What's New from the SEI in Insider Risk

Matt Butkovic

Dan Costa

Carrie Gardner

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0853

Advanced Hunting Queries for Microsoft Threat Protection

Detect Exfiltration after Termination

This query can be used to explore any instances where a terminated individual (i.e. one who has an impending termination date but has not left the company) downloads a large number of files from a non-Domain network address.

Query

```
// Look for any activity for terminated employee creating a NetworkCommunicationEvents after they announced termination or re
let TermAccount = 'departing.employee'; //Enter the departing employee's username
let ReleaseTime = datetime('MM/DD/YYY 00:00:00'); //Enter the date the resignation or termination was announced
DeviceNetworkEvents
| where InitiatingProcessAccountName == TermAccount
| where Timestamp  > ReleaseTime
//| project Timestamp , DeviceName, InitiatingProcessAccountName
| sort by Timestamp  desc
| join
DeviceFileEvents on InitiatingProcessAccountName
| where FileName endswith ".docx" or FileName endswith ".pptx" or FileName endswith ".xlsx" or FileName endswith ".pdf"
| join DeviceNetworkInfo on DeviceId
| where ConnectedNetworks !contains '"Category":"Domain"'  //looking for remote, non-domain networks
| summarize TotalFiles=count() by bin(5Minutebin=Timestamp, 5m), InitiatingProcessAccountName
|where TotalFiles >1000 // adjust accordingly
| project TotalFiles,5Minutebin,InitiatingProcessAccountName
```

- Goal: identify coverage of Windows telemetry to common insider threat observables from the CERT Insider Incident Corpus
- Open-source contributions of detectors for the following threat scenarios:
  - Data exfiltration to competitor organization
  - Data exfiltration after termination
  - Data exfiltration using steganography tools
  - Anomalous use of service accounts

https://github.com/sei-nitc/Microsoft-threat-protection-Hunting-Queries

Insider Risk Management Program Building

- Survey of insider threat program practitioner perspectives on:
  - Challenges faced and barriers to successful insider threat programs
  - Best practices for addressing challenges and removing barriers

What Insider Threats are Practitioners Faced With?

THREAT TYPE	THREAT EVENT	INCIDENT COUNT IN LAST YEAR
HIGH CONCERN	**HIGH CONCERN**	**MALICIOUS**

• Thief
• Disgruntled insider
• Nation State
• Reckless insider
• Untrained/distracted insider
	• Financial fraud
	• Sabotage of capability
	• Information/data theft
	• Workplace violence
		• Over 5 incidents
		  • 69% respondents
		• Over 10 incidents
		  • 44% respondents
		• Over 100 incidents
		  • 11% respondents

MODERATE CONCERN	**MODERATE CONCERN**	**OTHER**

• Sympathizer to external influence
• Irrational individual
• Competitor
	• Misuse of resources
	• Workplace harassment
	• Insiders tricked by outsider
	• Other accidental leakage
	• Physical theft
		• Over 5 incidents
		  • 84% respondents
		• Over 10 incidents
		  • 58% respondents
		• Over 100 incidents
		  • 13% respondents

https://www.cylab.cmu.edu/_files/documents/summary-irm-survey-results-20210331.6.pdf

https://www.cylab.cmu.edu/_files/documents/irm-survey-results-20210331.7.pdf

Common Sense Guide to Managing Insider Risk

- Best practices for preventing, detecting, and responding to insider threats and managing insider risk
- What's New?
  - Insider Threat → Insider Risk
  - 22nd Best Practice: Learn From Past Insider Incidents
  - Updated standards crosswalk
  - Updated case studies and statistics from the CERT Insider Incident Repository
- Coming soon to the SEI Website!

SEI Training & Assessments Move to Live Online

- Training:
  - Insider Threat Program Manager: Implementation & Operation
  - Insider Threat Analyst
  - Insider Threat Vulnerability Assessor
  - Insider Threat Program Evaluator
- Assessments:
  - Insider Threat Vulnerability Assessment
  - Insider Threat Program Evaluation
  - Coming Soon: Insider Risk Management Program Evaluation

More information and training dates: https://www.sei.cmu.edu/education-outreach/courses/

What's Next?

- White papers and technical reports on data for insider threat research and development, architecture for insider threat detection, and insider risk control efficacy
- Research projects focused on producing experimentally-derived knowledge of the most effective combinations of AI/ML approaches, data sets, and risk indicators
- Further exploration of scalable measures for organizational factors of insider risk

Stay up to date with us at https://www.sei.cmu.edu/our-work/insider-threat/index.cfm