BWI GmbH operationalisiert ihr Governed Cyber Threat Model

Case Study 2 von 2 · Von validierten STIX-Patterns zu nativen SIEM-Regeln – nachgewiesen durch Adversary Emulation

Ergebnisse auf einen Blick

Die Cyber Threat Modelling (CTM)-Plattform des Herstellers IdoubleS veredelt Cyber Threat Intelligence (CTI) in natürlicher Sprache zu einem **Governed Cyber Threat Model** – einem Attack Graphen, in dem jede Aussage Evidenz, Konfidenz und einen Validierungsstatus trägt. Die erste Case Study beschreibt diese Modellierung (Testszenario 2); diese zweite beschreibt, was die BWI GmbH mit dem validierten Modell tut: Die Plattform leitet daraus je Technik Pseudocode in Form standardisierter STIX-Patterns ab und übersetzt diese – angepasst an das Datenmodell des kundeneigenen SIEM – in native Detektionsregeln, die SVA als Hauptauftragnehmer, Value-Added Reseller und Integrationspartner von IdoubleS per Adversary Emulation auf die Probe gestellt hat.

- **Validierte Detektionslogik:** 14 STIX-Patterns aus dem Emotet-Delivery-Modell, von drei Experten unabhängig nach sechs Kriterien bewertet – **82,47 %** Gesamteffizienz, 8 von 14 Techniken bei 80 % oder besser, Einigkeit der Bewerter in 71 % aller Einzelbewertungen.
- **Native Regeln für das SIEM:** 11 von 14 Techniken im Labor testbar, **90,47 %** über sieben Kriterien; 4 Regeln mit 100 %, 10 von 11 bei 80 % oder besser – bei geringem manuellem Anpassungsbedarf.
- **Bewiesen, nicht angenommen:** In der Adversary Emulation mit MITRE Caldera erzeugten **11 von 11** Regeln ein Alarm im SIEM – 9 vollständig, 2 teilweise, keine blieb stumm.
- **Lücken benannt, nicht versteckt:** Drei Techniken konnten mangels Mail-Gateway-Logquelle im Labor nicht getestet werden; ein Regex-Escape-Problem wurde während der Validierung behoben; jede Bewertung hat einen Bewerter und eine Begründung.

Kundenprofil & Ausgangssituation

Die Bundesrepublik Deutschland hat die BWI GmbH mit der Modernisierung und dem zuverlässigen und wirtschaftlichen Betrieb eines Großteils der Informations- und Kommunikationstechnik der Bundeswehr beauftragt. Gesellschafter der BWI ist zu 100 % der Bund. Als IT-Systemhaus der Bundeswehr ist die BWI ihr primärer Digitalisierungspartner in Frieden, Krise und Krieg.

Mit der ersten Validierungsphase hatte die BWI nachgewiesen, dass sich CTI-Berichte automatisiert zu präzisen, nachvollziehbaren Attack Graphen veredeln lassen. Die nächste Frage war die entscheidende für ein SOC: Kommt dieses Wissen im SIEM an – als Regel, die feuert, wenn die Technik tatsächlich ausgeführt wird? Für diesen Schritt setzte die BWI auf SVA: SVA hat die projektbegleitende Cloud-Umgebung aufgebaut und betrieben, die Testfälle definiert und die Adversary Emulation mit eigenen SIEM-Spezialisten und Penetrationstestern durchgeführt (Testszenario 4); bei den STIX-Patterns (Testszenario 3) unterstützte der Hersteller.

Herausforderung

Der Weg vom Bericht zur Regel ist in den meisten SOCs eine Kette manueller Übersetzungen: Ein Analyst liest, ein Detection Engineer schreibt eine Regel, ein Hunter formuliert Abfragen, ein Incident Responder ein Playbook – jeder aus seiner eigenen Lesart desselben Berichts, in eigenen Tools und Vokabularen. Was dabei entsteht, ist inkonsistent und nicht rückverfolgbar: Niemand kann zeigen, welche Aussage im Bericht zu welcher Regel geführt hat, und die Abdeckung wird angenommen, nicht bewiesen.

Generative Sprachmodelle versprechen Abhilfe und schreiben auf Zuruf SIEM-Regeln. Doch eine Regel ist nur so gut wie ihr Kontext: Welche Logquellen und Ereignistypen existieren im SIEM des Kunden tatsächlich, welche Properties tragen für dieses Ereignis einen Wert, welche Reference Sets ersetzen die Platzhalter, ist die Syntax gültig, verhält sich die Regel bei einem echten Angriff wie erwartet? Nichts davon steht im Bericht, nichts davon kennt ein allgemeines Sprachmodell – und ohne Testfall bleibt jede Regel eine Behauptung. Für Nachweise gegenüber Regulatorik wie DORA und für bedrohungsgeleitete Tests nach TIBER-EU braucht es dagegen den nachvollziehbaren Pfad von der Intelligence über die Kritische Funktion bis zur Detektion. Die Frage lautet daher nicht, ob sich Regeln schneller schreiben lassen, sondern ob sie vertrauenswürdig sind: aus validiertem Wissen abgeleitet, an die reale Umgebung angepasst, geprüft und wiederholbar.

„Durch die KI-gestützte Plattform von IdoubleS wurde eine maßgeschneiderte Veredelung von CTI möglich, die für uns zuvor kaum vorstellbar war. Die tägliche Flut an CTI-Daten war manuell nicht zu bewältigen – heute gewinnen wir daraus ein vertrauenswürdiges Cyber-Threat-Modell, aus dem wir Detektionslogik für unser SIEM und EDR ableiten.“

[Head of Cyber Defence Center, BWI]

Zielsetzung

Im Validierungsplan legte die BWI zwei aufeinander aufbauende Testszenarien fest. **Testszenario 3:** Aus dem validierten Emotet-Delivery-Modell soll die Plattform je Technik automatisiert ein STIX-Pattern erzeugen – standardisierten, maschinenlesbaren Pseudocode, der als Grundlage für native SIEM-/EDR-Regeln taugt. **Testszenario 4:** Aus diesen Pattern sollen native SIEM-Regeln entstehen, die an die Kundenumgebung angepasst sind.

Die Prüfkriterien wurden vorab festgelegt und mit Punkteskalen versehen: sechs Kriterien je STIX-Pattern – Technikabgleich, Genauigkeit der Logquelle, realistische Ereignisse, Integrität des Attack Flows und verhaltensbasierte Erkennung statt Indicators of Compromise (IOCs) – je 0 bis 2 Punkte – sowie Gültigkeit der STIX-2.1-Syntax – 0 oder 1 – und sieben Kriterien je nativer Regel: Log-Source-Typen, Event-Typen, Property-Mapping, Befüllung der Platzhalter, Abgleich mit dem STIX-Pattern, Regelsyntax und Regel-Match in der Emulation. Bewertet wurde nicht vom Hersteller: Drei Cyber-Security-Experten beurteilten jedes Pattern unabhängig voneinander; SIEM-Spezialisten und Penetrationstester von SVA definierten die Testfälle und führten die Adversary Emulation nach gemeinsam vereinbarten Abnahmekriterien durch.

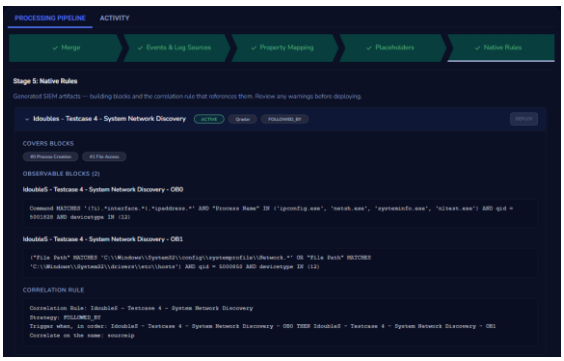
Lösung – vom Graphen zur Regel

Schritt 1 – Pseudocode. In der Detailansicht einer Technik erzeugt die Plattform auf Knopfdruck innerhalb von 30 bis 60 Sekunden ein STIX-Pattern – mit einer Zusammenfassung in natürlicher Sprache, einer Visualisierung des Ausdrucks, den zugehörigen MITRE Data Components/Detection Strategies/Analytics und einem Editor mit Syntaxprüfung. Das Pattern beschreibt Verhalten statt Indikatoren: Observable Blocks benennen Logquelle und Ereignis, FOLLOWEDBY-Ketten bilden den Attack Flow

ab, Platzhalter halten umgebungsspezifische Werte offen. Der Kontext stammt aus dem validierten Graphen – nicht aus einer freien Nachfrage.

```
[
    process:name IN ('ipconfig.exe','netsh.exe','systeminfo.exe','nltest.exe')
    AND process:command_line MATCHES '(?i).*interface.*|.*ipaddress.*'
    AND x-event:platform = 'windows'
    AND x-event:source = 'endpoint_edr'
    AND x-event:name = 'Process Creation'
  ]
```

STIX-Pattern für T1016 System Network Configuration Discovery – Pseudocode, abgeleitet aus dem validierten Attack Graphen



Schritt 2 – native Regel. Über den App-Module-Store verbindet die Plattform das SIEM des Kunden. Nach dem Verbindungsaufbau ruft sie Event Categories, Event Types, Log Source Types, Properties und Collections automatisiert über die SIEM-API ab und synchronisiert sie regelmäßig. Die Übersetzung läuft als Pipeline mit Kontrollpunkten: Correlation Property, Events & Log Sources, Property-Mapping, Platzhalter zu Reference Sets oder Inline-Literalen, native Regel. An jedem Schritt sieht der SIEM Engineer das Mapping und kann es anpassen – die KI schlägt vor, der Mensch entscheidet, und die Entscheidung bleibt dokumentiert.

Schritt 3 – Beweis. Zu jeder Regel gehört ein Testfall im YAML-Format. In dem von SVA aufgebauten und betriebenen Adversary-Emulation-Labor aus Windows-Servern und -Clients hinter einem Squid-Proxy führte MITRE Caldera die Techniken der Emotet-Delivery-Phase aus; die entstehende Telemetrie lief im SIEM auf, wo die generierten Regeln warteten. Damit schließt sich die Kette: Bericht › validierte Aussage › STIX-Pattern › native Regel › Offense. Jedes Glied ist nachvollziehbar, jede Bewertung hat einen Bewerter, und nach jeder Änderung läuft dieselbe Prüfung erneut.

Validierungsergebnisse

Testszenario 3 (Juni 2026): 14 Techniken der Emotet-Delivery-Kampagne, von T1566.001 *Spearphishing Attachment* über T1059.005 *Visual Basic* und T1105 *Ingress Tool Transfer* bis T1041 *Exfiltration Over C2 Channel*. Über alle 14 Patterns wurde eine Gesamteffizienz von **82,47 %** (381 von 462 Punkten) erreicht; die drei Bewerter waren in 71 % aller Einzelbewertungen einig. Stärken: verhaltensbasierte Erkennung statt Indikatoren und gültige Syntax. Schwächen: redundante bzw. überschneidende STIX-Patterns sowie Verbesserungspotenzial bei der präzisen Identifizierung und Darstellung relevanter Logquellen und Ereignisinformationen.

Kriterium	Erfüllungsgrad
Balance verhaltensbasierte Erkennung vs. IOCs	95,2 %
Gültigkeit der STIX-Syntax	92,9 %
Realistische Ereignisse	83,3 %
Integrität des Attack Flows	83,3 %
Genauigkeit der Logquelle	79,8 %
Technikabgleich	65,5 %

Tabelle 1 – STIX-Patterns: Erfüllung je Kriterium, drei Bewerter, 14 Techniken

Testszenario 4 (August/September 2026): Für 11 der 14 Techniken konnten native SIEM-Regeln im Labor von SVA getestet werden; drei Techniken (T1059.005, T1204.002, T1566.001) benötigen eine Mail-Gateway-Logquelle, die das Labor nicht hatte – eine

benannte Lücke, keine versteckte. Die elf Regeln erreichten **90,47 %** über sieben Kriterien; vier Regeln erzielten die volle Punktzahl, zehn von elf lagen bei 80 % oder besser. In der von SVA durchgeführten Emulation erzeugten alle elf Regeln eine Offense – neun vollständig, zwei teilweise. Der manuelle Anpassungsbedarf am Regelwerk war gering.

Kriterium	Erfüllungsgrad
Befüllung der Platzhalter (7 Regeln mit Platzhaltern)	100 %
Genauigkeit der Log-Source-Typen	95,5 %
Abgleich mit dem STIX-Pattern	95,5 %
Property-Mapping	90,9 %
Regel-Match in der Adversary Emulation	90,9 %
Realistische Event-Typen	81,8 %
Gültigkeit der Regelsyntax	81,8 %

Tabelle 2 – Native SIEM-Regeln: Erfüllung je Kriterium, 11 Regeln

Zwei Erkenntnisse fließen in die Roadmap des Herstellers ein: Für das Property-Mapping ist es hilfreich, tatsächliche Werte aus SIEM-Events als Telemetriebeispiele abzurufen, weil das Datenmodell nicht immer zeigt, ob eine Property für ein Ereignis befüllt ist. Und die Erstellung nativer Regeln soll künftig vollautomatisiert laufen – die KI trifft die Entscheidungen jedes Übersetzungsschritts, Kontrollpunkte halten sie für den SIEM-Engineer nachvollziehbar und überprüfbar. Eine Re-Validierung folgt nach der Umsetzung.

Use Cases

Aus einem validierten Modell entstehen bei der BWI – erbracht von SVA als Value-Added Reseller – mehrere operative Ergebnisse aus einer Quelle, nicht aus vier Lesarten:

- **Detection Engineering** – native Regeln für SIEM und EDR aus validiertem Pseudocode, mit Abdeckung je Technik und dokumentiertem Mapping.
- **Threat Hunting und Incident Response** – STIX-Patterns als Hunting-Abfragen und der Graph als Leitfaden in der Reihenfolge des Angreifers: Technik, Logquelle, Ereignis.
- **Regulatorik** – die Kette vom Bericht bis zur Offense als Nachweis für DORA; bedrohungsgeleitete Szenarien als Grundlage für TIBER-EU.
- **Agentischer SOC** – validierte Patterns und Regeln, die jede Plattform über STIX, APIs oder MCP konsumieren kann; das Wissen bleibt Eigentum des Kunden.

Nächste Schritte

Sprechen Sie mit uns: www.sva.de

Mehr zum Hersteller und zur Plattform: www.idoubles.net