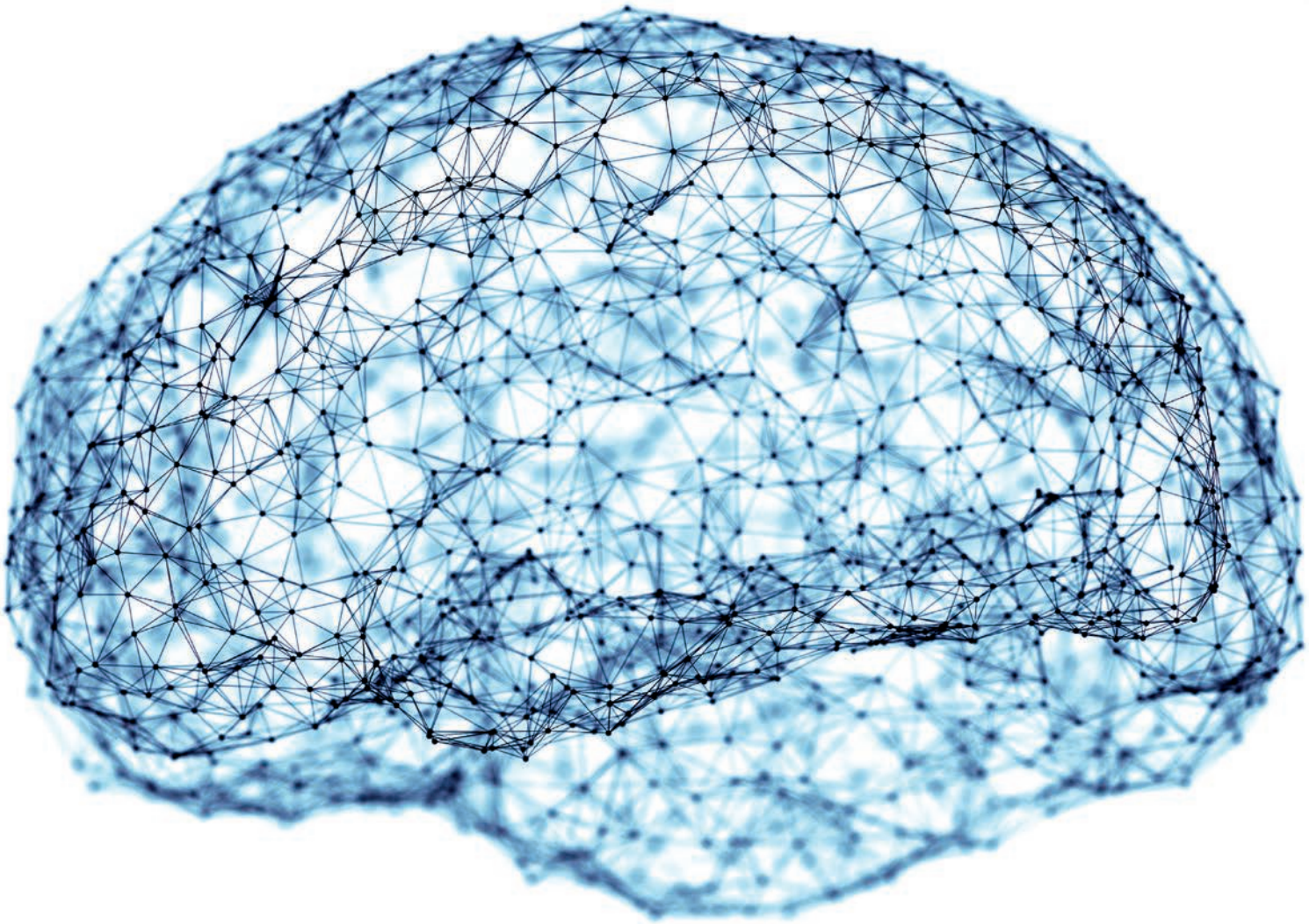
CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE
OF TECHNOLOGY



AECID – AUTOMATIC EVENT CORRELATION FOR INCIDENT DETECTION

Intelligente Sicherheitstechnologien basierend auf modernen Machine Learning Mechanismen

CYBER SECURITY INTELLIGENCE TOOL

"AECID" steht für „Automatic Event Correlation for Incident Detection" und ist ein intelligentes Cyber Security Tool, das anhand spezieller mathematischer Berechnungen abnormales von normalen Verhalten in komplexen Rechnernetzen unterscheiden kann.

Im Gegensatz zu herkömmlichen Systemen braucht der Algorithmus keine spezifische Kenntnis über die zu überwachenden IT-Systeme. Vielmehr erfolgt eine reine Mustererkennung nach entsprechender Beobachtungs- und Lernzeit durch einen selbstlernenden Algorithmus.

Die AIT AECID Technologie passt sich dadurch kontinuierlich an neue Situationen an und benötigt keine aufwändige Spezifikation des technischen Systems und kein kompliziertes „Konfiguration Management" des Betreibers. Indem AECID laufend neue Informationen aufnimmt und analysiert, erweitert und verfeinert das Tool selbstständig und kontinuierlich die eigene Wissensbasis hinsichtlich neuer Erkenntnisse über das System, in dem es eingesetzt wird.

Je mehr Daten AECID sieht, desto mehr lernt es. Durch dessen Anpassungsfähigkeit, hat selbst maßgeschneiderte Schadsoftware keine Möglichkeit, sich vor AECID zu verbergen. Sobald eine abnormale Verhaltensänderung innerhalb der Systemumgebung stattfindet, identifiziert AECID Systemabweichungen von den gelernten Normalzuständen und warnt über eine mögliche Bedrohung. Änderungen im System, die sich nicht als Bedrohung herausstellen, werden im laufend wachsenden AECID-Verständnis als Systemnormalität gespeichert.

Im Gegensatz zu herkömmlich definierten Regeln für die Überwachung eines IT-Systems ist AECID in der Lage, über die Analyse vieler unterschiedlicher Indikatoren aus verschiedenen Quellen, Standorten und Zeitpunkten einen realistischen Hinweis auf eine echte Bedrohung zu berechnen. Auf diese Weise werden die Spezialisten nicht mit der Bearbeitung von falsch-positiven Alarmen blockiert.

LEISTUNGSMERKMALE DER IM EINSATZ BEFINDLICHEN VERSION VON AECID

Die derzeitige Implementierung der AIT AECID Technologie basiert auf einer Logdatenanalyse. Die Logdatenanalyse zur Erkennung von Sicherheitsvorfällen hat in einigen Bereichen klare Vorteile gegenüber der Nutzung von Netzwerkdaten:

- Keine Analysebibliotheken für alle am Netzwerk gesprochenen Protokolle notwendig, stattdessen Nutzung der Logdaten der involvierten Programme.

- Keine aufwändige und risikobehaftete Entschlüsselung von verschlüsselten Netzwerkprotokollen notwendig.

- Kostengünstigere Analyse bei Alt/Legacysystemen, bei denen sich aufgrund der geringen Zahl bzw. nicht mehr vorhandener Dokumentation die Implementierung spezifischer Bibliotheken zur binären Netzwerkdatenanalyse nicht mehr rentieren.

- Rechenzeitgünstigere Analyse, da in Logdaten üblicherweise besonders wichtige Ereignisse und Informationen protokolliert werden, man auf der Netzwerkebene aber den gesamten Datenstrom zerlegen und diese Elemente erst extrahieren muss.

- Logdatenanalyse kann nicht nur kommunizierte Daten berücksichtigen, sondern auch den internen Zustand der beteiligten Systeme. So kann z.B. am Netzwerk nur erkannt werden, dass ein Server einen Loginversuch abgelehnt hat, aus den Logs wäre aber auch gleichzeitig zu erkennen, warum. Ein falsch eingetipptes Passwort als Grund könnte erwartbar und normal sein, ein gesperrter oder gelöschter Account oder sonstige Fehlerursachen nicht. So kann die Wahrscheinlichkeit des Passwortvertippens unterschiedlicher Nutzer ermittelt werden. Da der Nutzer „backup" sich automatisiert anmeldet und sich daher nie vertippt, würde schon ein einziger Fehlversuch eine signifikante Abweichung darstellen.

- Unser Ansatz erlaubt eine Anpassung der Regeln an das jeweilige Betriebsumfeld. So kann z.B. erkannt werden, dass die erfolgreiche Anmeldung eines Nutzers immer nur von gewissen Rechnern aus erfolgt. Zugriffe von anderen Maschinen sind daher potentiell verdächtig.

EINFACHE INTEGRATION IN VORHANDENE SYSTEME

Die Eine Besonderheit der modernen AIT AECID Technologie ist die einfache Einbindung in vorhandene IT- Infrastrukturen und entsprechende Betriebsprozesse. Da eine Musteranalyse erfolgt, ist keine detaillierte Kenntnis über die konkreten IT-Systeme für die Konfiguration notwendig. Vorteile sind damit:

- Integration in bereits bestehende Sicherheitsinfrastruktur: unsere Lösungen agieren als weitere Sensoren und melden erkannte Abweichungen an die bereits etablierten Systeme, also z.B. die SIEM (Security information and event management) -Lösungen. Damit können auch die bereits etablierten Incidenthandlingprozesse beibehalten werden.

- Nutzung der in Produktionsfeldern häufigen zentralen Logdatenaggregation als einfach anzuzapfende Quelle von Logdaten. Dadurch kann meist eine aufwändigere verteilte Installation vermieden werden.

- Automatisierte Erkennung der Logdatenstruktur zur Extraktion der analyserelevanten Daten aus den Logeinträgen zur Reduktion des menschlichen Aufwands beim Einbinden neuer Quellen.

- Spezielle Implementierungen mit geringsten Leistungsanforderungen an das Zielsystem sind z.B. zur internen Überwachung von Embedded-Devices möglich.

BEISPIEL VON MÖGLICHEN AUSWERTUNGEN DURCH DIE AECID TECHNOLOGIE

- Network Interaction Graph Analyse: welche Maschinen kommunizieren miteinander

- Authentication Interaction Graph: wer meldet sich von welcher Maschine wo an, mit welchen Credentials/Key Fingerprints)

- Syscall Audit Anomalieerkennung: Erkennen von atypischen Abläufen wie z.B. Admin-Fehlverhalten, Software-Fehlfunktion, Angriffen, aber auch von unsicheren Software- & Fehlkonfigurationen

WEITERENTWICKLUNG IM PLAN MIT ZUGESICHERTEN FORSCHUNGSMITTELN 2017+

Nutzung der Technologie in Industrieautomatisierung/SCADA (Supervisory control and data acquisition) mit besonderem Fokus auf kritische Infrastruktur.

REFERENZEN

Mehrere Validierungsprojekte sind derzeit in Betrieb. Folgende Proof of Concept (PoC) Projekte sind beispielhaft angeführt:

INTERN AM AIT

AECID ist am AIT auf einem zentralen Remotesysloggingserver im Einsatz. Dort werden Logs von 25 Servern aus 4 Zonen (DMZ, interne Services, 2 Entwicklungszonen) zusammengeführt. Das Volumen beträgt ~1GB Logdaten/Tag entsprechend 4 Mio Zeilen.

Zum Beispiel wurden konkrete Sicherheitsmängel identifiziert: Weiterführende Informationen zum Thema „Sicherheitsvorfälle erkennen am Beispiel von Linux Syscall-Audit-Logs" sind in den Präsentationsunterlagen der IT-SecX-Konferenz zu finden: https://itsecx.fhstp.ac.at/wp-content/uploads/2016/11/06_RomanFiedler_SyscallAuditLogMining-V1.pdf (die identifizierten bisher unentdeckten Schwachstellen haben u.a. folgende CVE-Nummer erhalten: CVE-2016-8649).

SPEZIELLER ANWENDER-POC

Für einen Kunden mit extrem hohen Sicherheitslevel haben wir einen PoC laufen, bei dem der Schwerpunkt auf einer Linux Syscall-Audit-Logs Analyse liegt.

POC BEI EINEM GROSSEN MOBILFUNKPROVIDER

Installation von AECID in einer Testumgebung. Konfiguration und Adaption erfolgt durch den Kunden aus einer ausgewählten Menge von Produktionssystemen. Ziel der Installation ist es, die Prozessintegration bei einem Netzbetreiber zu optimieren.

TECHNISCHE LEISTUNGSMERKMALE

Leistungsbedarf des Systems

- RAM-Bedarf zur Verarbeitung 15MB
- Disk 350kB
- CPU-Bedarf 1-2% bei 2.5GHz CPU

Beispiel für eine zu analysierende Netzwerkinfrastruktur:

- 4 Zonen: DMZ, interne Services, 2 Entwicklungszonen; getrennt durch Firewalls
- 25 Server
- 25 Firewalls, je 1 auf 1 Server
- Analysierte Log-Zeilen: 4Mio/Tag
- Apachesysteme (6 Stück) mit etwa 20k Zugriffen/Tag
- Netzwerktransfers mit ~20GB/Tag
- ~20 Entwicklersysteme

AIT AUSTRIAN INSITUTE OF TECHNOLOGY
Dr. Dr. Florian Skopik
Tel +43 664 8251495
Donau-City-Straße 1, 1220 Wien
florian.skopik@ait.ac.at
www.ait.ac.at