

## About Me

My CV

- +10 years of experience in information security
- Expertise: security monitoring, security incident response, security architecture and security operations
- Previously: security consultant @AtosConsulting
- Currently: Product Owner Cyber Defense Center @deVolksbank
- Chairman of FI-ISAC SOC/CSIRT workgroup
- Education: Bachelors degree in 2007, Masters degree in 2016
- Owner @Argos CSA

# **Security Operations Centers**

#### **Security Operations**

- Central point of knowledge & expertise on cyber defense
- Prevent, detect & respond

## Effective vs. Efficient

#### Effectiveness

 Effective (adj.) – Adequate to accomplish a purpose; producing the intended or expected result.



#### Efficiency

Efficient (adj.) – Performing or functioning in the best possible manner with the least waste of time and effort.

# Effective Cyber Defense

#### Definition

 Effective cyber defense means controls are functioning as designed, systems are secure and incidents are followed up directly to limit or negate impact



### **Measurement & metrics**

OFF

#### Measure

To establish effectiveness of the SOC, measurements are required SOC-CMM and MaGMa provide means to measure and improve

# SOC-CMM

### Maturing your SOC

- Designed to grow and mature your SOC
- Built on scientific research
- Measures capability & maturity
- Can be used to demonstrate ROI to SOC investments

## Creation

### **Multi-sector research**

- Cooperation with multiple SOCs
- Research focus on usability and diversity
- Model and tool developed

# SOC-CMM Model



# Example - Charter



# Input

#### Usage

- 5-point scale for scoring each parameter
- Advanced version also contains weighing feature
- Guidance provided for all maturity questions



# Input (example)

### People

- 1. Employees
- 2. Roles and Hierarchy
- 3. People Management
- 4. Knowledge Management

#### **3 People Management**

- 3.1 Do you have a job rotation plan in place?
- 3.2 Do you have a career progression process in place?
- 3.3 Do you have a talent management process in place?
- 3.4 Do you have team diversity goals?
- 3.5 Do you perform a periodic evaluation of SOC employees?
- 3.6 Do you have a 'new hire' process in place?
- 3.7 Are all SOC employees subjected to screening?
- 3.8 Do you measure employee satisfaction for improving the SOC?
- 3.9 Are there regular 1-on-1 meetings between the SOC manager and the employees?

5. Training and Education

3.10 Do you perform regular teambuilding exercises?

#### Importance Answer ▼ • A plan covering some roles is in place and operational Averagely Normal Partially -• A process covering some roles is in place, but not operational Normal A full process is in place, but not performing effectively • Mostly • Normal -Diversity goals have been formally defined and are met Fully • Normal • -Periodic evaluation is perform in a structured fashion Averagely Normal • -A formal process covering people, process and technology is in place Fully Normal Formal screening procedure and background checks applied structurally Fully --Normal --Employee satisfaction is measured in an ad-hoc fashion Sometimes Normal --Formal 1-on-1 meetings are regularly held, results are not structured Mostly Normal --Exercises are performed in an ad-hoc fashion Sometimes Normal

#### Comments and/or Remarks

3.11 Specify any comments or remarks you feel are important to this part of the assessment

# Output

#### Assessment output

- Detailed maturity & capability scoring
- Maturity & capability scoring per domain
- Results compared to target levels



# Output (example)

#### Full maturity & capability scoring



#### Aggregated domain scoring



# Alignment

#### **NIST alignment**

- Granular mapping of SOC-CMM to NIST CSF 1.1
- Details available as separate download

# Alignment (example)

#### Maturity & capability scoring across NIST CSF domains



# SOC-CMM Model



# Use Case Management

7802mm?u?750gd8uo2ss4MiPLac1housEYAdpusc:mm。	104000 1051201 - 69	●1-111~111~111~111~111~111~111~111~111~1
10%83%-2023576%3100PC611.968%-2025	hf: **==>>>*==* 30/5+	1914 8 244 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Dod+39、1××××××××××××××××××××××××××××××××××××	\$63H9±?C\17B <b>f?4</b> 2¥9Hk0441××363bi	*OM 62?36< .868M908 11 44 849
1 101000000000000000000000000000000000	> ∈ ΝΦΦ <sup>2</sup>	037b74706543j6764423 37b74706563j67642 1847857065947571423 1847865947571423
<b>5F</b> 11	4(au 2610 <b>4 °N 4 D</b> 9:27	r314+ r3227- r3227- r3227- r3227- r44 r3227- r327-
	n E i B F I I I I I I I I I I I I I I I I I I	рестемия» А. т. ротована в с 46 №
1806 K783 H 1 J C	1592176 <b>19 81</b> 592176 <b>19 81</b> 592176 19 82 823147	6 670 6 7547 7 357 3 7547 - 18 -
8 *** 5 000 %		2411422j6RC0640000000000000000000000000000000000
「 「 つうか」、 のでは、 ないので、 で		
5.5.4.2.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1		Brank Arthur State
11、11、11、11、11、11、11、11、11、11、11、11、11、	nct:?LACUTEPNO.	The state of the s
LEAUREGRAPHINE FAUX FOR STORES OF STATE		11-1-1-2-1-2-1-1-1-1-1-1-1-1-1-1-1-1-1-
000012744500888 978884911482148888 9788849198538888 0419814985388988 0419814985388988	11x 95 60 pz 2x0 9d y071W - 2 k316c0 14 k316c0 14	11 11 10 10 10 10 10 10 10 10 10 10 10 1
ала 1988-1992 (1996) 1989-1992 (1996) 1995 (1996) 1995 (1996) 1995 (1996) 1995 (1996) 1995 (1996) 1996 (1996) 199	↓ ↓ ± 22   ↓ ↓ 593 ↓ 593   ↓ ↓ ↓ 784 50   ↓ ↓ ↓ 9 6 10   ↓ ↓ ↓ ↓ 9 6 10   ↓ ↓ ↓ ↓ ↓ ↓ 10 10   ↓	* 5007 JO 00 20 10
37275984880; t C 286 the ADAFACE5589884	用10以くフト5日6一州2上編は3	столос 
1987年の1991日0000000000	N	
0 37V 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	<mark>//</mark> a	Pr\$Pa(a) J500 B00Nd(2) 1 J500
	a <b>C</b>	HARVARCHORNEL BORNER STAR
**************************************	B	A HOLE C
Anadian and a share with the second s	1a	n 2 0 1 2 0 1 0 1 2 0 1 0 1 2 0 1 0 1 2 0 1 0 1 2 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
こうくの しょう の しんしょう そうしょう ほく じょういん こうかん	]	P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P   P P P P P
LGY-LGY-LGY-RGC-GELGY-RGF-GELGEG 1-90-(197-2034-94-19-10-10-19-10-10-19-10-10	al Growers and A	15913 NPLOT NO REPORTS 134 CLOCK
HAR WALTERS IS ONLY JAPAS . SANGARANA	5559NU = 207 - 19 0 9 7 0 10 5759NU = 5664 0 7 0 1 = 59	N I SA ME SAN A COMPANY A DO NO COMPANY A DO N
4075133220RI14H08000*FTnE29RQ		9288974 - 14458 14469 1487 1489 148 148 148 148 148 148 148 148 148 148
741718379172884 74971837919884 74171837919884 74171837919884	21+1-05349A: AFERA 21+1-02-053602100 01-1-1-5-0602100 01-1-1-5-0602100 01-1-1-5-060210 01-1-5-060210 01-1-5-060210 01-1-5-060210 01-1-5-060210 01-1-5-060210 01-1-5-060210 01-1-5-060210 01-1-5-0602000000000000000000000000000000000	A AGALONANA ANA ANA ANA ANA ANA ANA ANA ANA AN
558 0514 au 464 9 26	· · · · · · · · · · · · · · · · · · ·	CHARLON CARACTER CARA
аяна (р. 186 с. мнови - Акойнан. Аверикана каракарана каранара са	0~9~4385+6419375	CHARGE BEAR STREAMER STREAMERS
2601 2601 2601 2602 2602 2602 2602 2602		
900		SPR? 1C = 0 S BE S 2007 - 10 NO2 PARTS 1C = 0 S BE S 2007 - 10 NO2 PARTS 1 NO
scologication of the second seco	0%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%	5 <b>10</b> 5 <b>10</b> 5 <b>1111111111111</b>
N   X   X   X   X   X   X   X   X   X	RpyR152-cc2? 12t3	5m22F0884332H11454XEU009
50000 1000 1000 1000 1000 1000 1000 100	7011?A?	rations, the siski
9 유전에 전쟁 유럽 보장 수 명 입 미 1 김 수 있다.	529.44	181, 031, 01, 531, 01, 531, 12, 50, 04, 04, 04, 04, 04, 04, 04, 04, 04, 0
	111723W211161=1sr	алан <b>лас</b> . Флартияст и в
a? D288H9 Construction of the series of the	1T6512100k90FW85 1N100215760CH12	
80 D? > 0? Fi 96 092 CI?= Glijun???? 450 du@ o212 128039 noPenii??s22342a25>BK?	20 cd 0178105 PMT5 J9 20 cd 0178105 PMT5 J9 20 0 0749 23	111 46 J 50 8 49 8 1 7 5 9 5 5 9 5 7 5 7
сла імомска зохах очат фанамарністі осо са со «Х. — нажемина очат фанамарністі осо са со «Х. — нажемина»	XHFANTS	
F##1,4260×8年1,91200月20日20月19975×	HO NO US STORY Y' XLOG	HE: SEERSEN X SARA RELOVAD

# MaGMa Development

#### Creation

- Created as a joint effort of Dutch banks as standard for use case exchange
- Based on existing ABN AMRO framework



# MaGMa Use Case Model

#### Layers

- MaGMa use cases have layers
- From high-level risks to low-level implementation
  - L1: Risks
  - L2: Tactics
  - L3: Implementation



# MaGMa



# MaGMa UCF Tool

#### Usage

- Supported by the MaGMa UCF tool
- Predefined use cases based on MITRE ATT&CK framework
- Provides a means to structure and measure use cases



# Wrap-up

### Key take-aways

- Increasing SOC effectiveness requires insight and improvement using measurement
- SOC-CMM and MaGMa provide such insight
- Free download / free usage



# Final remark

#### Validation

- Red team or it didn't happen
- Good scores on paper are great, but how does the team deal with an actual attack?



