Asking the Right Questions

A Data-Driven Blueprint for Effective Defense



About Me

20 years in cyber defense

Former CTO, Raytheon Cyber

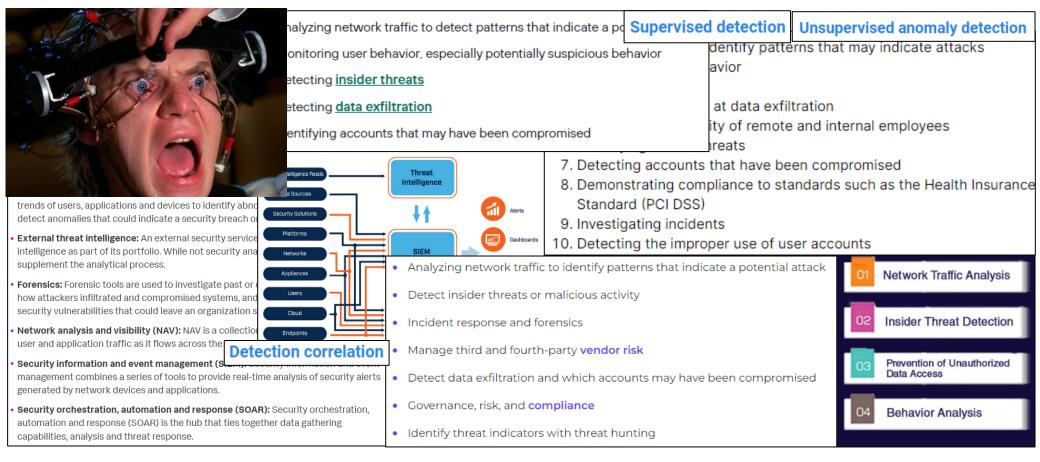
Co-inventor, Automated Internet threat detection and mitigation system and associated method







Analytics in Cyber Defense







The Right Questions

- 1. What do I have that is worth protecting?
- 2. How might that value be degraded or destroyed?
- 3. How likely is that to happen?
- 4. How much work am I willing to do to keep that from happening?
- 5. What don't I know?



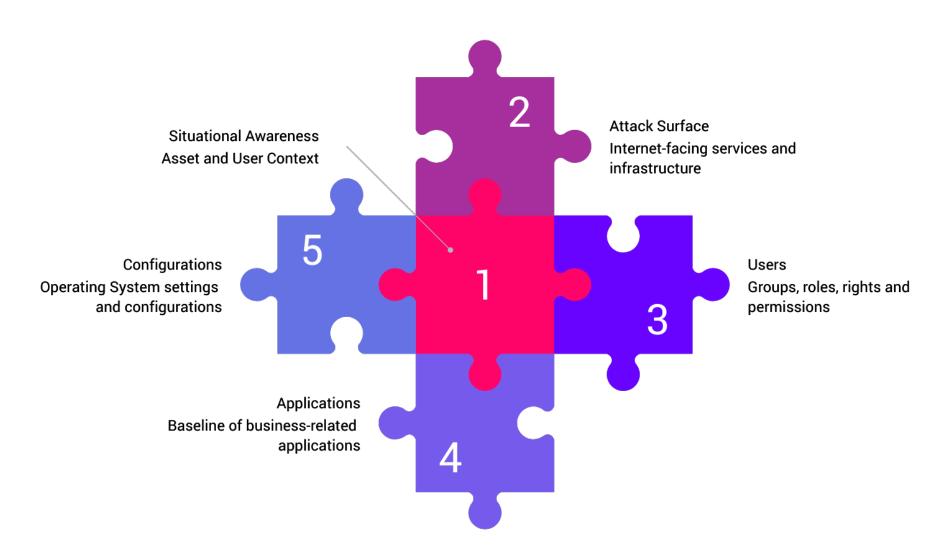


Blueprint for a Better Night's Sleep

- Know what you have
- Understand how it is being used
- Know what is leaving your network
- Revisit your assumptions (constantly)
- Trust but verify
- Learn from what you have done
- Measure and improve



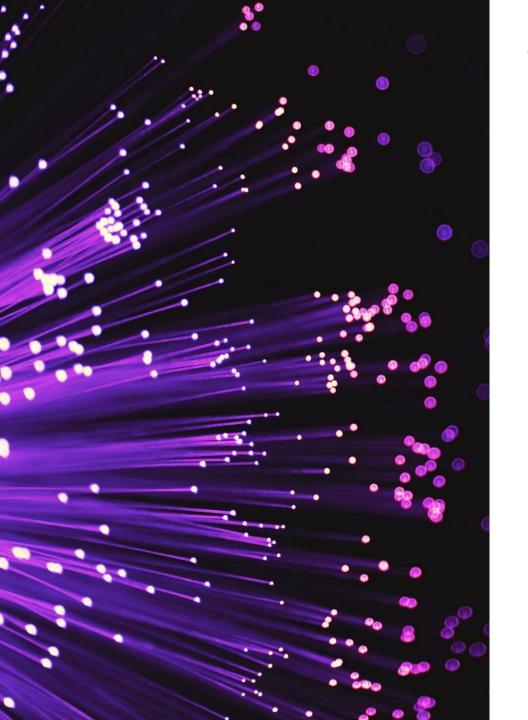
What Do You Have?



How Are Your Assets Being Used?

- Application control
- Executables, scheduled tasks, autoruns, scripts
- Administrative functions and commands
- Login activity





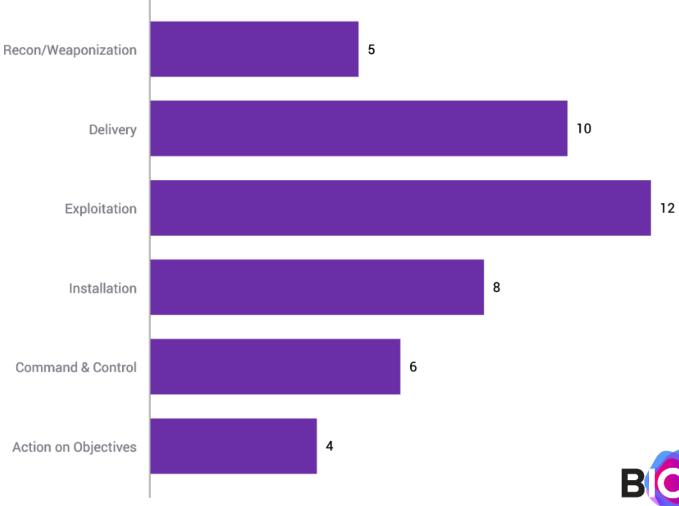
What Is Leaving Your Network?

- Watch your outbound communications
- Long term retention is not as important as complete data
- New implementations of DNS, HTTP, TLS are making this harder



How Many Chances Do You Have?

Detection Capabilities by Kill Chain Phase





Are You Sure Your Defenses Work?

1

Atomic tests for your analytics

2

Purple team assessments for your enterprise logging and detections



Red team assessments for your preventative controls



Adversary emulation for your enterprise controls and detections











Visualizing Detections with MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Supply Chain Compromise	Control Panel Items Service Execution	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture Credential	Password Policy D T1056 Score: 5	Logon Scripts	Input Capture	Domain Fronting Uncommonly	Data Compressed	Endpoint Denial of
Drive-by Compromise	PowerShell		Extra Window Memory	Control Panel Items	Dumping	Metadata: tem De-Applicable to: client	Application	Network Shared Drive	Used Port	Data Encrypted	Service Network Denial
Spearphishing	Regsvr32	Logon Scripts Image File	Injection	Extra Window Memory Injection	Credentials in Registry	endpoints Sy-Detection score: 4	Deployment Software	Email	Remote Access Tools	Exfiltration Over	of Service
Attachment Exploit Public-	Rundli32	Execution Options	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and	D -Overlay: Detection System Owner/User	Distributed Component	Collection Audio Capture	Commonly Used Port	Command and Control	Data Encrypted for Impact
Facing Application	Scripting Scheduled Task	Application	AppCert DLLs	Process Injection	Relay	Discovery	Object Model	Automated	Data Obfuscation	Channel Automated	Data Destruction
External Remote	User Execution	Shimming Scheduled Task	Image File Execution	Regsvr32 Rundll32	Account Manipulation	Account Discovery Process Discovery	Exploitation of Remote	Collection Clipboard Data	Standard Application Laver	Exfiltration	Defacement
Services	CMSTP	Accessibility	Options Injection	Scripting	Brute Force	Custom Maturals	Services	Data from	Protocol	Data Transfer Size Limits	Disk Content
Hardware Additions	Command-Line Interface	Features Account	Application Shimming	Image File Execution Options Injection	Credentials in Files	Configuration Discovery Application Window	Pass the Ticket Remote	Information Repositories	Communication Through	Exfiltration Over	Wipe Disk Structure
Replication Through	Compiled HTML File	Manipulation	Scheduled	Timestomp	Exploitation for Credential	Discovery	Desktop Protocol	Data from Local System	Removable Media Connection Proxy	Alternative Protocol	Wipe Firmware
Removable Media	Dynamic Data	Applnit DLLs Authentication	Task Accessibility	Obfuscated Files or Information	Access	Browser Bookmark Discovery	Remote File Copy	Data from	Custom	Exfiltration	Corruption
Spearphishing Link	Exchange Execution through	Package	Features	Binary Padding	Forced Authentication	Domain Trust Discovery	Remote	Removable Media	Comr Contr	legen	d
Spearphishing	API	BITS Jobs	Applnit DLLs	BITS Jobs	Hooking	File and Directory Discovery	Services Replication	Data Staged	Custo Crypt #ffcece	Tech. ref. for 1	1 group X
via Service Trusted	Execution through Module Load	Bootkit Browser		Bypass User Account Control	Input Prompt	Network Service	Through Removable	Man in the Browser	Proto		
Relationship	Exploitation for Client Execution	Extensions	DLL Search	CMSTP	Kerberoasting Network Sniffing	Scanning Network Share Discovery	Media	Screen	Data #ff0000	Tech. ref. for 1	1 groups X
Valid Accounts	Graphical User	File Association	Order Hijacking	Code Signing Compile After Delivery	Password Filter		Shared Webroot	Capture Video Capture	Gene #ff8f00	Tech. in group	+ detection X
	Interface	Component Firmware	Privilege Escalation	Compiled HTML File	DLL Private Keys	Peripheral Device Discovery	Taint Shared Content		Fallba #8BC34A	Tech. in detec	etion ×
		womani siriinii C		Component Firmura		A STATE OF THE STA	ou.noin		N. 4. (14)		

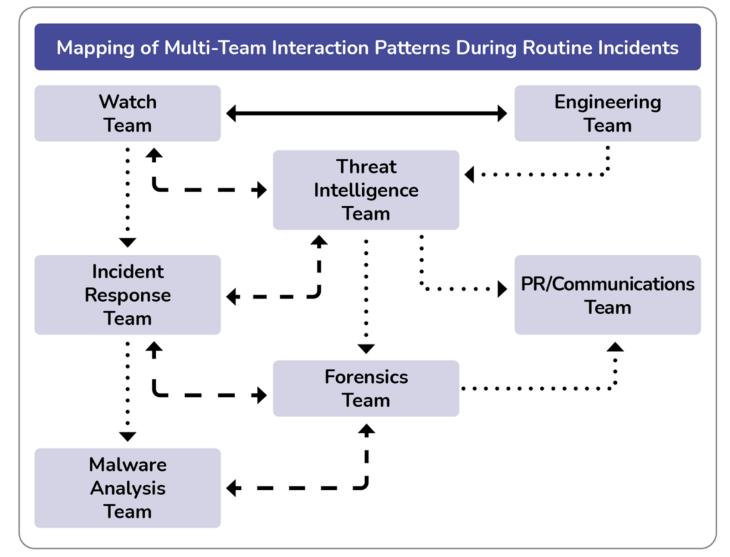


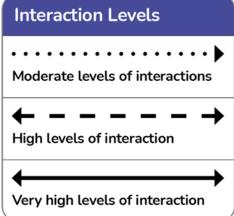
Is Your Team Collaborating?

- Increase trust and shared knowledge of unique expertise (SKUE)
- Reduce friction in crisis situations
- Promote learning and teamwork
- Track when and how often your team collaborates



Mapping Team Interaction

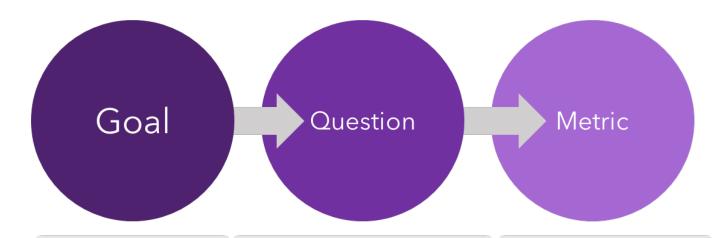




Note: At higher levels of incident severity, interactions between teams increase in intensity. Also, teams that do not generally interact begin to interact more frequently.



Are You Improving?



"Reduce successful phishing attacks."

What is our target range?

What impact constitutes a successful attack?

What attempt constitutes a successful attack?

KPI is <5 per week

Number of infections

Number of messages delivered

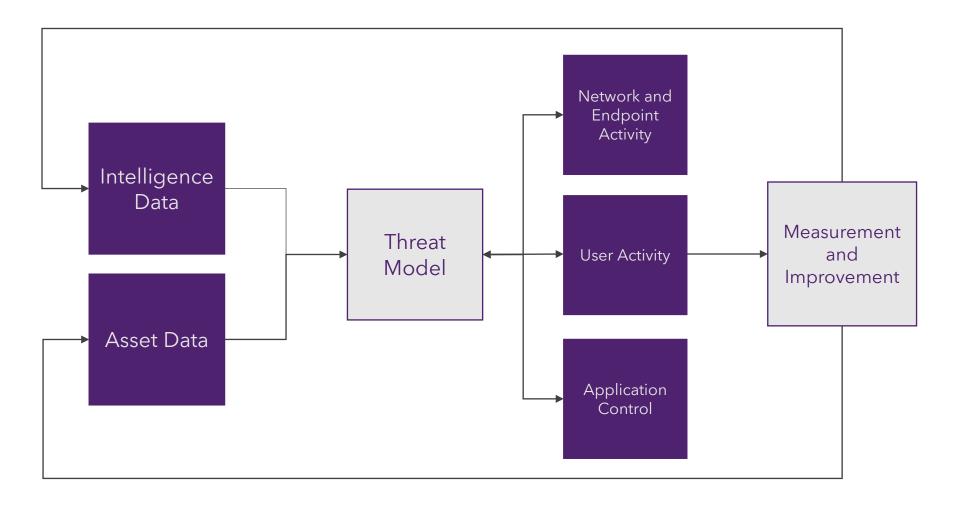


What Are You Assuming?

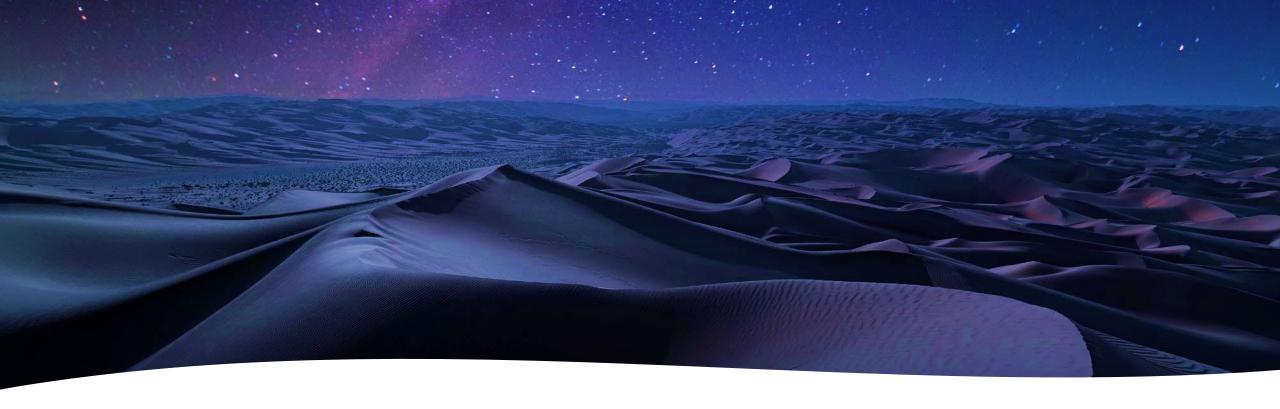
- Security tools will save you
- Your data is not desirable to an attacker
- Users will not find a way around your security
- Security is more important than productivity
- You know what's going on



Blueprint for a Data-Driven Defense







Summary

- Analytics are decision support, not easy buttons or products.
- They can give defenders superpowers if driven by the right questions.
- Collect some data. Process, interpret, repeat.
- Start with your goals and security "hygiene", not vendor use cases.



Thank You

Email: <u>mark@bioniccyber.com</u>

LinkedIn: https://www.linkedin.com/in/marko16/

Web: https://bioniccyber.com

