Advance Threat Hunting 24×7: Fighting Cybercrime with Artificial Intelligence



April 2019 Nikitas Kladakis Information Security Director





Cybersecurity Challenges



Intelligence Drive Defense

Cybersecurity Challenges





Technology Evolution - IoT



at

v),+function(a){"use strict";function b(b){return this.each(function()) we[b]()}) var c=function(b){this.element=a(b)}; c.VERSION="3.3.7", c.TRANSITION_DURATION=150, c.pro down-menu)"),d=b.data("target");if(d||(d=b.attr("href"),d=d&&d.replace(/.*(2=#[^\s]*\$)/,"")), st a"),f=a.Event("hide.bs.tab",{relatedTarget:b[0]}),g=a.Event("show.bsg -functi aultPrevented()){var h=a(d);this.activate(b.closest("li"),c),this.a {fun rigger({type:"shown.bs.tab",relatedTarget:e[0]})})}},c.prototype & (1)>.active").removeClass("active").end().find('[data-toggle="tab'] ia-expanded",!0),h?(b[0].offsetWidth,b.addClass("in")):b.removeC).find('[data-toggle="tab"]').attr("aria-expanded",!0),e&&e()}va e")//!!d.find("> .fade").length);g.length&&h?g.one("bsTransition" var d=a.fn.tab;a.fn.tab=b,a.fn.tab.Constructor=c,a.fn.tab.noCon# show")};a(document).on("click.bs.tab.data-api",'[data-toggle="tag se strict";function b(b){return this.each(function(){var d=a(thi typeof b&&e[b]()}) var c=function(b,d){this.options=a.extend({}; ,a.proxy(this.checkPosition,this)).on("click.bs.affix.data-api" wll,this.pinnedOffset=null,this.checkPosition()};c.VERSION="3.3.7"; larget=a State=function(a,b,c,d){var e=this.\$target.scrollTop(),f=this.\$elem osition bottom"==this.affixed)return null!=c?!(e+this.unpin<=f.top)&&"botty"</pre> affix-top !=c&&e<=c?"top":null!=d&&i+j>=a-d&&"bottom"},c.prototype.getPinned RESET).addClass("affix");var a=this.\$target.scrollTop(),b=this this.\$tar http://www.settimeout(a.proxy(this.checkPosity) &"bottom nt.height(),d=this.options.offset,e=d.top.f=d eof e&&(e=d.top(this.\$element

Global Interconnection





Complex Infrastructure

© netl





Demanding Business





Compliance & Regulations





Limited Resources





Explosion of Data





Sophisticated Attacks





Advance Malware



יייין אינטיין א and a brate or a set and the analysis the set of a set of the set of a set 01110 1 of the 1 of 1 101 11011 10110101110 1 101 10 01 101 01

111101-01111-12 101018 3151961100 109090109516197878784 698 989591540914

0001 1 110 01010101101 1 11 101010001 1 101

sign og i terer at not ing og er de tereraioterer perot er

100001000010010101010101010101010010 110 10 101101011 610 01

101 101-130311 oro 101010 1010101 1010101 101 01031

totose tun antescrimer sub later (1.10) (e) equiption (1.10) of a second (1.10) of a seco 1010101 11 303(20010101 3101111201 1010101 1001 de 10 de 1

Threat Landscape





Common Source of Cyber Threats

- Nation states
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists
- Business competitors
- Disgruntled insiders







unie: ποι προτεί το στο ποιοχρηπού του Αιχαρίας στο του ποιοτικο στο στο προτεί το που το που το που που το τ στο προτεί το ποιοτικό το ποιοτημού από το ποιοτημού το προτεί το ποιοτημού τ ποιοτημού το ποιοτημού τ ποιοτημού το ποιοτημού τ ποιοτημού το ποιοτημο







Organizational

Cyber Kill Methodology





With 'Hands on Keyboard' access, intruders accomplish their original goals

Impacts



Last week, British Airways announced that the personal and financial information of 380,000 of their passengers had been hacked. Passenger names, home addresses and credit card data were all stolen during the 15-day security breach, catching BA flat-footed.





A massive breach of Marriott guest data that was thought to have affected around 500 million people may have had a smaller impact than initial reports suggested, but also exposed the passport numbers of several million people, the company **announced on Friday**.

Marriott first disclosed the breach on November 30, saying hackers targeted its Starwood reservation system and accessed the personal information of hundreds of millions of guests who had stayed in the hotel chain's properties since 2014.

Intelligence Driven Defense





Intelligence Driven Defense

Centralize

Operations

Focused

Organization

SOC Services

Executive Buy-in

Detection

Monitoring



Developed by Lockheed Martin

Centralize Operations: Intelligence Driven SOC





Monitor Threats: Advance Threat Hunting



 Threat hunting involves searching through large volumes of data to identify bad actors and threats to an organization's IT infrastructure

 The goal is to prevent attacks before they happen and eliminate or minimize their effects



Threat Hunting Technologies / Services









Artificial Intelligence (AI): a software that perform tasks normally requiring human intelligence, such as decision-making





- Big Data
- Machine and Deep Learning Algorithms
 - ✓ Network Behavior Analysis (NBA)
 - Users and Endpoint Behavior Analysis (UEBA)





- Network behavior analysis (NBA) analyze traffic and noting unusual actions or departures from normal operation
- After establishing a benchmark for normal traffic, the NBA program passively monitors network activity and flags unknown, new or unusual patterns that might indicate the presence of a threat.
- NBA can also monitor and record trends in bandwidth and protocol use

• NBA use:

- Data volume (octets, packets)
- Flows (number, duration, size, service type)
- Communication matrix (src/dst IP, src/dst ports)
- Packets (size, flags)



NBA use cases



- **DoS/DDoS** attacks
- Large Outbound Transfer
- New Services
- Unusual Communication



Users and Endpoint Behavior Analysis (UEBA)



 UEBA analyzes user and device activity to detect malicious insiders and determine if a user's credentials or a device have been compromised

• UEBA adds user and device context to network, log, vulnerability and threat data to more quickly and accurately detect attacks





• UEBA use:

- Traffic around access, authentication, and account changes
- User behavior on the network
- Endpoint and application agent & logs, such as from Windows or Linux, and SAAS applications
- Endpoint Behavior

centralen occumy ministryence bourd Offinses Lag.Activity Activity Assets Foremics Reports Risks Valmerabilities Admin Über Analytics						adre	t V Rep V		System 1
uick insights	Search for User		0,						
unitored Users	Current High Risk	Isense Events (last hour)			Offenses Generated (last hour)				
32	7	1.6k			7				
System Score (Last 24 H	lours)	Risk Category Breakdown (Last Hour)			Recent Sense Offenses				
41895			User Geography User Privi	lege	Offense # 3828 User: nobody		abo	aut 12 ho	um ago
30000					Event Count: 448	Flow Count: 0	Magnitu	dia: 3	
20000				Offense # 3827		abo	about 12 hours ago		
21.30 00.00	06.00 12.00 18.00 21.30				Event Count: 665	Flow Count: 0	Magnitu	de: 3	
fost Risky Users (Overa	all Score)	Most Suspicious Users (W	indow Score)	-	Watchlist				
John	4357 💿	milignou 📉	+390	۲	John		4.4k	7	Θ
Suman	4341 🖲	Jane	+360	۲	Natasha		4.3k	И	Θ
A Maturka	4241		.260		Jose	•	4.3k	И	Θ
Natasria	4341		+360	-	Jane		4.3k	И	Θ
Jose 🗭	4341 💿	Natasha	+360	۲	Matthew		0.2	И	Θ
Jano	4335 💿	Suman	+360	۲					0



- Large Outbound Transfer by High Risk User
- User Account Created and Deleted in a Short Period
- High Risk User Access to Critical Asset
- Replication Request from a Non-Domain Controller
- User Access from Multiple Hosts
- 0-day Malware Detection
- non Malware Detection



Knowledge Management

- Threat Intelligence Management
- Cyber Analyst Training
- Cyber Threat Analysis Services





Proactively Defend: Analysis and Mitigation





Measurement and Accountability



- Penetration Test
- Information Security Audit
- Vulnerability Assessment



Thank you for the attention!

