Threat Detection Webinar

Reduce Time to Detect and Contain Cyber Incidents

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Exciting times for threat detection

Offensive Zone

- Explosive growth of cyber crime
- Rapidly expanding attack surface
- Rise of ransomware and attack automation
- Diverse adversaries
- Increasing geopolitical threats

Defensive Zone

- Board level awareness and support
- New and innovative security products
- Emerging technologies
- Rapidly expanding attack surface
- Serious shortage of cyber security talent
- Poor global performance for cyber detection and response
  - >190 days MTTI
  - >66 days MTTC

Reducing time to detect and contain incidents

Opportunities for improvement

Big Data Analytics

Real-time security insights across the large and growing data of the modern enterprise

Emerging Technologies

Machine learning and behavior anomaly detection beyond traditional event correlation

Enhanced Use of Threat Intelligence

Integration of threat intelligence correlation across data sources

Visibility into IoT & OT

Behavior based analytics for Internet-of-Things and Operational Technology

Risk-Aligned Threat Detection

Focus detection on top risks, accelerate investigation and response, and report on capabilities and operational metrics

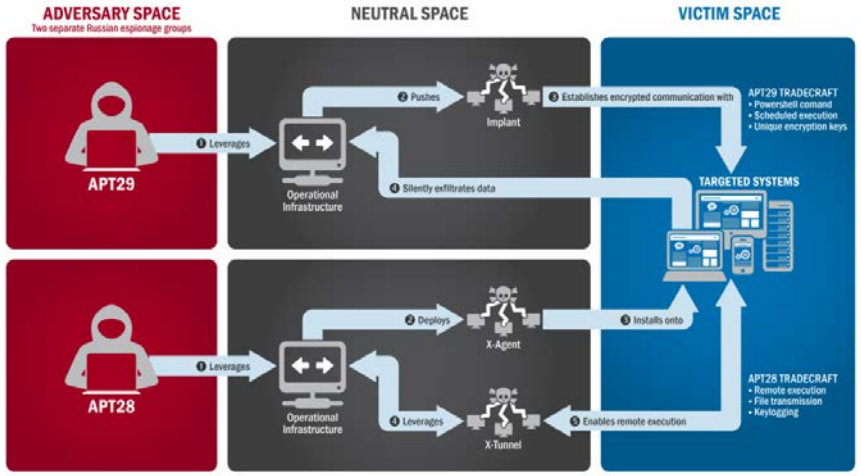
Risk-aligned threat detection approach

1 Identify top risks

Top Cyber Risks

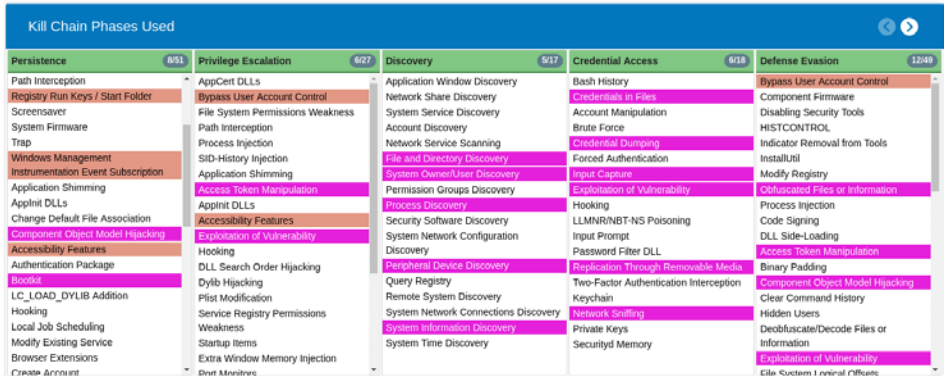
- Industry Risk Profiles
- Enterprise Risk Register

2 Define related attack scenarios



Source: DHS & FBI Joint Analysis Report 16-20296A

3 Map threat activities



4 Develop Analytics

5 Monitor, Investigate & Respond

6 Capture Metrics & Inform GRC

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Identify Top Risks

Example: Healthcare Delivery Organization (HDO)

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Top HDO Cybersecurity Concerns

1

Patient Safety

- Medical device (IoT) Security
- Integrity of healthcare data
- Availability of healthcare data

2

Availability of Healthcare Data and Systems

- Ransomware
- Denial of Service

3

Breach of Protected Health Information (PHI)

- Phishing
- Malware
- Vulnerable software
- Shadow IT
- Insider

4

Business Associate Security

- Compromised vendor or partner

5

Data Theft (non-PHI)

- Research data
- Proprietary information
- PoS payment information

HDO Threat Actors & Motivation

Nation State

Espionage
Theft of intellectual property and proprietary information to benefit nation's healthcare

Warfare
Sabotage critical infrastructure as part of political conflict or agenda

Hacktivists & Terrorists

Hacktivism
Cyber-attacks to promote political agenda or social change

Terrorism
Sabotage of critical infrastructure for terrorism

Cyber Criminals

Crime
Steal or ransom data for financial gain
(e.g. black-market sale, fraud, extortion)

Outsider

Personal
Data theft or healthcare sabotage for personal or ideological reasons (e.g. revenge, malice, euthanasia, family concern)

Insider

Personal
Data theft or healthcare sabotage for personal or ideological reasons

Accidental
Unintentional or negligent actions

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

HDO Cyber Risk Categories

Confidentiality

- PHI
- Financial information
- Research data
- Proprietary information

Integrity

- Medical device functionality
- Clinical systems and applications
- Patient records and healthcare data
- Financial information

Availability

- Medical device functionality
- Clinical systems and applications
- Patient records and healthcare data

Safety

- Medical device functionality
- Clinical systems and applications
- Patient records and healthcare data

HDO Major Asset Classes

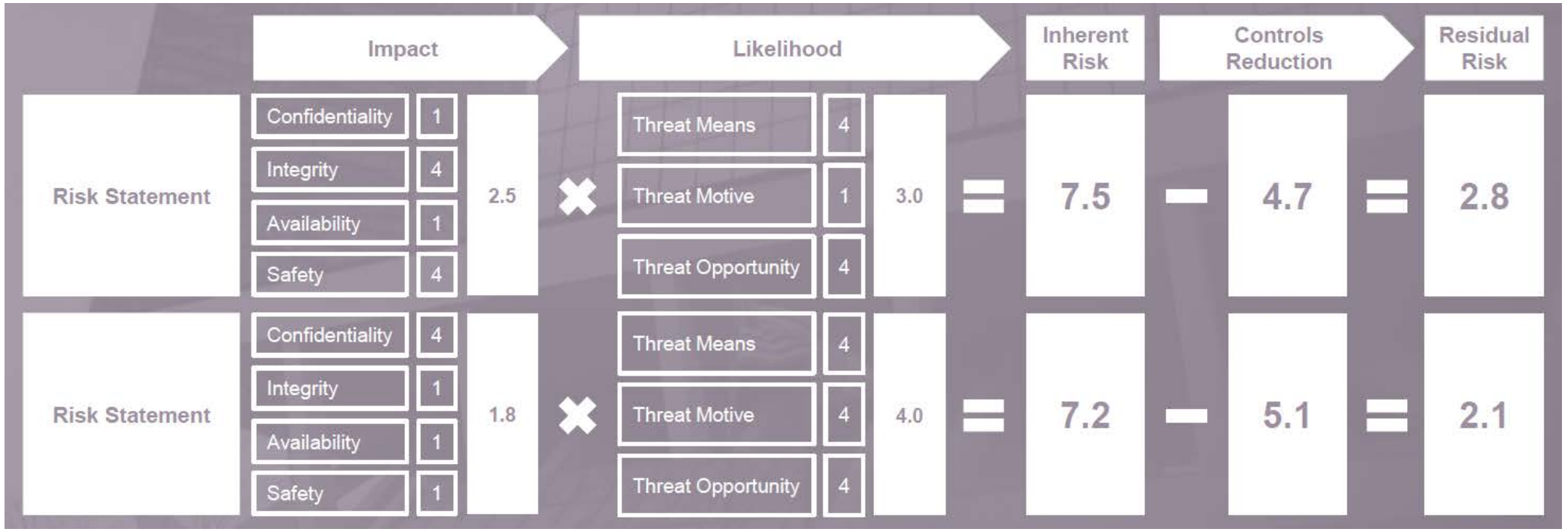
Asset Class	Examples
Active medical device (AMD)	Insulin pumps, heart defibrillators, machines that emit radiation, or any equipment that sustains life
Passive medical device (PMD)	Vital signs monitors, pulse oximeters
Healthcare information system	Electronic Medical Records (EMRs), Electronic Health Records (EHRs), Personal Health Records (PHRs), clinical and administrative systems
Financial system	Billing, Point of Sale (PoS)
Identity and access management (IAM) system	Active Directory, SSO
Internet of things (IoT)	Pharmaceutical distribution, environmental controls
Operational technology (OT)	Power, HVAC, elevators, physical security technology
IT networking technology	Routers, switches, wireless access points
IT security technology	SIEM, endpoint protection, IDS/IPS
Office & mobile technology	Email servers, file servers, workstations, printers, mobile devices

HDO Top Cyber Risk Statements

1. Critical data is encrypted in a ransomware attack, disrupting healthcare delivery operations, resulting in permanent injury or death, or significant financial loss
2. Healthcare information system availability is denied, disrupting healthcare delivery operations, resulting in permanent injury or death, or significant financial loss
3. PHI is breached, exposing confidential information, resulting in financial loss
4. AMD is modified to fail to deliver the necessary treatment or to deliver the incorrect medicine or incorrect dosage, resulting in permanent injury or death
5. AMD is modified to cause harm, such as delivering an electrical shock or emitting radiation, resulting in permanent injury or death
6. EHR is modified to contain false information, compromising healthcare treatment or medical or surgical procedures, resulting in permanent injury or death
7. PMD is modified to fail or to report false readings or alerts, compromising healthcare treatment or medical or surgical procedures, resulting in permanent injury or death
8. Work orders are altered causing nurses or other physicians to administer incorrect medicine or incorrect dosage, resulting in permanent injury or death
9. Work orders are altered causing incorrect surgical or medical procedures, resulting in permanent injury or death
10. Medical inventory system is modified, causing medical dispensary systems or clinical staff to provide incorrect medicine or incorrect dosage, resulting in permanent injury or death

Risk Prioritization

Many ways to prioritize risk – this example uses a scoring method and considers controls and residual risk



OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Define Related Attack Scenarios

What are the most likely attack scenarios for the risk statement?

Example Risk Statement:

Critical data is encrypted in a ransomware attack, disrupting healthcare delivery operations, resulting in permanent injury or death, or significant financial loss

Ransomware attack scenarios

- Phishing attack: malicious email attachment
- Phishing attack: malicious email link
- Vulnerability: internet facing system
- Vulnerability: laptop on untrusted network
- Compromised vendor/partner: software update
- Compromised vendor/partner: network trust relationship
- Malicious insider: intentional
- Etc.

Map Threat Activities

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Define threat activities by attack phase for the selected attack scenario

Models available to assist

Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

CIS Community Attack Model

- Initial Recon
- Acquire/Develop Tools
- Delivery
- Initial Compromise
- Misuse/Escalate Privileges
- Internal Recon
- Lateral Movement
- Establish Persistence
- Execute Mission Objectives

MITRE ATT&CK

- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command & Control

Cyber Threat Framework

- Preparation
- Engagement
- Presence
- Effect/Consequence

Leverage ATT&CK

Persistence	Privilege Escalation	Defense Ev					Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Toke Manipulation					Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padd					Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass Use Account Co					Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Comm History					Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signin		Discovery		Module Load	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Browser Extensions	Dylib Hijacking	DLL Search Order Hijacking	Hooking	Process Discovery	Remote Desktop Protocol	LSASS Driver	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting

.bash_profile and .bashrc

`~/.bash_profile` and `~/.bashrc` are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. `~/.bash_profile` is executed for login shells and `~/.bashrc` is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), `~/.bash_profile` is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, `~/.bashrc` is executed. This allows users more fine grained control over when they want certain commands executed.

.bash_profile and .bashrc

Technique

ID	T1156
Tactic	Persistence
Platform	Linux, macOS
Permissions Required	User, Administrator
Data Sources	File monitoring, Process Monitoring, Process command-line parameters, Process use of network

Mac's Terminal.app is a little different in that it runs a login shell by default each time a new terminal window is opened, thus calling `~/.bash_profile` each time instead of `~/.bashrc`.

These files are meant to be written to by the local user to configure their own environment; however, adversaries can also insert code into these files to gain persistence each time a user logs in or opens a new shell.

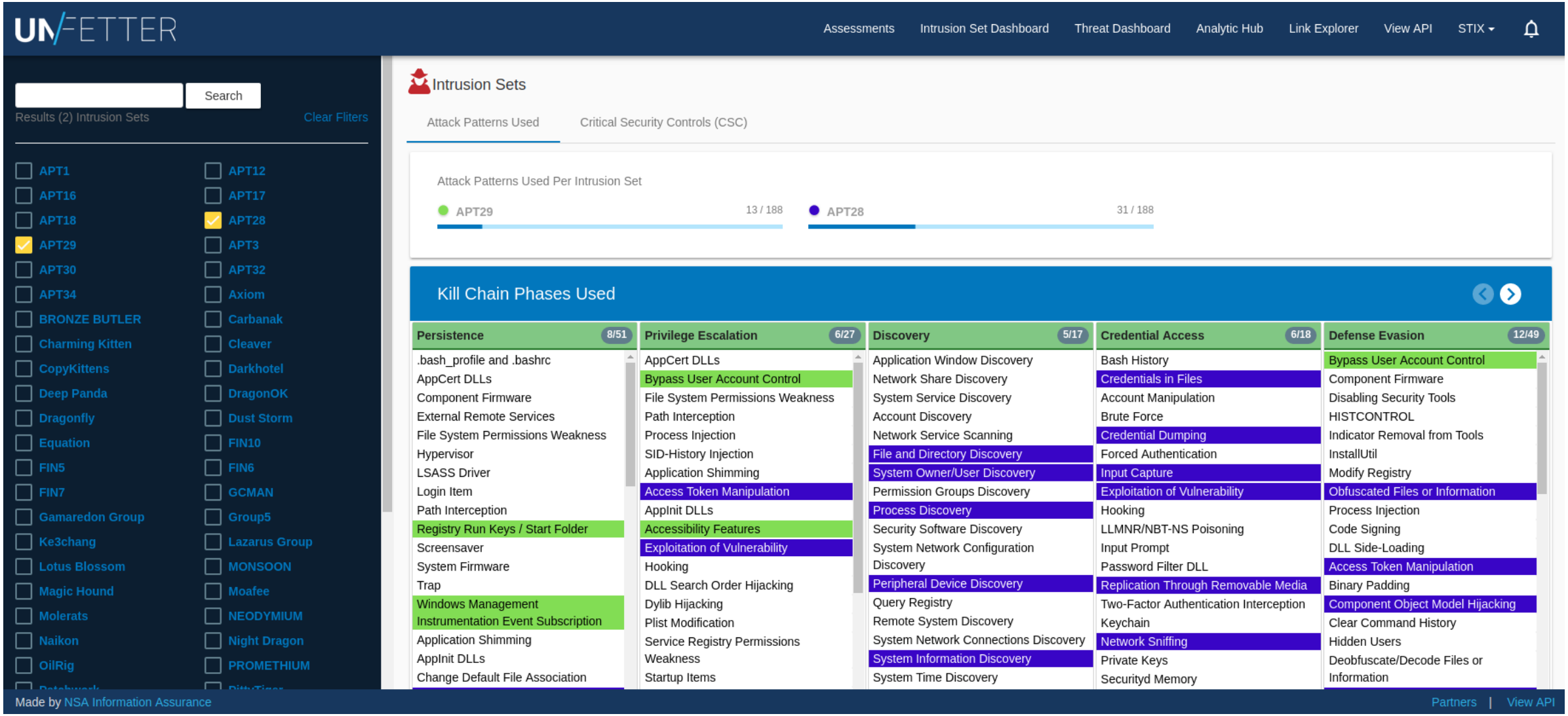
Mitigation

Making these files immutable and only changeable by certain administrators will limit the ability for adversaries to easily create user level persistence.

Detection

While users may customize their `~/.bashrc` and `~/.bash_profile` files , there are only certain types of commands that typically appear in these files. Monitor for abnormal commands such as execution of unknown programs, opening network sockets, or reaching out across the network when user profiles are loaded during the login process.

Unfetter – NSA tool that utilizes ATT&CK



OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Example activities for prior phases (ATT&CK focuses on post exploitation)

Attack Scenario: Web application user bypasses authorization or role-based privileges

Recon / Discovery

- Attacker spiders the application using an automated tool to map the application and catalog its content and functionality
- Attacker looks for pages that receive the path to a file as user input, and attempts to test various directory traversal and local file inclusion requests
- The attacker systematically tests access to application content and functionality that should not be permitted from the current role, particularly administrative pages or functions
- Etc.

Exploitation

- Attacker accesses a file through directory traversal / file inclusion manipulation
- Attacker accesses application functionality or data that is not meant to be accessible from their current role through a privilege misconfiguration or authorization flaw
- Attacker discovers and accesses higher-privilege functionality that is merely hidden from lower-privilege or unauthenticated users, rather than being enforced through access controls
- Etc.

Process to map and review threat activities

1. Document key activities by attack phase for attack scenario
2. Document all assets involved in attack scenario
3. Review and document existing detection capabilities for each activity
4. Identify and prioritize opportunities to improve detection

Develop Threat Detection Analytics
Monitor, Investigate & Respond

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Develop and documenting threat analytics

- Threat activity
- Analytic name
- Analytic description
- Key risk indicator
- Data sources
- Required data
- Analytics (platform specific)
- Threat detection guidance
- Notes
- Map to risk statements
- Author
- Date

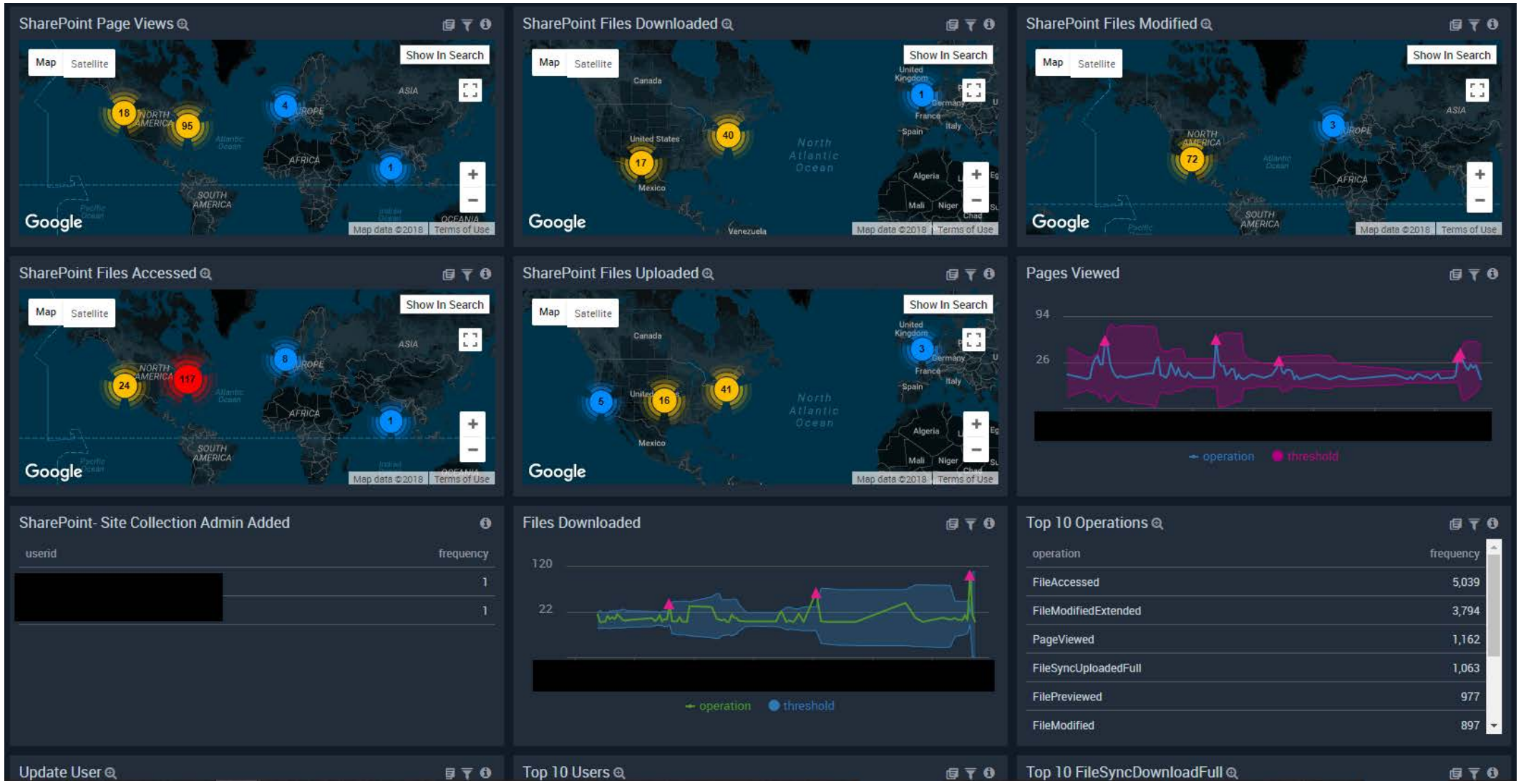
Example: threat activity = login with compromised credentials (exploit phase)

Threat Activity	Analytic Name	Analytic Description	Key Risk Indicator	Data Sources	Required Data
Azure AD login	Login from unusual location	GeoIP lookup for successful login from unusual location	Login outside of geographic area of business that does not correspond with authorized work travel	Azure Active Directory	1. Login success 2. Source IP 3. GeoIP 4. Authorized travel
Azure AD login	Concurrent logins from separate locations	GeoIP lookup for successful login concurrently from separate locations	Concurrent logins from geographically separate areas	Azure Active Directory	1. Login success 2. Source IP 3. GeoIP
Azure AD login	Logins from separate locations within unreasonable timeframe	GeoIP lookup for successful logins from separate locations where travel time is unreasonable between logins	Logins from separate locations within unreasonable travel time	Azure Active Directory	1. Login success 2. Source IP 3. GeoIP
Azure AD login	Login from anonymous IP address	Login IP correlated against threat intelligence for known anonymous proxy IP address	Login from an IP address that has been identified as an anonymous proxy IP address	Azure Active Directory Threat Intel	1. Login success (AD) 2. Source IP (AD) 3. Anonymous IPs (TI)
Azure AD login	Login from known malicious IP address	Login IP correlated against threat intelligence for known malicious IP address	Login from an IP address that has been identified as a known malicious IP address	Azure Active Directory Threat Intel	1. Login success (AD) 2. Source IP (AD) 3. Malicious IPs (TI)

Example: Threat Activity = Windows account discovery

Threat Activity	Analytic Name	Analytic Description	Key Risk Indicator	Data Sources	Required Data	Analytics	Threat Detection Guidance
Windows Users enumeration via net command or powershell	Unusual enumeration of users	Abnormal use of user discovery commands	Unusual behavior	Windows domain controllers	1. Event ID 4661	_index=WINDOWS _sourceCategory=CORP/*/WINDOWS event_id=4661 | parse "Security ID:\t*" as security_id | parse "Object Name:\t*" as object_name | parse "Object Type:\t*" as object_type | where object_type matches "SAM_USER" | where object_name matches "S-1-5-21domain-500" OR object_name matches "S-1-5-21domain-502" | where !(security_id = "System" OR security_id = "S-1-5-18")	ObjectType "SAM_USER" querying the following ObjectNames: "S-1-5-21domain-500" (Domain Local Administrator) "S-1-5-21domain-502" (KRBTGT) Exclude SubjectSecurityID "System" OR "S-1-5-18"
Windows Groups enumeration via net command or powershell	Unusual enumeration of groups	Abnormal use of group discovery commands	Unusual behavior	Windows domain controllers	1. Event ID 4661	_index=WINDOWS _sourceCategory=CORP/*/WINDOWS event_id=4661 | parse "Security ID:\t*" as security_id | parse "Object Name:\t*" as object_name | parse "Object Type:\t*" as object_type | where object_type matches "SAM_GROUP" | where object_name matches "S-1-5-21domain-512" OR object_name matches "S-1-5-21domain-516" OR object_name matches "S-1-5-21domain-519" | where !(security_id = "System" OR security_id = "S-1-5-18")	ObjectType "SAM_GROUP" querying the following ObjectNames: "S-1-5-21domain-512" (Domain Admins Group) "S-1-5-21domain-516" (Domain Controllers Group) "S-1-5-21domain-519" (Enterprise Admins Group) Exclude SubjectSecurityID "System" OR "S-1-5-18"

Real-time data visualization and alerting



OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Accelerate investigation and response

Example: Pass-the-hash attack with Mimikatz

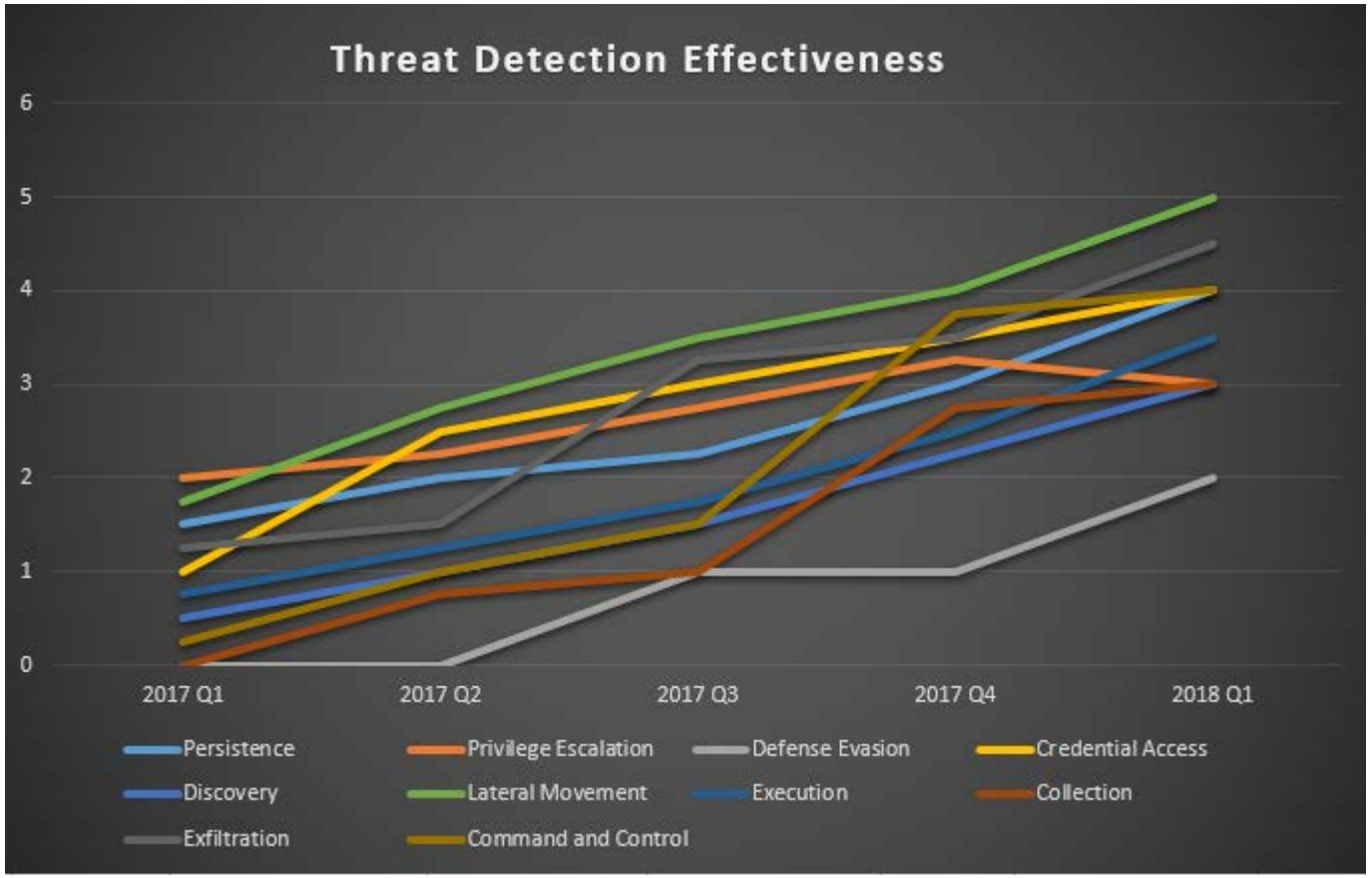
- Suppose we build behavioral detection analytics around specific Windows event logs
  - Event ID 4624 (New credentials based logon) with Logon Type 9
  - Event ID 4648 (A logon was attempted using explicit credentials)
  - Event ID 10 (Process Access) with Granted Access 0x1010 & 0x1038
  - Event ID 4768 (A Kerberos authentication ticket (TGT) was requested) with Ticket Encryption Type 0x17
- Upon detection, we can not only run additional analytics to investigate and validate threat activity, but also to gather relevant information for incident response
  - Determine every user that logged on since last boot
- Opportunities for automation to speed containment

Capture Metrics & Inform GRC

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.

Quantify threat detection capabilities



Report metrics to risk management

Risk Management

Priorities

KRIs
KPIs
Threat event frequency

Threat Detection

Conclusion

Benefits of risk-aligned threat detection

- Better focus on threat activity that matters most to the organization
- More context and clarity about detected threat events
- Opportunities to automate investigation and response activities
- Improved risk management program
- Reduced time to detect and contain incidents

Thank you

Brian Nolan

Chief Technology Officer, Advanced Threat CoE

TÜV Rheinland Group

bnolan@us.tuv.com

OPENSKY
A TÜV Rheinland Company

TÜVRheinland®
Precisely Right.