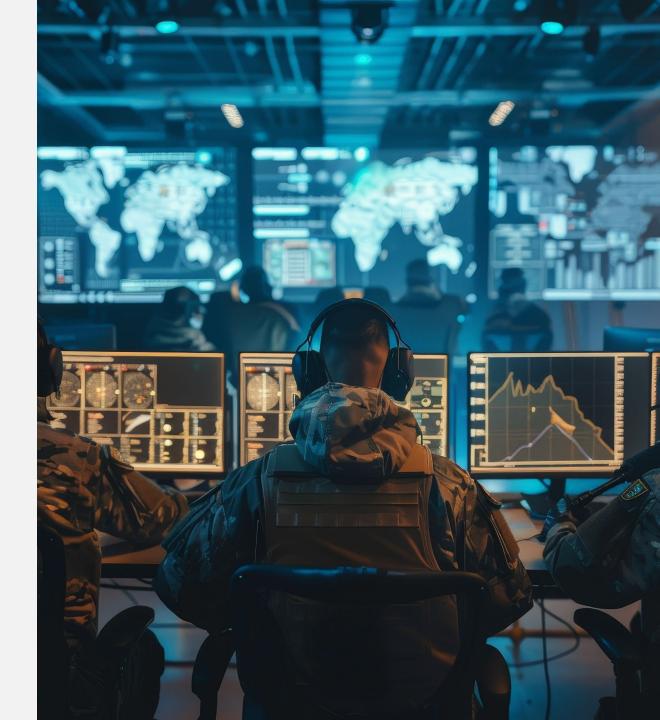


Advanced Cybersecurity with SITU-X:

Real-Time Entity Level Intelligence on Zero-Trust Architecture

January 16, 2025



From groundbreaking research to leading-edge cybersecurity solutions

SITU-X represents a strategic alliance between cutting-edge research and enterprise innovation. This unique platform combines **SITU's** advanced anomaly detection and cybersecurity research from **Oak Ridge National Laboratory (ORNL)** with the enterprise-grade distributed AI infrastructure of **Xenese™**, delivering the next-generation cybersecurity intelligence.

Research-driven innovation

- Developed at ORNL with funding from DOE, DoD, and DHS to safeguard mission-critical systems.
- Built through multidisciplinary research in data science, AI, and national security sciences.

A collaborative consortium

 U2opia acquired SITU from ORNL and integrated it with Xenese[™], forming a consortium to merge advanced AI/ML, entity-level intelligence, and zero-latency solutions on distributed node technology.

Real-time threat intelligence

 SITU-X delivers adaptive, real-time cybersecurity solutions, and enhances existing investments by complementing platforms like BeyondTrust and Splunk.



Our advanced capabilities deliver real-time cyber intelligence and resilient security solutions

Intelligent Threat Detection

• Entity-Level Models: Millions of supervised and unsupervised probabilistic models for advanced anomaly detection.

• **Distributed Analytics:** Detects and mitigates threats instantly across hybrid and distributed environments.

Contextual Insights at Scale

• Probabilistic Scoring: Prioritizes threats with advanced anomaly scoring using sliding time windows.

• Contextual Analysis: Tracks behavior patterns to uncover low-and-slow attacks and complex threats.

Resilient Security and Compliance

• Zero-Trust Architecture: Ensures secure, immutable infrastructure.

GenAl-Powered
Actions: Delivers
prescriptive analytics
and automated
recommendations for
faster response.

Distributed Hybrid Integration

• Scalable Infrastructure: Processes massive data volumes across edge, on-premises, and cloud.

• API and Privilege Monitoring: Realtime detection of misuse and vulnerabilities in privileged access.

Navigating the DoD's evolving cyber threat landscape: Key challenges in Defense

Top Cyber Threat Challenges

- Detecting Advanced Persistent Threats (APTs): Stealthy nation-state attacks blend into normal traffic, evading traditional systems.
- 2. Managing Overwhelming Data Volumes: Petabytes of daily data overwhelm analysts with false positives.
- **3. Preventing API & Privileged Access Exploits:** API misuse and credential theft lead to undetected breaches.
- 4. Ensuring Resilience in Distributed Environments: Hybrid and edge environments create visibility gaps and latency issues.

Cyberattack Rates and Volumes



Incident Reporting Trends (2017-2022): Reports **surged** from 780/month in 2020 to 1,240/month in 2021, normalizing to 602/month in 2022.



Federal Cybersecurity Incidents (2022): 800,944 cyber-crimes reported, with financial losses rising 50% to \$10.3 billion.



Defense Sector Trends:

300% increase in cyberattacks since 2018, with an average breach cost of \$5.46M.

References: 2023 DoD Cyber Strategy Summary, DoD Cyber Crime Center (DC3) Annual Report.

Responding to DoD Cybersecurity challenges with **SITU-X** advanced capabilities ⁽¹⁾

Detecting Advanced Persistent Threats (APTs)

Problem Solved: SITU-X uncovers APT behaviors that blend into normal traffic, enabling real-time defense.

Entity-Level ML Models: Tracks user, device, and API behaviors to uncover subtle deviations.

Probabilistic Anomaly Scoring: Prioritizes complex behaviors with likelihood scores.



Managing Overwhelming Data Volumes

Problem Solved: SITU-X reduces analyst overwhelm by filtering petabytes of daily data, eliminating false positives, and highlighting critical threats for faster response.

- Automated Anomaly Detection: Filters false positives with millions of autonomous models.
- Petabyte-Scale Processing: Ingests and analyzes vast streaming data in real-time.

Responding to DoD Cybersecurity challenges with **SITU-X** advanced capabilities ⁽²⁾

Preventing API & Privileged Access Exploits

Problem Solved: SITU-X uncovers APT behaviors that blend into normal traffic, enabling real-time defense.

3

- API Behavior Monitoring: Detects unusual patterns, privilege escalation, and geo-locations
- Prescriptive GenAl Insights: Recommends remediation actions like revoking keys or blocking access.



Achieving Resilience Across Distributed & Hybrid Environments

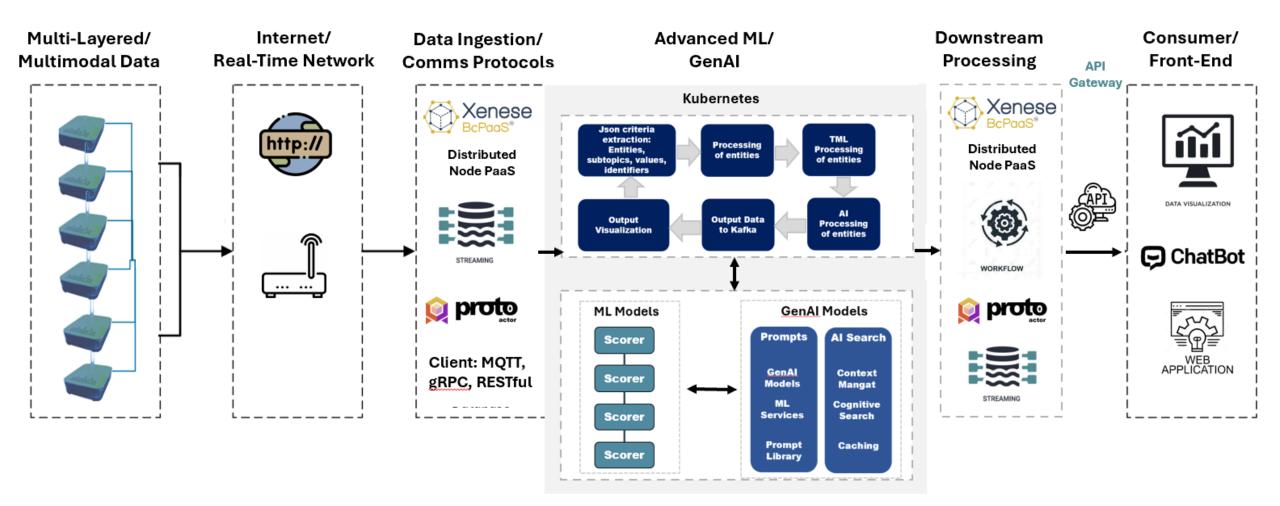
Problem Solved: SITU-X ensures resilience by closing gaps and reducing latency with distributed AI and real-time edge processing.

- Distributed Al Infrastructure: Processes data at the edge for low-latency insights
- Zero Trust Architecture: Secures systems with real-time, continuous verification.

We built differentiation from the start with the latest advances in Fast ML and Actor Models

Ca	pabilities	SITU-X	BeyondTrust	Splunk	CrowdStrike	Palo Alto Networks	Google Mandiant
1.	Entity-level Autonomous, in-memory, ML models for real-time threat detection at scale	1	X	X	X	X	X
2.	Petabyte-scale data ingestion with Distributed AI	1	x	✓	X	✓	1
3.	GenAl-powered prescriptive analytics for real- time threat remediation	1	X	X	X	x	X
4.	Entity-level autonomous, in-memory, Al prompts for real-time threat analysis	1	X	X	X	х	x
5.	Actor model scale framework on Node technology (immutable cryptography)	1	X	X	X	x	x
5 .	Distributed edge processing with zero latency	1	X	X		✓	1
7.	Integrated API behavior monitoring and privilege escalation detection	✓		X	X	X	■ 100 000 000 0000 0000 0000 0000 0000
8.	Cross-platform integration and visibility (on- prem, cloud, hybrid)	✓	-			~	√
9.	Dynamic scaling, resilient processing, and fine-grained parallelism through actor models	~	X	•	X	0	O

Transactional ML, GenAl, and real-time streaming define the uniqueness of our architecture





SITU-X DEMO

1-20 of 1000 records														
estination	Top Destination Ports	Unique Source IPs ①	Unique Ports 🗘	Median Anomaly ψ	Max Anomaly \oplus	Flow Count	Rank (1)	Change ()						
92.31. × ÷ 🗋 ©	6667 × 20000 ×	2	2	6.09	6.10	2	1	924 ^						
0.1. × ∻ D ©	44050 × 53930 × 56048		3	4.77	4.78	3	2	-1~						
0.123. × ∻ □ ©	56290×	1	1	4.71	4.71	1	3	-1~						
0.149. × ∻ D ©	443 ×	1	1	4.65	4.65	1	4	New *						
	443×				4.65									
0.233. × ∻ □ ©		6	1	4.52		11	5	909 ^						
0.233. × ∻ □ ©	80 ×	17	1	4.44	4.72	27	6	24 ^						
0.1. × ∻ D ©	56482 × 57048 ×	2	2	4.41	4.41	2	7	New *						
0.233. × ∻ □ ©	80 ×	15	1	4.41	4.78	24	8	512 ^						
0.233. × ∻ D ©	80 ×	6	1	4.41	4.95	22	9	-2 ~						
28.219. × ∻ D ©	443×	14	1	4.34	4.86	16	10	-7 ~						
0.149. × ∻ D ⊗	25 × 587 ×	12	2	4.33	4.68	26	11	4 ^						
0.149. × ∻ D ©	25 × 587 × 90000	Manufacture Constitution	deal and the second	and the state of the	Intelligent State	in the second second				الاروا	a de la com	استرزار		
0.159. × ∻ D ©	8× 0	1/5/2625, 13/00.00.000 EST	145/2025, 16:46:40	000 EST 1000	15, 20:33:20.000 (ST	18/2025, 00:20:00	000 EST	1/10/2025, 04:05:	40.000 EST	1000	025, 07153120.000 ES			
28.219. × ÷ D ©	443×	papersa, internet sar	papaone, nonerico		Stime					416				
0.159. × ∻ D ⊙	8×		×®	_	× 18		_		୍ଞ				×⊗	
	190	0000	1500000			15030000			20000000					
0.233. × 4 □ ©	80×		10200020			12020000			10000000					
0.233. × ∻ 🗋 ©			5203020			\$000000			5000000					
0.233. × ∻ □ ©	80 ×	0 1 2 3 4 5 6		outboard internal network.direction - (2)	inbound		ublic	private		public	nation in turns to	private		
								www.rd - (21850688)						
0.233. × ∻ □ ◎	80 ×	anomaly.network.score - (21,850		network.direction - (2)		situn	a.source.ip_type.ke	ryword - (21,850,688)	< @	situng.dest	nation.ip_type.ia	word - (21,850,68		
0.233. × ∻ □ ◎	8× 2000	0000	× (3) 1500000	network.direction - (2	× (9	situn	a.source.ip_type.ke		10303000	situng.dest	inition.ip_type.iki	rword - (21,850,68	8) ×®	
	8× 2000	0.00	×ø	network.direction - (2		situn	g.source.jp_type.ke		< (2) 10303030 8003030 8003030	situng.aest	and the second second	word - (21,850,68		
0.159. × ∻ □ ⊙	8× 2000	0.00	×ø	network.direction - (2		5000000	, source.ip_type.ke		10000000			rword - (21,880,68		
0.159. × ∻ □ ⊙	8× 2000		0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 ×	Νρ υήρ	× Ø	0 5000000 0 50 50 50 50 50	тн зн	RSTOSO SHR RSTR-	10000000 8000000 4000000 2000000		228 9354 5:	23 8883 0		
0.159. × ∻ □ ⊙	8× 2000	en a a a a a a a a a a	×		× Ø	0 5000000 0 50 50 50 6		RSTOSO SHR RSTR-	10000000 8000000 4000000 2000000			23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000		×	Νρ υήρ	× (2) kmp. ct,850,688)	0 5000000 0 50 50 50 6	TH SH itung.state.keyword	851050 SHR 8518- d - (21,850,688)	10000000 8000000 4000000 2000000		228 9354 5:	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000	en a a a a a a a a a a	× (2) 5 0 0 6 0 0 6 0 6 0 6 0 6 0 6 0 6	Νρ υήρ	× (2) kmp. ct,850,688)	00000000 00000000 0	TH SH itung.state.keyword	851050 SHR 8518- d - (21,850,688)	10000000 8000000 4000000 2000000		228 9354 5:	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000	time Constraints and the second secon		NA	× (3) (1,850,688)	0000000 0 50 50 0 50 50 0 50 0 50 0 50	TH SH itung.state.keyworn ME TOIKE TOOME 1	A11000 DH-R A2100- d - (21,850,688) dda 10da 10da Dest Port ©	1939320 800000 200000 200000 0 443 0 443	d	228 9364 St estination.port - (SPCAP	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000	son	× () 0	to we network transvert - () for ty 0 19231 - × D 0	× (2) uny transcense SecPart 2 Sector 11× 204	0000000 0 000000 0 000000 0 000000 0 000000	TH SH Itung, state, Jeryworn MB 10MB 100MB 1	язтою (н. я. язто- d - (21,850,689) тба тобов тобов Вект Рига () О ×	1000000 800000 400000 200000 0 0 0 0 0 0 0 8	n no 1 d	228 9364 0: sstination.port (SPCAP	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000	1 2 3 4 1 2 3 5 1 5 1 3 3 5 8 5 1 - 1 3 5 8 -	× (0) unconstruction cent refer 5 cent v 7 c47 7 c16	to	× (2) 	0000000 0 000000 0 00000 0 0000 0 00000 0 0000 0 00000 0 00000 0 00000 0 00000 0 00000 0 00000	DH 3H THUNG STATE Jeyworn ŠE 10Å/B 10Å/B 1 Č ↓ × D * 3. × D *	язтоо эня ято - (21.250,688) года тода тода Бектрог () О × 443 ×	1000000 400000 400000 200000 0 0 0 0 0 0	Preto icmp tcp	2228 9364 0: stination.port - (SPCAP S	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000		× (2) 1 million 1 mi	No uo netrosite transport - () 192.31. × () ↔ 192.31. × () ↔	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	1000000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	111 54 111 102 state keyword ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	19000000 8000000 4000000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Prote iomp tcp tcp	2220 9354 0: estimation port - (0 0 2 2 2 3 2 3 2 4	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000	1 2 3 4 1 2 3 5 1 5 1 3 3 5 8 5 1 - 1 3 5 8 -	× (2)	to	× (2) 	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	1000000 400000 400000 200000 0 0 0 0 0 0	Preto icmp tcp	2220 9354 0: estimation port - (0 0 2 2 2 3 2 3 2 4	23 8883 0	× @	
0.159. × ∻ □ ⊙	8× 2000	and a transport of the second seco	× (*) *	Np → √0 network brancor - () 192.31. × () 0 192.31. × () 0 192.31. × () 0 192.31. × () 0	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	1000000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	00000000000000000000000000000000000000	Prete icmp tcp tcp	2220 9354 0: estimation port - (0 0 2 2 2 3 2 3 2 4	23 0083 0	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	the second	× (*) unset cest) d Turfo test 2.047 7.059 2.047 7.059 0.054 0.054 0.054	10	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Ceet Bytes 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Prete icmp tcp tcp	272 936 2 Composite : Blockint ©	23 0083 0	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	time Scotler (1997)	× () unconstruction cent drafte cent fr	10 ∞ Bre (p. 0) 192.31. 192.31. × () o 192.10. × (> () a	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Ceet Bytes 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Prete icmp tcp tcp	220 0.04 € sstination.pert - (SPCAP ⊗ © (b) (b) Composite : Mosciliat © DNS Rate ©	23 M683 0 1,850,6689	× @	Anomaly Scor
0.159. × ← □ ⊙	8× 2000	the state of	× () u u u u u u u u u u u u u u u u u u u	to we network transect - D 192.31. × D ≎ 192.31. × D ≎ 192.31. × D ≎ 192.31. × D ≎ 192.31. × C ≎ 192.31. × C ≎ 192.31. × C ≎ 192.31. × C ≎	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Cert Bytes 2	Prets icmp tcp tcp tcp 20 20 T-AS	222 BIGE ST SPCAP SPCAP Composite Bioskies © DNS Bate © SAMSR Role Ch	23 M683 0 1,850,6689	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Contigues	Prese icmp icp icp icp icp icp icp icp icp icp ic	272 BIGG E SPCAP © © © Composite : Biochist © DNS Rate © SANSK Role Ch Packet Byre Ra	zz deci 0 t, aso, ceay core mge © ge [betenst] ⊙	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Contigues	Prote icmp tcp tcp tcp tcp tcp tcp tcp tcp tcp tc	SPCAP SPCAP SC SPCAP SC Composite : Blocklist © DNS Rate © SAMSIR Role Ch Packet Byte Ra	zz deci 0 t, aso, ceay core mge © ge [betenst] ⊙	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Cost System Cost Syst	Preise icmp iccp iccp iccp iccp iccp iccp iccp	272 BLG E SPCAP SPCAP SPCAP Composite : Bioskilat © DNS Rate © DNS Rate © Packet Byte Ra Packet Byte Ra Packet Byte Ra Packet Byte Ra Packet Byte Ra Packet Byte Ra	23 0000 0 1,150,068) COOPE Inge © Scope Inge (Disternal) ⊙ ort Range ©	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Ceet Byes 3 Ceet Bye	Prete Icop tcp	SPCAP	23 Adda 0 1,150,0689) CCOTE ange © up (Diternal) © ur (Range © up (Bitckilat) © 0	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Cost Syne () Cost Syne () Co	Prote imp	SPCAP	23 8663 0 17,850,668) CCOPE CCOPE age ((Netenda) ⊙ ref Range ⊙ age ((Netenda) ⊙ age ((Netenda) ⊙	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Ceet Byes 3 Ceet Bye	Pretes Pretes top top top top top top top top	222 USG S SPCAP S S C US C US C S C S C S C S C S C S C	23 4663 0 1,155,068) Core age (biternal) ⊙ ret Range ⊙ age (biternal) ⊙ rege (Bitechlint) ∩ rege (Bitechli	× @	Anomaly Scor
0.159. × ∻ □ ⊙	8× 2000	timp biodint.comt - 1200 3 0 10 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	× () u u u u u u u u u u u u u u u u u u u	to uo metrosek transact of 192.31. × 0 o 192.31. × 0 o	V (2) Ump TLABORED SIE Part 2: Siece 11× 200 115007× 2,33 38407× 711	a tio sin of the second	D1 34 Rung state Anywor û 0 3. × D * 7. × D * . × D *	821000 00-8 82100 d- (21.850,688) Has table toolds Dest Port 0 0 × 443 × 80 ×	Continue	Prese imp tep tep tep tep tep tep tep te	272 BIGG S. SPCAP SPCAP S Composite : da Bioskins Color Packet Bye Ra Packet Bye Ra Packet Bye Ra Packet Bye Ra Packet Stre Ra Pack	23 4663 0 1,155,068) Core age (biternal) ⊙ ret Range ⊙ age (biternal) ⊙ rege (Bitechlint) ∩ rege (Bitechli	× @	Anomaly Scor

Achieving Enhanced Business Outcomes with SITU-X's Advanced Cyber Defense Capabilities

Reduce Detection Time: Advanced AI/ML-driven platforms can reduce threat detection and response time by **up to 96%** (Ponemon Institute, 2023).

SITU-X Impact: Real-time streaming intelligence identifies threats faster, minimizing potential dwell time and damage.

Lower False Positives: Al-enhanced cybersecurity solutions reduce false positives by 70-90%, improving operational efficiency (Gartner, 2024).

SITU-X Impact: Tailored entity-level models filter noise, allowing analysts to focus on real threats.

Improve Analyst Productivity: Automation and advanced analytics increase security team productivity by 40%, enabling teams to handle more incidents effectively (Deloitte Cyber Risk Report, 2022).

SITU-X Impact: Automated anomaly detection and prescriptive insights reduce manual effort.

Reflecting on the Recent Treasury Hack—How SITU-X Could Have Made a Difference

The Incident

 In December 2024, hackers exploited API vulnerabilities in third-party cybersecurity software to access U.S. Treasury systems. They bypassed security, obtained sensitive access using stolen API keys, and infiltrated workstations undetected.

If SITU-X Had Been in Place:

Entity-Level Intelligence API behavior would have been tracked in real-time, flagging unusual usage patterns and privilege escalations.

Probabilistic Anomaly Detection

Sliding-time windows would have identified irregular API calls, such as unexpected geo-locations or excessive access attempts, by scoring deviations in real-time

Distributed AI for Resilient Defense The SITU-X Distributed AI infrastructure would have ensured low-latency response and detection directly at the edge.

Thanks for your time.



Contact Us

Website: www.u2opiatech.com Key Contact: Joaneane Smith Email: Jsmith@u2opiatech.com

