Teamcenter Security Monitoring through SAS Analytics Siemens - SAS joint user behavioral analytics project

Scott Allen Mongeau Cybersecurity Data Scientist – Principal Business Solutions Manager SAS Institute



Overview

- Requirements
- Solution overview
- Development process
- Analytics methods
- Example anomalies
- Conclusion





Requirements





Teamcenter Security Requirements

- **Teamcenter PLM** = managing product lifecycles, contains sesitive intellectual property
- Multi-tiered web services, browser based application with array of add-on modules

High-level requirements - PoC

- Key use case = protecting intellectual property / preventing improper use and exfiltration
- Non-invasive, automated, asyncronous
- Minimize administrative overhead
- Strict user privacy (anonymization)
- Identify highly unusual anomolous user behaviors
- Minimize false alerts through embedded contextual understanding of typical / atypical behavior





Teamcenter Security Requirements

- **Teamcenter PLM** = managing product lifecycles, contains sesitive intellectual property
- Multi-tiered web services, browser based application with array of add-on modules

High-level requirements - PoC

- Non-invasive, automated, asyncronous
- Minimize administrative overhead
- Strict user privacy (anonymization)
- Key use case = protecting intellectual property / preventing improper use and exfiltration
- Identify highly unusual anomolous user behaviors
- Minimize false alerts through embedded contextual understanding of typical / atypical behavior







Solution Overview



TeamCenter Log Analytics



Ingest raw log data in batch

Refine data and Deliver focused apply advanced anomaly alerts analytics

Internal follow-up



High-Level Functional Process



Anomaly Detection: Simply Complex







Assessing Key Features to Produce Focused Anomalies







Development Process





Cybersecurity Analytics for TeamCenter PLM









Inferential Exploration

- Exploratory analytics
- Initial sample = 2 weeks TC syslog sessions
- Initial challenges
 - Unstructured
 - Little documentation
 - Little known concerning structure/context (codes, functional relevance)
 - Verbose (many codes, commands, etc.)

	tcserver_1499120139_396YOSZ8WA36_124079.txt ×	
	services disabled Teamcenter, SUA, Server	St. 25
	INFO - 2017/07/03-22:15:22.856 UIC - 0D5NYEC00112.6/102.8519.1EWAFRG90N8V.00001.Mgr.Svr.12HC018VL1X7.00001 - Service	
	Request: Iclogingervice:authencicatewithlocale - leancenter.soa.communication	0000-00.000
	WILE - 2017/07/03-22:13:22:005 UIC - 005NTECOUIL:07102:0519.1EMAY RG5UN0V.00001.ngtr.SVT.12RCU10VLIX.00001 - D0CS AL52U176	
	Via UB-ICXI mapping - leamcenter.PUM at /pim/cynas/tce_iproot4/units/tcii221_c0i_build/src/toundation/pom/eim/	Marter Jonatio
	ell_trans_util.cxx(/15/) THEG _ 0017/02_2215/22_963_UTC0DENVECC0117_67102_9510_1EUAEDC018/9V_00001_Man_Sup_17//C019V/1V7_00001lockmutous	
	1 m 0 - 2017/07/05-22:15:22:005 010 - 00541100012:0515:1144-M350000.00001.mgt.5vt-1210010017.00001 - 1004 mulex.	
	Reprocessoure name-initia_nome_initiantoxitxa_imp_ritoool:co.ci_co/co/co/co/co/co/co/co/co/co/co/co/co/c	A DESCRIPTION OF THE OWNER, STATE
	Then $\sim 2017/07/2012/1015/2018$ ITC $\sim 0.05NVFCON17/67142/8519 (EMERGINER) CARACTERISTIC (CONFUNCTION 1) (CON$	-201001 1-00-0201
	semanhore key-semanhore TD=26211. Teamrenter Constructional follosce at /mm/runas/tre incont/units/	
	tc11221 c41 hulldsr/ccos/fclasses/memorymanagement.cvx/225)	
	INFO 2017/07/03-22:15:22.864 UTC - 005NYEC00112.67102.8519.1EWAFRG9UN8V.00001.Mgr.Svr.17HC018VL1X7.00001 - Creating	Contraction of the second second
	allocator m segmentKey [/hdla/home/HT15W1UKJCW/tmp/V11000.2.0.21 20 20161029.00/481884931/TextSrv/en US/emh text.xml.mem]	
	m segmentMutexName [hdla home HT15W1UKJCXW tmp V11000.2.0.21 20 20161029.00 481884931 Textsrv emh text.xml.seg.mtx]	C. S. Barrison
	mutexKey [8cd6efe5] - Teamcenter.TextServer.textsrv at /plm/cynas/tce iproot4/units/tc11221 c01 build/src/core/textsrv/	
	textpool.cxx(197)	
	INFO - 2017/07/03-22:15:22.864 UTC - 0D5NYEC00112.67102.8519.1EWAFRG9UN8V.00001.Mgr.Svr.1ZHC018VL1X7.00001 -	
	semaphore_key=8cd6efe5 semaphore_ID=294920 - Teamcenter.CoreModelGeneral.fclasses at /plm/cynas/tce_iproot4/units/	
	tc11221_c01_build/src/core/fclasses/memorymanagement.cxx(225)	
	INFO - 2017/07/03-22:15:22.864 UTC - 0D5NYEC0011Z.67102.8519.1EWAFRG9UN8V.00001.Mgr.Svr.1ZHC0I8VL1X7.00001 - segment mutex:	E COL
	key=8cd6efe5 name=_hd1a_home_HT15W1UKJCXW_tmp_V11000.2.0.21_20_20161029.00_481884931_Textsrv_emh_text.xml.seg.mtx -	A STATUTE AND A STATUTE AND
	Teamcenter.TextServer.textsrv at /plm/cynas/tce_iproot4/units/tc11221_c01_build/src/core/textsrv/textpool.cxx(249)	the New I-
	INFO - 2017/07/03-22:15:22.864 UTC - 0D5NYEC0011Z.67102.8519.1EWAFRG9UN8V.00001.Mgr.Svr.12HC018VL1X7.00001 -	Julyar
	<pre>semaphore_key=8cd6efe5 semaphore_ID=294920 - Teamcenter.CoreModelGeneral.fclasses at /plm/cynas/tce_iproot4/units/</pre>	
	tc11221_c01_build/src/core/fclasses/memorymanagement.cxx(225)	NAME OF CONTRACT OF CONTRACT
	INFO - 2017/07/03-22:15:22.864 UTC - 0D5NYEC00112.67102.8519.1EWAFRG9UN8V.00001.Mgr.Svr.12HC018VL1X7.00001 - Default	
	encryption configuration Teamcenter.FoundationBase at /pim/cynas/tce_iproot4/units/tcl1221_c01_build/src/foundation/base/	
170	Successfully loaded dynamic module /hdia/home/hliswitk.jcw/appi/tcpbi0/t4sii_z/apps_poolmanager/ildo4/ildt4s.so	
178	Load the Custom Library (110(45) V11.2.2.0 (May 20 2010 21:22:43) METWIDE for LOV type TAS ListOffvalueString susceptibily pegitaneed	10111011111000000000000000000000000000
170	Successfully loaded durante module /hdia/home/HTISMIW/CM/4/annl/ren010/t4s11 2/anns nonlmanagen/lib64/libtds sigmons inc so	
180	Successfully loaded dynamic module (bdla/home/ITLSHINCY/A) (cp/10/4312_) apps_nolamingsr/ib6/1/btds manufacturing on	l'allim .
181	Load the Custom Library vibites manufacturings VII 2.2.4 (May 28.2016) 21-255)	
187	Successfully loaded dynamic module /bdl/abme/HTSWIIKICW/annl/tcn010/t4s11 2/anns poolmanager/lib64/libt4y guery so	
183	Load the Custom Library <libt4x guery=""> V11.2.2.0 (May 28 2016 21:29:51)</libt4x>	L LOZINAR
	Successfully loaded dynamic module /appl/tcp010/tcl1 2/lib/libym.so	
	ERROR - 2017/07/03-22:15:23.209 UTC - 005NYEC0011Z.67102.8519.1EWAFRG9UN8V.00001.Mgr.Svr.12HC018VL1X7.00001 - 1146 - Could	
	not load the Entry Point Function Ptr <libvm_register_callbacks> for the Custom Library <libvm> -</libvm></libvm_register_callbacks>	
	Teamcenter.CoreModelGeneral.tccore at /plm/svnas/tc_work/estifano/tc11221a01/src/core/tccore/custom_itk.cxx(371)	
	ERROR - 2017/07/03-22:15:23.210 UTC - 0D5NYEC00117.67102.8519.1EWAERG9UN8V.00001.Mgr.Svr.17HC018VL1X7.00001 - 1143 - Could	

• Initial investment in data selection and feature engineering





States Indicative of Exceptions

Example: 'SEVERITY'

- Determine how many users and sessions with term
- Aggregate total for each user and make record
 - Expand details for frequent terms (e.g. mean, st dev, total)
- Profile and determine outliers
- Record flag for outliers
- Validate with systems experts to determine significance





Quantiles					
100.0%	maximum	2559			
99.5%		2559			
97.5%		1889.725			
90.0%		517.5			
75.0%	quartile	172.75			
50.0%	median	55.5			
25.0%	quartile	9.75			
10.0%		3.3			
2.5%		1.825			
0.5%		1			
0.0%	minimum	1			

Summary Statistics				
Mean	184.01786			
Std Dev	380.96684			
Std Err Mean	35.997982			
Upper 95% Mean	255.35026			
Lower 95% Mean	112.68545			
N	112			



'Severity' messages per user (112 users)

Principal Component Analysis (PCA)



Log File Measures Extracted





Resulting ETL Process

- SAS extract-transform-load (ETL) to process data and orchestrate analytics
- Specialized data handing: *i.e. time zone adjustment, segmentation of specialized users & subcommand handling*
- Regularized and reliable *flat data goes in and focused anomalies are produced*





Analytics Methods



Cybersecurity Anomaly Detection USER 1 **Multiple Methods to Surface Anomalies** Summarv Session Exception USER X-WK 1-6 USER X-WK7 Calls Summary Summary Multiuser Session Session Exception Exception **USER 2** Calls Calls 3 Summarv Multiuser Multiuser Anomalous Session 8 clusters Exception PEERGRP-WK 1-6 USER X-WK7 Calls Summary Multiuser Summarv Session Session 6 USER 3 Exception Exception 4 Summary Calls Calls 8 2. UNSUPERVISED MACHINE LEARNING Session Multiuser Multiuser 3 Exception Calls **3. DEVIATION FROM OWN PATTERNS** Multiuser (OWN & PEER GROUP)





1. 'FLAG' Messages

Univariate Flag Outliers (MSG1) - Many Individual Outliers in 1 Week



Each week a flag is generated per UserId for all high measures (90th percentile)

Number of flags per UserId are totaled

UserIds with high total number of outliers are Messageed (99.5th percentile)



Unsupervised Machine Learning: Cluster Analysis



Sas

2. 'UNUSUAL' Messages

Multivariate Cluster Anomalies (MSG 2, 3, 5 & 6) - Small or Rejected (1 & 6 wks)

Each week all UserIds are run through cluster analysis – both on *1 week* and *6 weeks* of aggregated data



"UNUSUAL"

Anomalies surface from cluster analysis

"NORMAL"

Large clusters indicate users behaving in similar ways



3. 'CHANGE' Messages

Latest week against six previous weeks (MSG 4 & 7)





Summary Overview

Anomaly Detection Methods



Sas





Example Anomalies



Example Anomaly: Red Teaming

- Alert messages UNUSUAL (3) and CHANGE (4&7)
- Some of variables showing particular spike:

Very high session activities, large number of system calls





SumNonIcctCalls
SumNonICCTOther
SumNonIcctCore



Example Anomaly: Team Leader in Performance Incident

Alerted – CHANGE (MSGs 4 & 7)





Example Anomaly: Unusual Behaviour

- System calls spike during week 36
- Received alert UNUSUAL (MSG 2) on week 36





Conclusion





Continuous Detection Improvement Process



Scott Mongeau **Certified Analytics Professional (CAP)** MA MA GD MBA PhD (ABD)





scott.mongeau@sas.com







QUESTIONS?





APPENDIX



References

- Aggarwal, C. (2013). "Outlier Analysis." Springer. <u>http://www.springer.com/la/book/9781461463955</u>
- Kirchhoff, C., Upton, D., and Winnefeld, Jr., Admiral J. A. (2015 October 7). "Defending Your Networks: Lessons from the Pentagon." Harvard Business Review. Available at https://www.sas.com/en_us/whitepapers/hbr-defending-your-networks-108030.html
- Longitude Research. (2014). "Cyberrisk in banking." Available at <u>https://www.sas.com/content/dam/SAS/bp_de/doc/studie/ff-st-longitude-research-cyberrisk-in-banking-2316865.pdf</u>
- Ponemon Institute. (2017). "When Seconds Count: How Security Analytics Improves Cybersecurity Defenses." Available at https://www.sas.com/en_us/whitepapers/ponemon-how-security-analytics-improves-cybersecurity-defenses-108679.html
- SANS Institute. (2015). "2015 Analytics and Intelligence Survey." Available at <u>https://www.sas.com/en_us/whitepapers/sans-analytics-intelligence-survey-108031.html</u>
- SANS Institute. (2016). "Using Analytics to Predict Future Attacks and Breaches." Available at https://www.sas.com/en_us/whitepapers/sans-using-analytics-to-predict-future-attacks-breaches-108130.html
- SAS Institute. (2016). "Managing the Analytical Life Cycle for Decisions at Scale." Available at https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/manage-analytical-life-cycle-continuous-innovation-106179.pdf
- SAS Institute. (2017). "SAS Cybersecurity: Counter cyberattacks with your information advantage." Available at https://www.sas.com/en_us/software/fraud-security-intelligence/cybersecurity-solutions.html
- SAS Institute. (2019). "Data Management for Artificial Intelligence." Available at <u>www.sas.com/en_us/whitepapers/data-management-artificial-intelligence-109860.html</u>
- Security Brief Magazine. (2016). "Analyze This! Who's Implementing Security Analytics Now?" Available at https://www.sas.com/en_th/whitepapers/analyze-this-108217.html
- UBM. (2016). "Dark Reading: Close the Detection Deficit with Security Analytics." Available at https://www.sas.com/en_us/whitepapers/close-detection-deficit-with-security-analytics-108280.html

