# Trellix

## Al & Adaptive Security Operations



## **Advancing Security Operations**

#### Creating an Adaptive Model

Security operations (SecOps) **must find ways to adapt**. To do so, SRM leaders should adopt an exposure-based approach to operations, promoting business relevance. As a primary function, SecOps is **responsible for maintaining visibility** across technology estates for the purposes of monitoring and responding to potential threat activity, and **actively advising and reducing risk through careful orchestration of controls**. To achieve its goals, it's equipped with technologies and services aimed at providing deep visibility of technology networks, assisting with diagnostic outcomes and, in some cases, control implementation.

• 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability



### **Security Operations Revolution**

#### **SOC 1.0** Foundation + Discovery

- **Basic** Security concepts, **Legacy AV**, Firewalls
- Appliances **not connected** or talking to each other
- Correlation often after post mortem forensics

SOC 2.0 XDR - Operational

- Alerts correlated and accurately diagnosed
- IR Focused
- Best Detection
- Best Response countermeasures and Playbooks
- Limited in Proactive approach, Intelligence is alert driven (data-enrichment)

#### SOC 3.0

Aimed at Longevity Adaptive platform (XDR+Insights + AI)

- **Proactive**, **and Adaptive**, measure and check-up (Threat Intel, Threat modeling, Attack surface monitoring, automated red teaming etc.)
- In control of your Security posture, limit the chance of any of breach to occur and have an adaptable mindset to limiting RISK.



### **SOC Maturity Journey**



Increasing Decision Speed, Effectiveness, and Business Value



### **SECOPS Readiness** (Adaptive XDR)

#### **Pro-Active/ Adaptive (Insights) XDR Platform** WHY NOT HERE? **CURRENT APPROACHES Proactive** Reactive Attacks occur in **Attacker** Attacker Remediation You Response the wild searches victims aimes at Are Hit YOU

'Thanks to Trellix Insights, we can confidently answer questions from upper management, such as 'Are we protected against this?' It helps us focus on what to do next and informs our cybersecurity strategy." — Karsten L., CISO at SMS Group



### **Leading Security Forward**





### **AI Drivers**





### **AI: Reduce Risk**

#### Protect Data exposure through GenAl Inter

≡ Tre	DLP Incider	t Manager Dashboards Classificatio	n DLP Policy Manager	DLP Case Management DLP Discover Appliance M	magement DLP Cap	sture Policy Catalog System Tree Queri	es & Reports		
ata Protection									
DLP Incid	ent Manager								
alytics Inciden	n Uat Incident Tasks In	diant Watery Custom Attributes							
resent: Data in usa/motic	et v Filters:	luie Set Indd No Filter V Ro F	nit Type iber 🗸 🗸	User Time Account Destinations No Filter III No Filter V Ro Filter	Classific No File	alions - Sher Filters			
Top 10 Rule Sets			Top 10 Incident Types			Top 10 Users with Violations			
	Number of DLP Date	In-use/mation Incidents :		Cloud Protection 2	7	# None	268		
50	3 100 15	0 200 250 300		Web Protection 21		sam@sc.com	91		
-				Email Protection		E MaryginGutern	83		
	-			Network Share Protection		ededwards@colutiondelta.org	60		
and the second s	129-10 C			Ferrovable Storage Protection		edgsolutioncenturg	58		
				Claboard Protection 2		E None-0	30		
R PCI Contan	t	210		Printer Protection		# sam@solutioncentr.org	32		
high importan	d ruka	216		Screen Capture Protection		mary@solutioncentcorg	17		
HAY US PIL CON	rbent	101		Total 7.		a marymason@solutiondelta.org	0		
HIY ODPR. con	tunt	60				Total	//1		
nitor HIPAA co	intent	59							
ck Source Coo	50	63							
Top 10 Number of Incidents per Week			Top 10 Destinations			Top 10 Classifications			
			Destination	Number of DLP Data In-use/rection Incidents :		# PCI	.343		
31			box	176		• US PIL	576		
			www.csm-bestoenten.org	152		· HURA	20		
			Dvapbax	59		None	52		
* I I I			Fiet Avellable	41	(	Source-Code	54		
			-grass.com	37		e PCI (Custore)	53		
1	11		10.1.20.63	23		# US PII (Custorn)	24		
			None	22		# Seurce-Code (Custom)	22		
	14		sharepoint	21		# Heeting Recordings	19		
7/1/19 1/1/20 7/1/23 1/1/21 7/1/21 1/1/22 7/1/22 Documed (UTC)			onedrive	19		Total	35		
			Mare	202			994		
			Total	771					
ing 771 out of	771 events								
er ID	Reporting Anduct	Occurred (UTC) V Severity	Incident Type	User Principal Name Disernal User Logon Name (domain), Computer	Name Adual Ad	tion Rules	Rule Sets	CassFicences	Distination
1	DLP far Windows	December 28, 2022 10:0010   Celecal (4)	Email Protection	ebedwards@solutiandeita.er SOLUTIONDELTWadedwards DLPCI7-9	Block	Bieck K3 content says by entail	Block PCI Content	PCI (Custom) (114)	Selected feitz-
	DUP far Windows	Deceviter 28, 2022 9-53-06 😐 Major (3)	Clabsard Protection	eledvards@solutiondetta.er SOLUTIONDELTA/ededvards_DUPCJ74	Pre Activ	<ul> <li>Aut Py US PII servers pasted inte any applications</li> </ul>	Justily US PEI content	US PII (Custore) (22)	watersk.com
	DLP far Windows	December 25, 2002 5:52:00 🔮 Major (3)	Clipboard Protection	ededvards@esiztendeita.er_SOLUTIONDELTA\ededvards_DLPCUTIG	No Action	<ul> <li>3.or/y US PE consent pasted into any applications</li> </ul>	Justify US PEI content	US PE (Custom) (22)	autook.eoa
-	OLP for Windows	December 28, 2022 5:31:00 👄 Mejor (3)	Clipboard Protection	ededvards/jectusondeita.or SOLUTSONDELTA/ededvards DLPCUT-0	E Block	Block pasting of Sensitive information into Neeting C	hat 5 Online Newting protection.J	L US VII (Custorn) (22)	10077-808
	DUP for Windows	December 28, 2022 9:31:00 ● Major (3)	Email Protection	eded-ands@solutiondeita.or SOLUTIONDELTA\ededvands DLPCUT-0	Block	Prevent emailing Heating Recordings	Online Meeting protection	Meeting Recordings	aslutiondelta,
2	DLP for Windows	December 29, 3022 9-31/00 🔮 Major (3)	Entail Protection	ededvards@solutiondetta.ar \$0LU/T30ND\$LTA\ededvards DLPCLT-0	Buck	Prevent extailing Heating Recordings	Coline Meeting protection	Meeting Recordings	solutiondelta.
	DLP far Windows	December 29, 3522 9:51:00 🔮 Major (3)	Email Prosection	ededuarde@solutiondebs.or GOLUTIONDELTA/jededuarde DLPCLT-0	Diark .	Prevent extailing Heeting Recordings	Online Meeting protection	Weeting Recordings	epi.ciatete.c

#### Reduce risk of data leakage in GenAl



## **Al: Leverage Capability**

Al Augmented Personnel

Employees utilizing for their jobs LLM's significantly outperformed those who did not.

**25.1% increase in speed** 



+40% improvement in output quality

12.2% more tasks completed

Based on the research by Harvard Business School that was published recently.

#### **Skill Leveling Effect of Al:**

Al augmented staff demonstrated a skill-leveling effect where lower-performing consultants experienced a 43% performance boost, diminishing the performance gap between top and bottom consultants.



### **AI: Enhance Posture**

#### Security Content Creation

rule CVE\_2018\_4878
{
 rmeta:
 description = "Yara rule for
 CVE-2018-4878"
 author = "Your Name"
 reference = "CVE-2018-4878"
 strings:
 \$string1 = "swf" wide ascii
 \$string2 = "AS3" wide ascii
 \$string3 = "LoaderInfo" wide ascii
 condition:
 \$string1 and \$string2 and \$string3

Create a Trellix Endpoint Security Expert Rule to block JavaScript files from launching in the user directory

Create a Yara rule for CVE-2018-4878

S alert tcp any any -> any any (msg:"DoS Attack against Docker Honeypot"; flow:established, to\_server; content:"GET"; nocase; pcre:"//containesV(.\*V)\*(w+)\.json/"; sid:1000001; rev:1;) ExpertRule { Class "Process" ld 1000001 Rule { Process { CommandLine { Include { -v "\*.js" } Target { FilePath { Include { -v "%USERPROFILE%\\\*" } Reaction { Block

#### Create a SNORT Rule for DoS attacks using Docker honeypots

Trellix

## Where Do You Want to Start Your Revolution?





