PROTECTING YOUR ENTERPRISE FROM CORPORATE ESPIONAGE: KEEPING INSIDER THREATS OUTSIDE

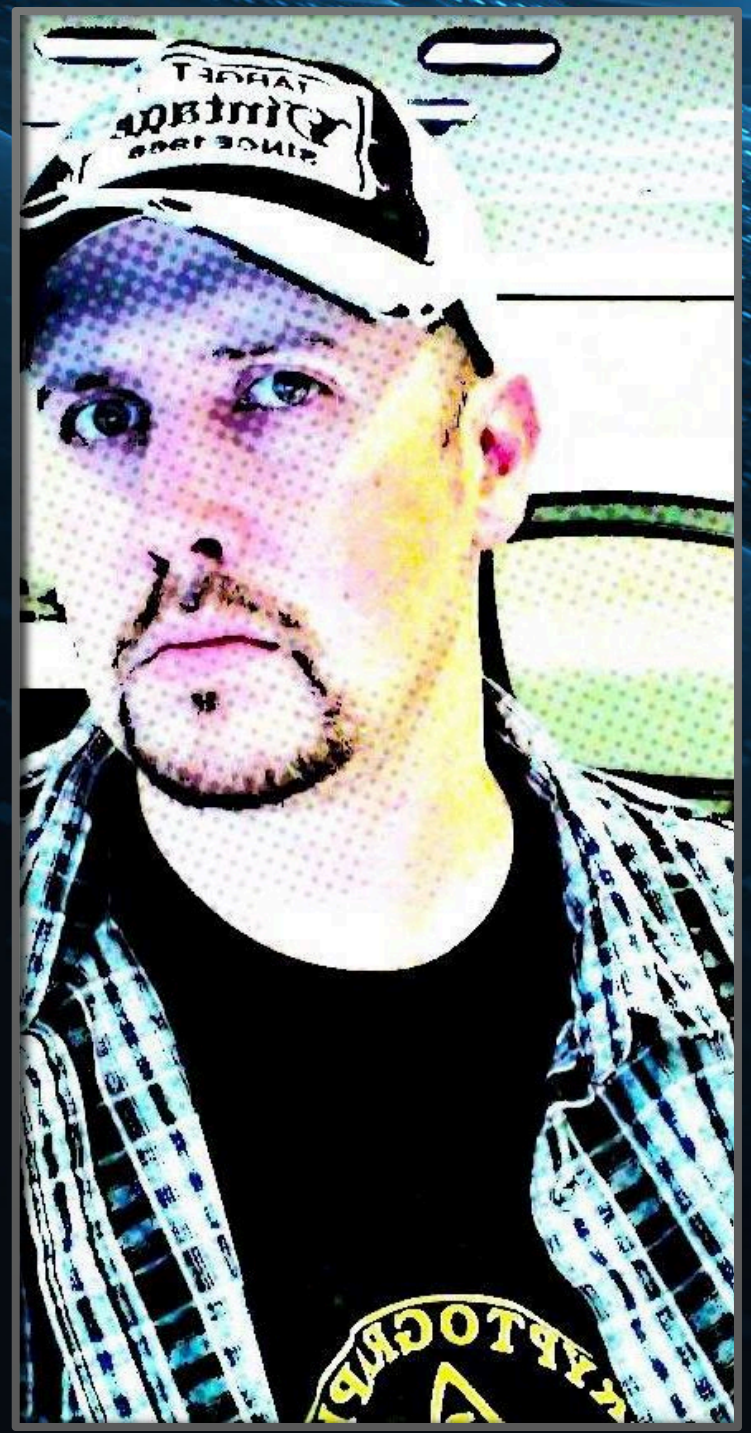
June 2018


3:05

CYBERARK

```
09-18 * * * /home/dbadmin/check-db-status
#5 1 * * 6 /home/backupadmin/full_backup
#0 1 * * * /home/backupadmin/incremental_backup
23 2 5 5 * /opt/bin/prod/SCREW_YOU_GREG.sh > /dev/null
* * 4 20 /sbin/ping -c 1 192.168.0.1 > /dev/null
0 8 * * 1 /home/reports/weeklyreporting.sh
00 09-18 * * * /home/ramesh/bin/check-db-status
```

CYBERARK

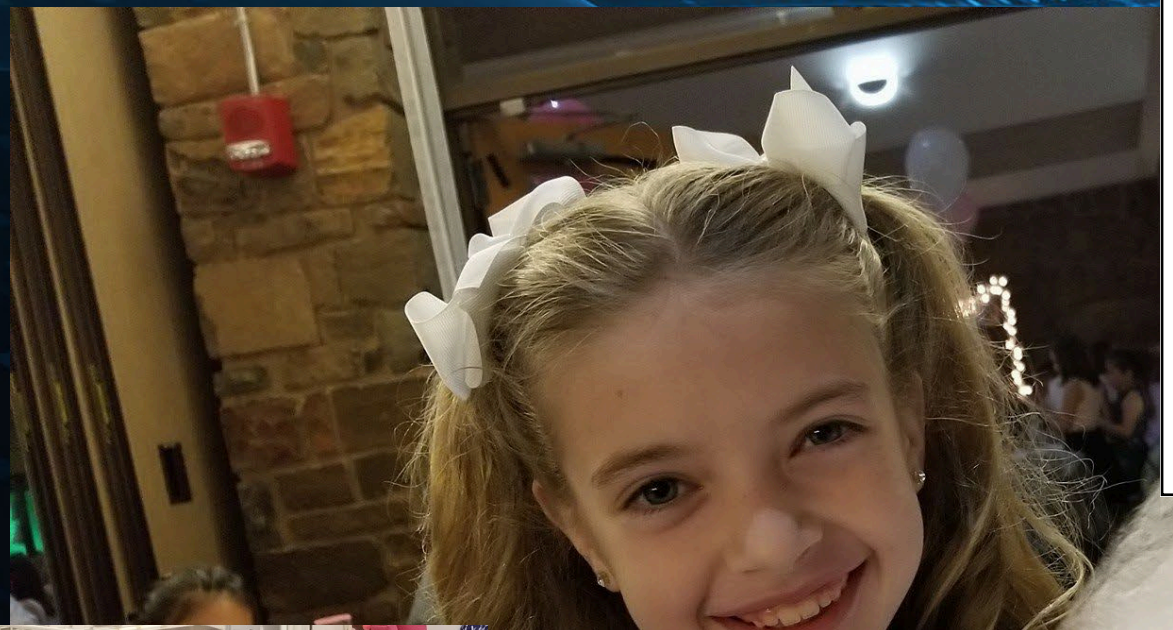


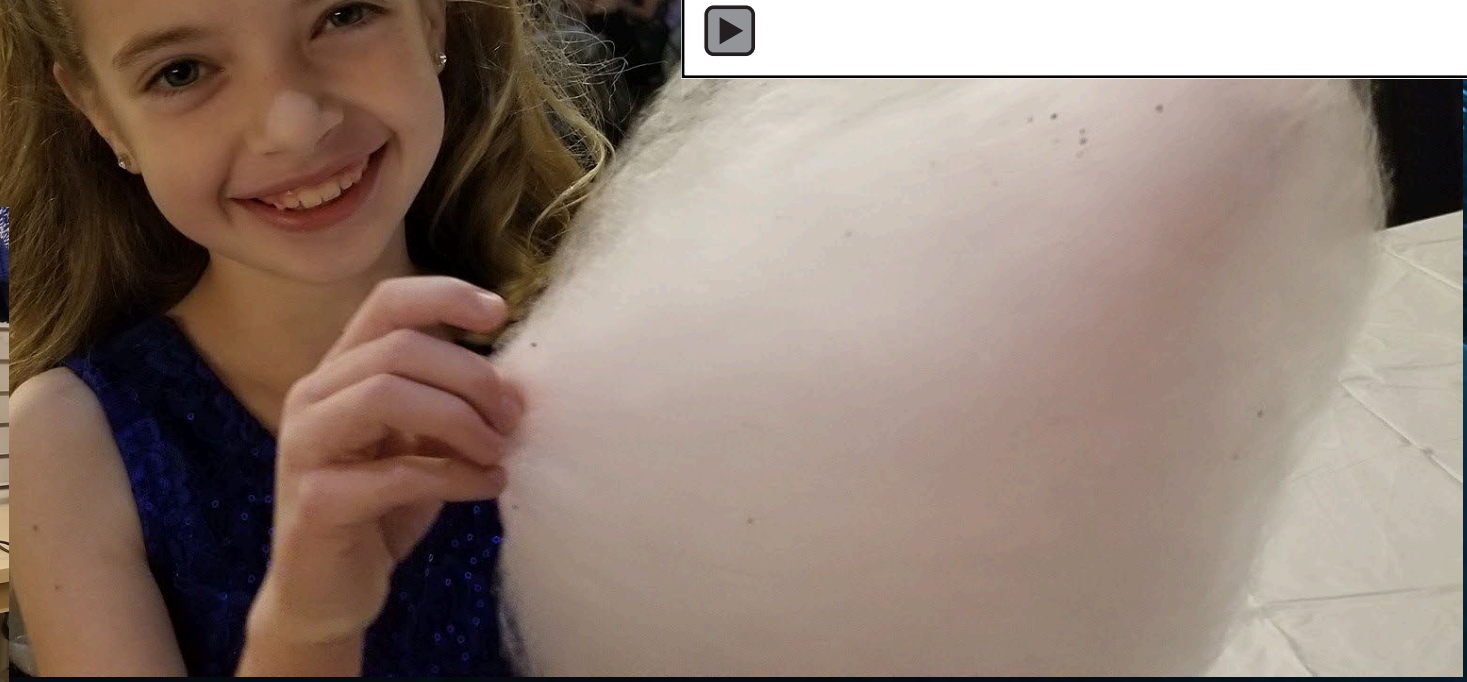
Andy Thompson

- National Manager Customer Success CyberArk Software
- B.S. MIS – University of Texas at Arlington
- COMPTIA A+ & Sec+
- (ISC)2 SSCP & CISSP
- GIAC – Certified Penetration Tester (GPEN)
- SANS Advisory Board Member & Mentor
- Member of Shadow Systems Hacker Collective
- Member of Dallas Hackers Association
- Scared of Earthquakes and Snow-Skiing

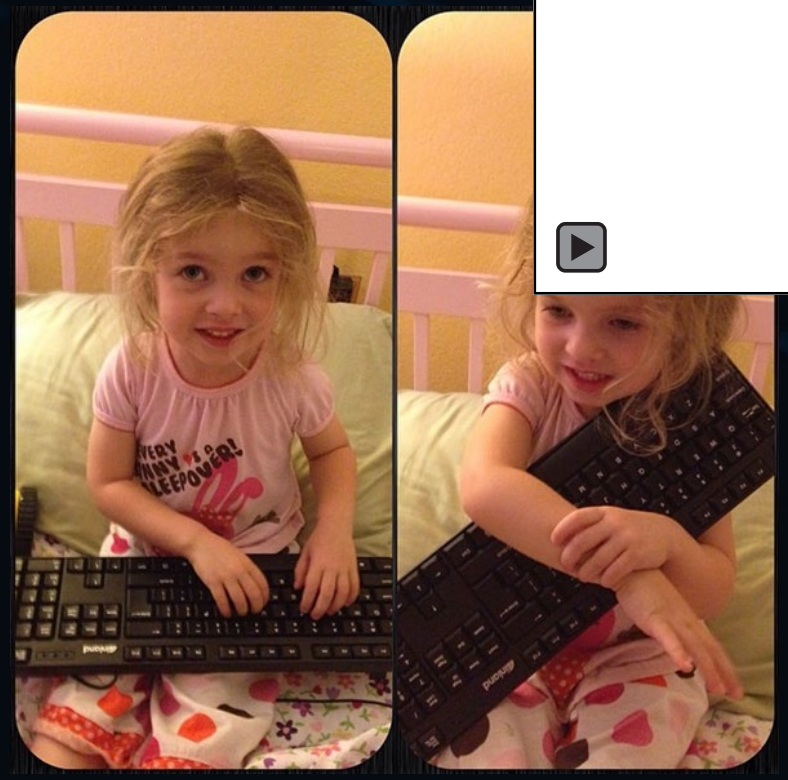
THE REAL TRAVEL HACKER

CYBERARK





CYBERARK



CYBERARK

AGENDA

- Historical cases.
- Profile of a malicious insider & attack flow.
- Defense strategy
  - Malicious Insider Kill-Chain
  - Technical Controls
- Insider Threat Pro-Tips


CYBERARK
CORPORATE ESPIONAGE & INSIDER THREATS
CASE STUDY

IBM VS HITACHI

- 1983
- Stolen Proprietary Data
  - FOR INTERNAL IBM USE ONLY
- Settled Out of court $300 Million.

HITACHI IBM

CADENCE DESIGN VS AVANT!

- Stolen Source Code
- Criminal case filed.
  - Restitution of $200 million.
- Civil Case filed.
  - $265 million in restitution.

cadence

THE INSIDER THREAT

Georgia-Pacific

- Brian Johnson, former Systems Administrator
- Fired. And then…
  - Logged in via VPN from home.
  - Caused over $1 mil in damages to Industrial control systems.
- Sentenced to 3 years in jail.
- Ordered to repay $1,134,818 in damages.

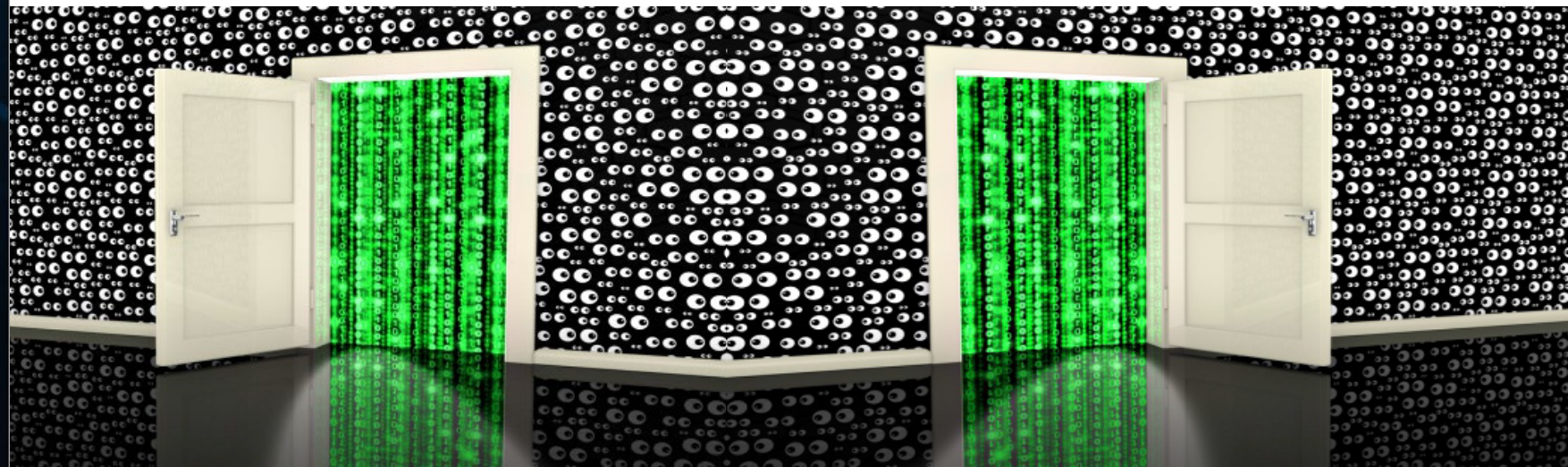
THE INSIDER THREAT

Columbia Sportswear Company™

DENALI
ADVANCED INTEGRATION

CYBERARK

- Michael Leeper, Senior Director of Technology Infrastructure
- 2 Backdoors
  - Accessed over 700 times over 2 years
  - Repeatedly accessed the emails of Columbia Sportswear senior executives
  - Stole relevant data to Denali.
- 3 Years probation + 400 hours community service.

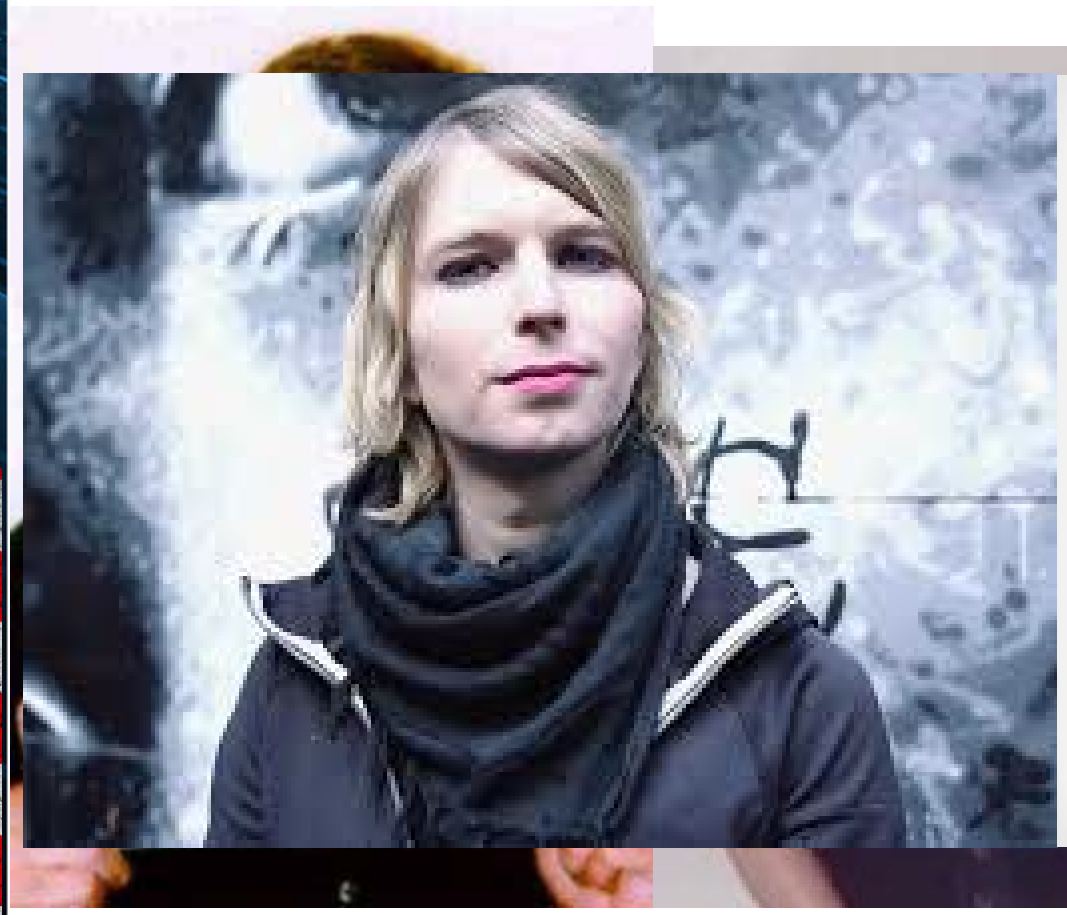


GOOGLE VS UBER

- Jan 2016 - Anthony Levandowski abruptly leaves Waymo (Google) and starts Otto.
- Otto almost immediately acquired by Uber for $700 mil.
- Lawsuit claims Levandowski stole confidential trade secrets from Google.
- Feb 9th, 2018 – Waymo receives at least .34 percent stake in Uber **(~$245 million)**
  - Uber will not use any of Google's intellectual property in its own self-driving efforts.

ESPIONAGE & MALICIOUS INSIDERS

THE FED.

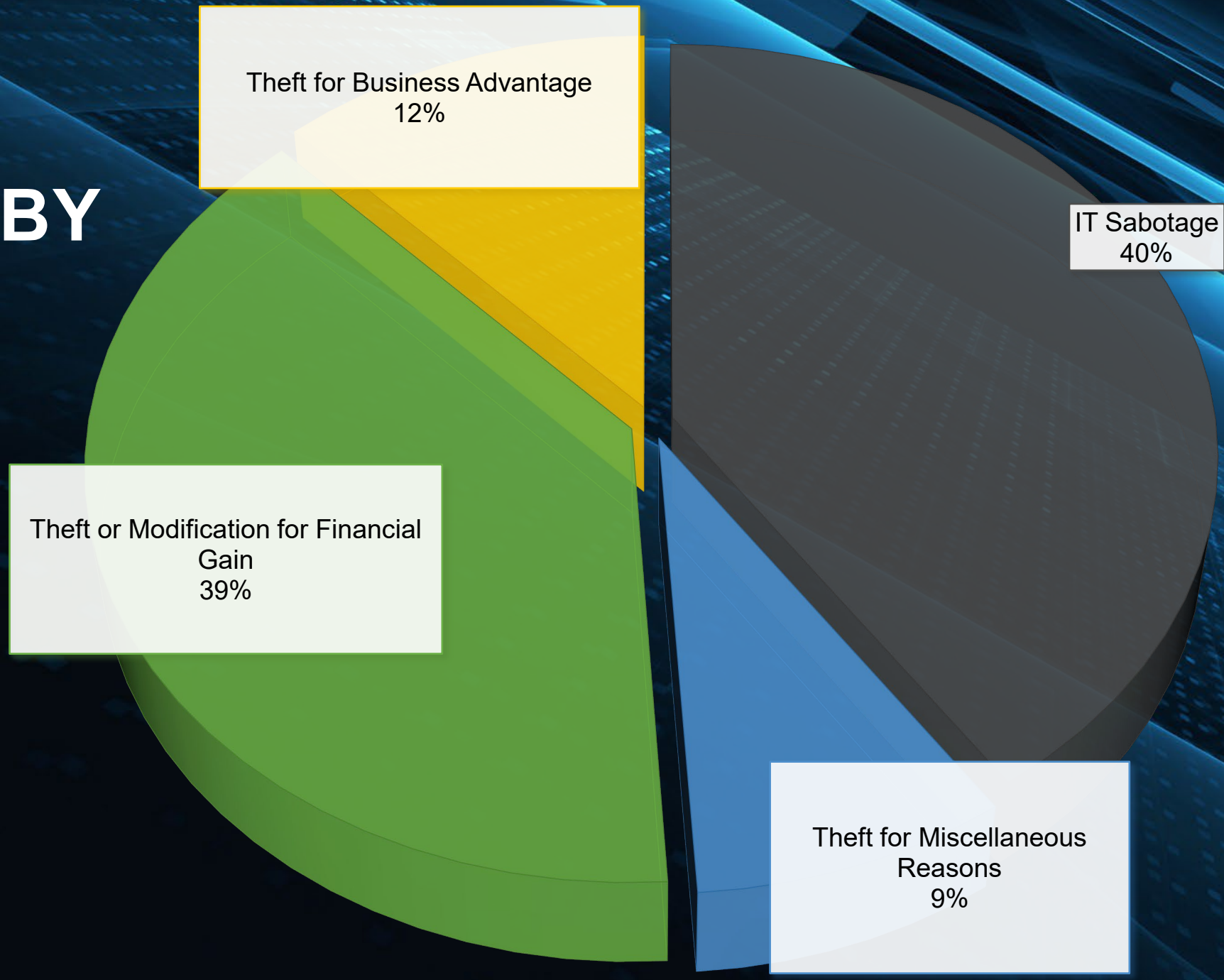


FOUR TYPES OF DAMAGE

- IT Sabotage
- Theft or modification for financial gain
- Theft of modification for business advantage
- Miscellaneous

CYBERARK

BREAKDOWN BY CATEGORY

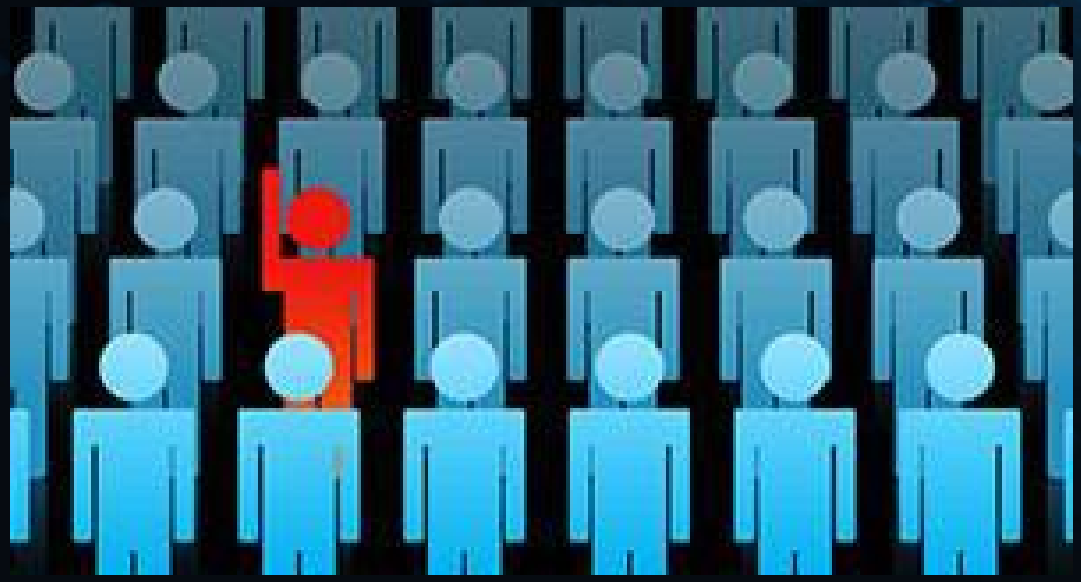


INTERESTING STATS ON SYSADMIN MOTIVATION

- Only **1.5%** of espionage cases use sysadmin privileges for financial gain or business advantage.
- **90%** of IT sabotage cases use sysadmin privileges.

CYBERARK

THE MALICIOUS INSIDER



CYBERARK

US CERT - DEFINITION OF "MALICIOUS INSIDER"

- A current or former employee, contractor, or business partner who:
  - Has or had authorized access to an organization's network, system, or data and
  - Intentionally exceeded or misused that access in a manner that negatively affected the confidentially, integrity, or availability of the organization's information or information systems.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

CYBERARK

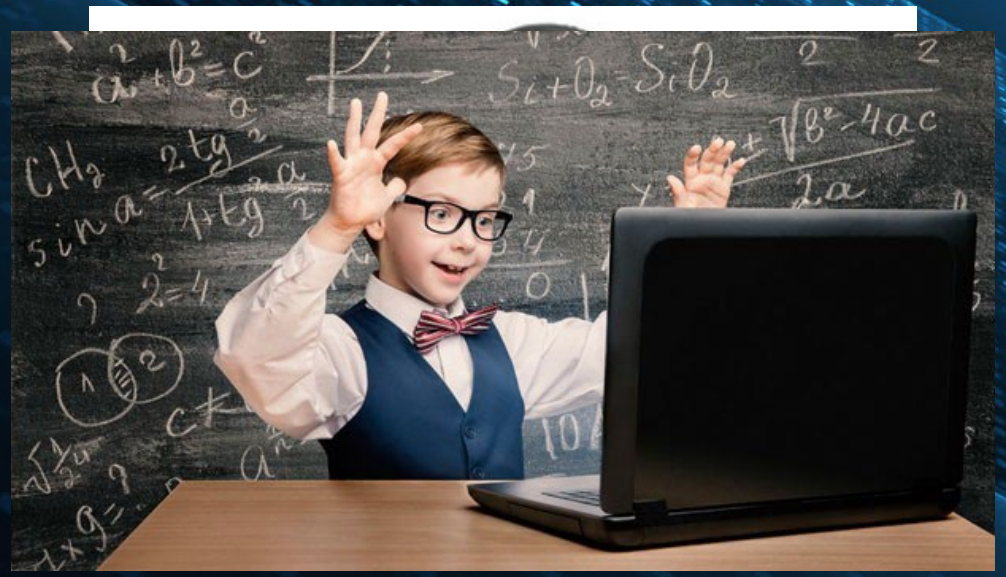
36% of surveyed companies have experienced **security incidents** involving malicious employees in the past **12 months**.

-Imperva 2016

CYBERARK

4 TYPES OF MALICIOUS INSIDER

- Compromised actors
- Negligent actors
- Malicious insiders
- Tech savvy actors

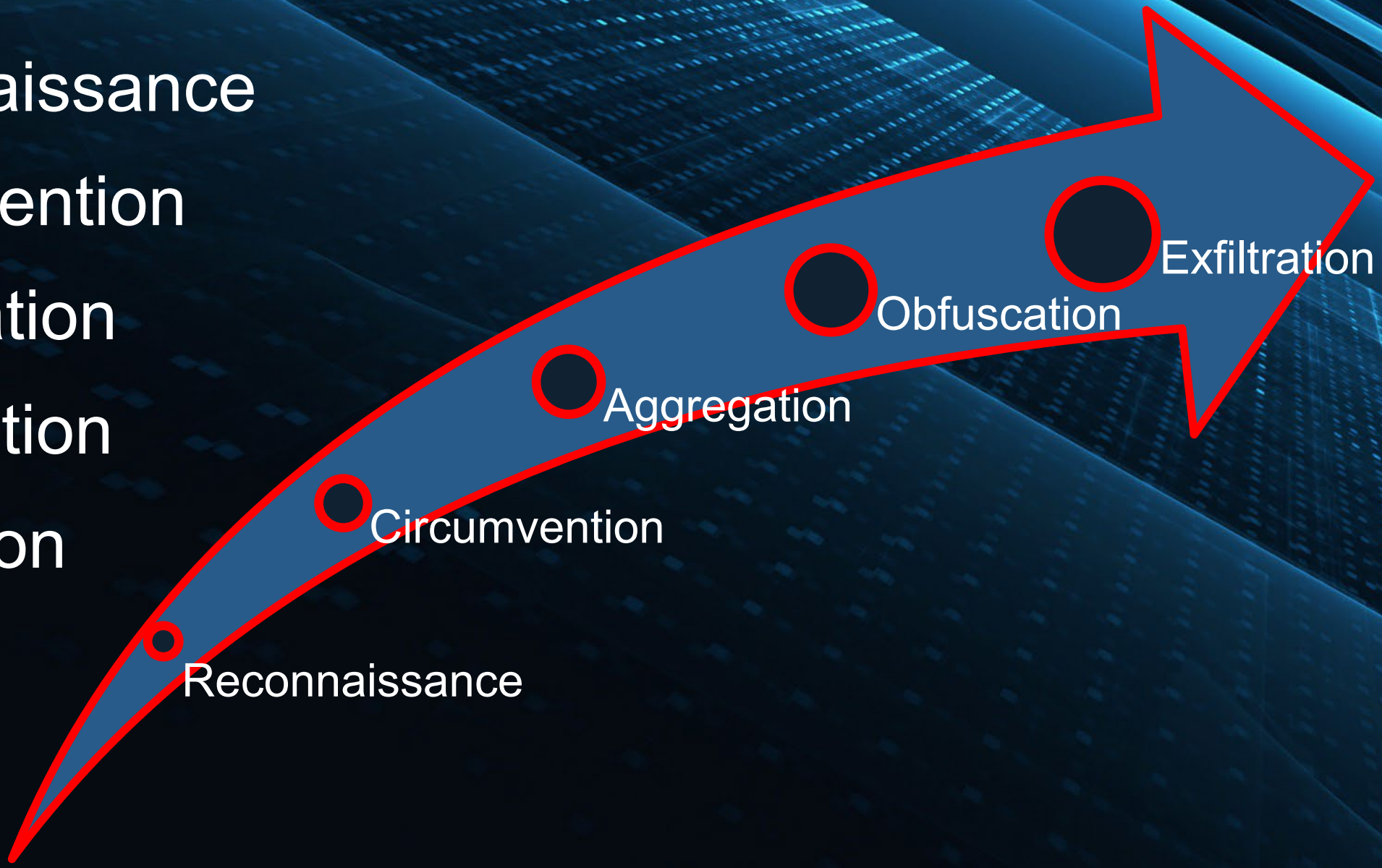


PROFILE OF A MALICIOUS INSIDER

- Inability to assume responsibility for their actions
- Intolerance of criticism
- Self-perceived value exceeds performance
- Lack of empathy
- Predisposition towards law enforcement
- Pattern of frustration and disappointment
- History of managing crises ineffectively.
- Introversion
- Greed/financial need
- Vulnerability to blackmail
- Compulsive and destructive behavior
- Rebellious, passive aggressive
- Ethical “flexibility”
- Reduced loyalty
- Entitlement – narcissism (ego/self-image)
- Minimizing their mistakes or faults

DATA LOSS – “THE PATH OF PAIN”

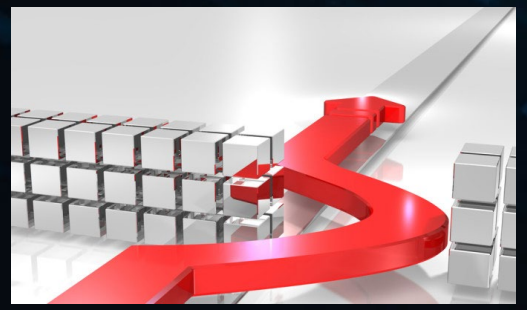
1. Reconnaissance
2. Circumvention
3. Aggregation
4. Obfuscation
5. Exfiltration



STEP ONE: RECONNAISSANCE BEHAVIOR

- Accessing a new or unusual location in a document repository.
- An unusual increase in error or access denied messages.
- Failed attempts to mount USB devices and access external websites.
- Unusually rapid rate of opening files in a short period of time.
- Network scanning and use of network tools.
- Running applications that they've never run before — especially hacking applications.

STEP TWO: CIRCUMVENTION BEHAVIOR

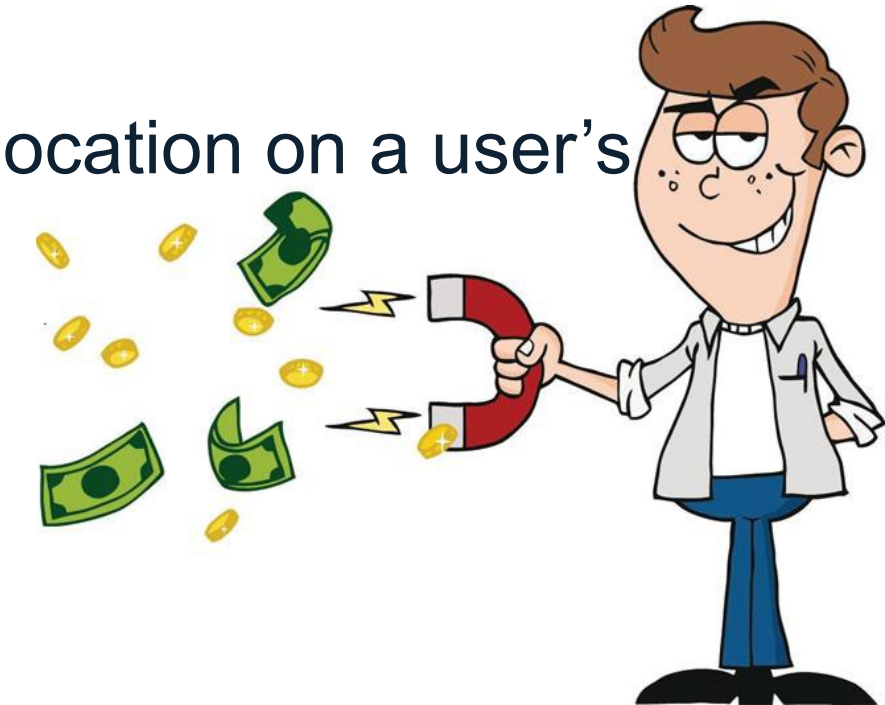


- Use of tools like TOR, VPNs and proxy servers to engage in untraceable internet activity.
- File transfers through instant messaging, to evade DLP restrictions.
- Sharing information online, whether it be through copy/paste sites like PasteBin, communities like Reddit, or social networks like Facebook or LinkedIn.
- Disabling or bypassing security software, or researching how to do so.

PASTEBIN

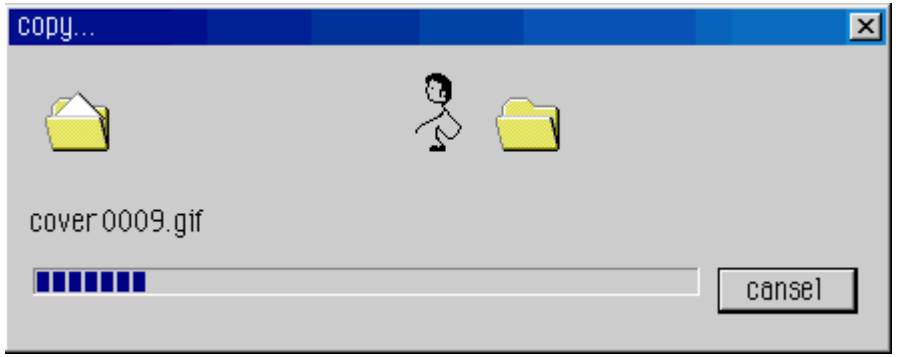
STEP THREE: AGGREGATION BEHAVIOR

- Unusual amounts of file copies, movements, and deletions.
- Unusual amounts of file activity in high-risk locations and sensitive file types.
- Unusual creation of files that are all exactly the same size.
- Saving files to an usual location on a user's endpoint.



STEP FOUR: OBFUSCATION BEHAVIOR

- Unusual rates of file renaming, especially to a different file type.
- Unusual rates and sizes of file compression.
- Clearing cookies and event viewer logs, or unusual use of browser “stealth” settings like Chrome’s Incognito mode.
- Hiding sensitive information in image, video, or other misleading file types.



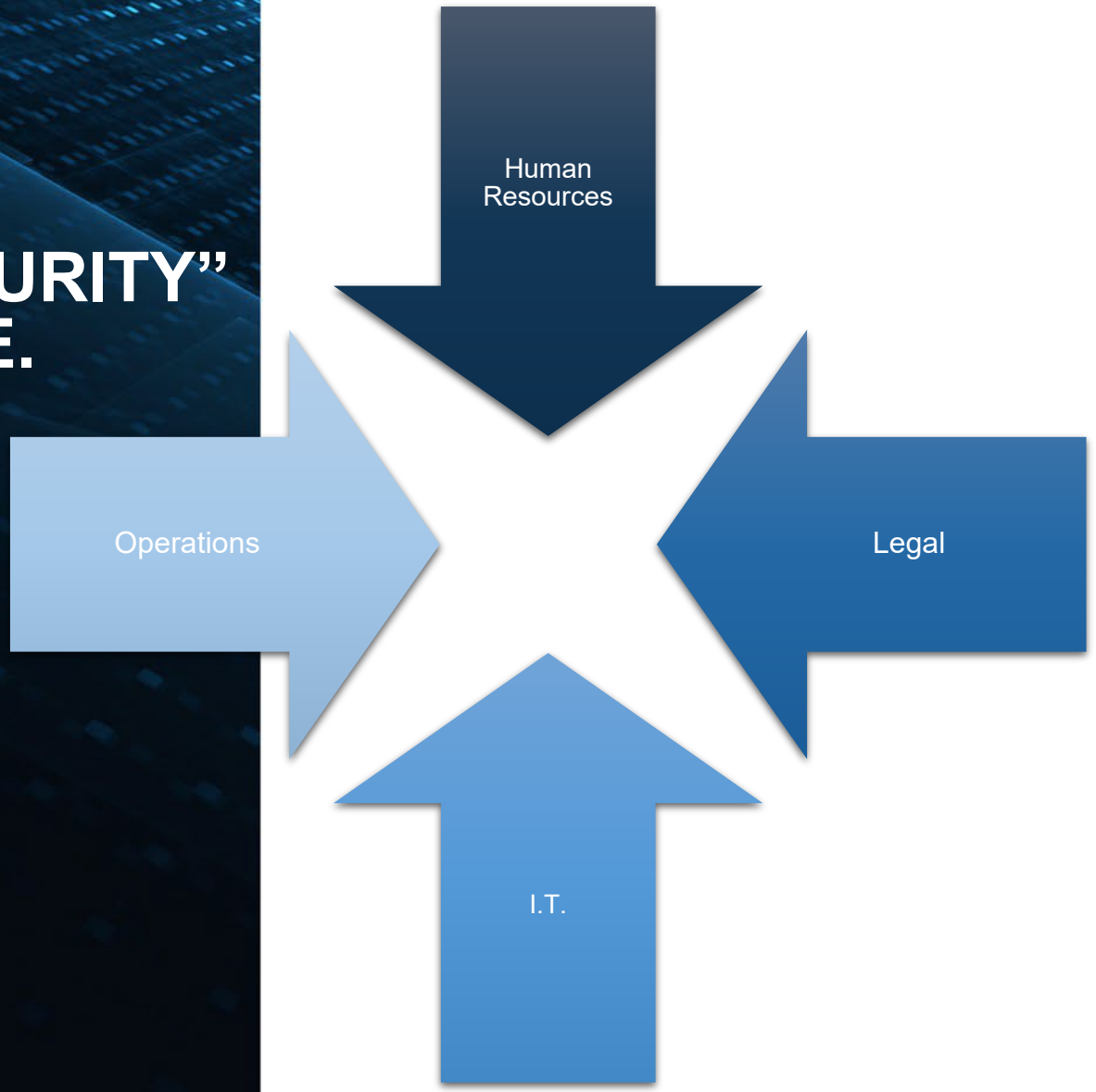
CYBERARK

STEP FIVE: EXFILTRATION

CYBERARK

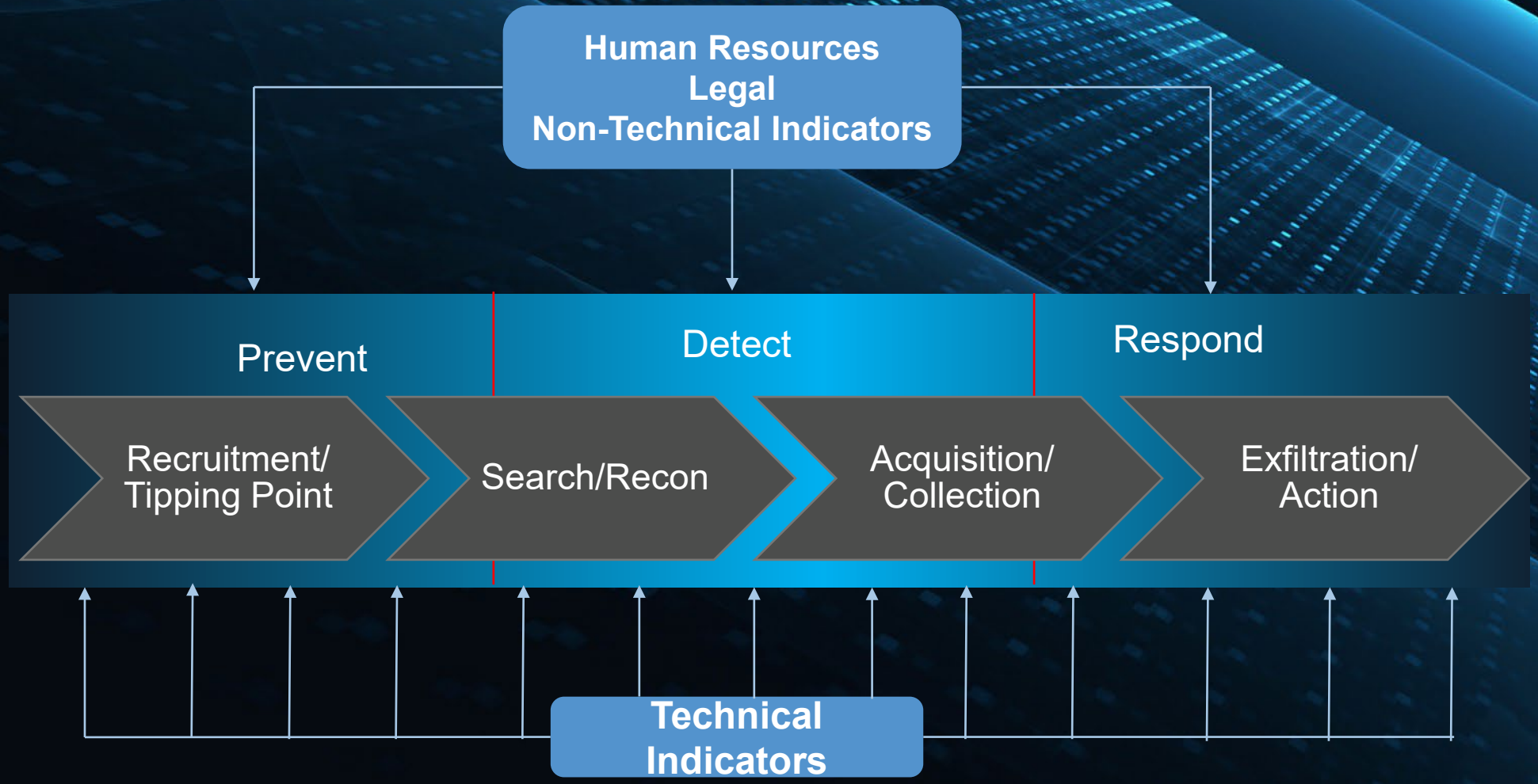
HOW TO DEFEND

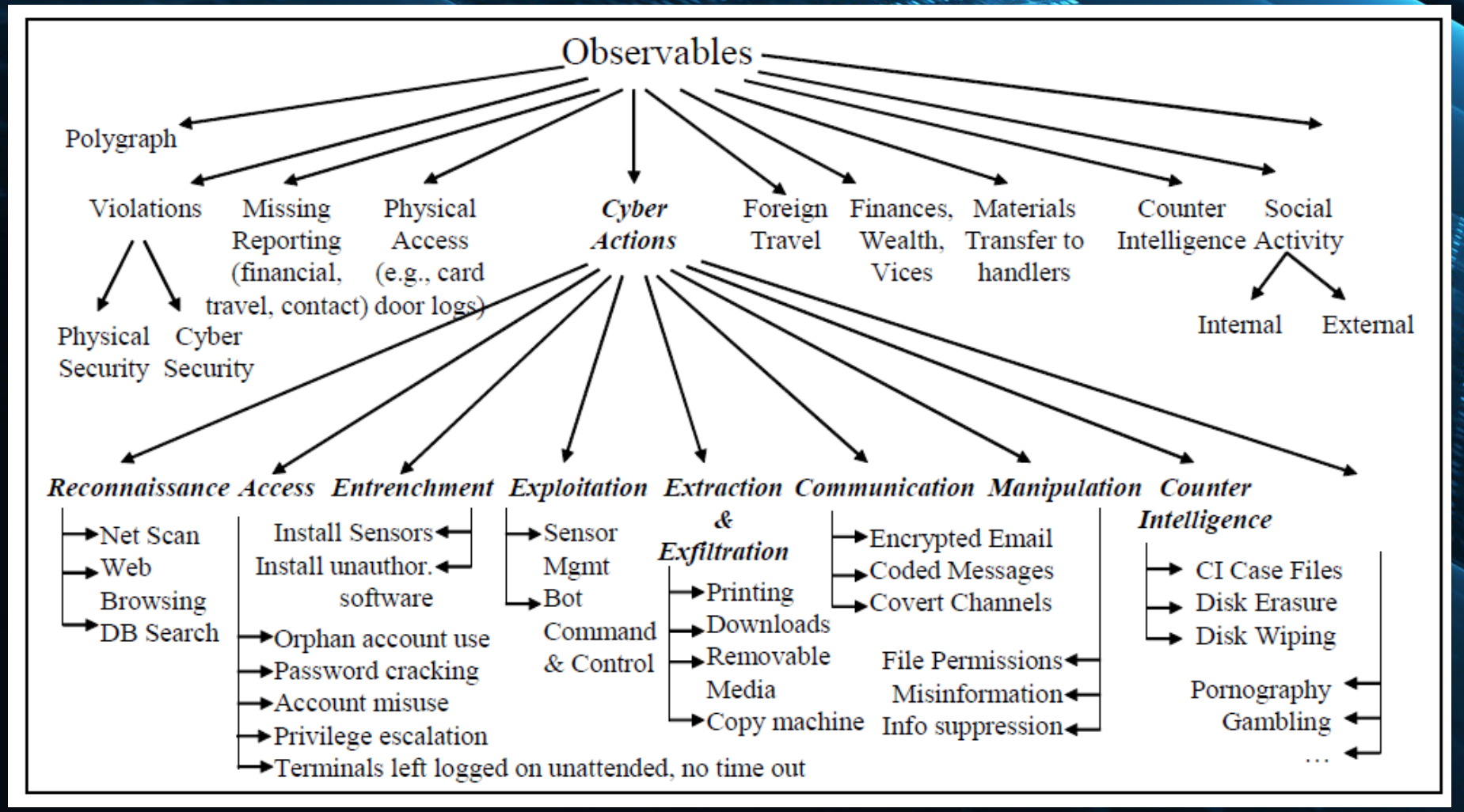
NOT A "CYBER SECURITY" ISSUE ALONE.



- Policies & Procedures
- Regular scheduled training
- Prevent at hiring process
- HR anticipating negative workplace issues
- Focus on deterrence not just detection.
  - Can't detect outliers if P&P's don't exist.

CYBERARK


Human Resources
Legal
Non-Technical Indicators
Prevent
Detect
Respond
Recruitment/
Tipping Point
Search/Recon
Acquisition/
Collection
Exfiltration/
Action
Technical
Indicators



OBSERVABLE VS CYBER ACTIONS


CYBERARK
TECHNICAL CONTROLS

TECHNICAL CONTROLS

- DLP solutions.
- Deactivate computer access following termination.
- Separation of duties.
- Least Privilege.
  - Application control.
- Encryption.

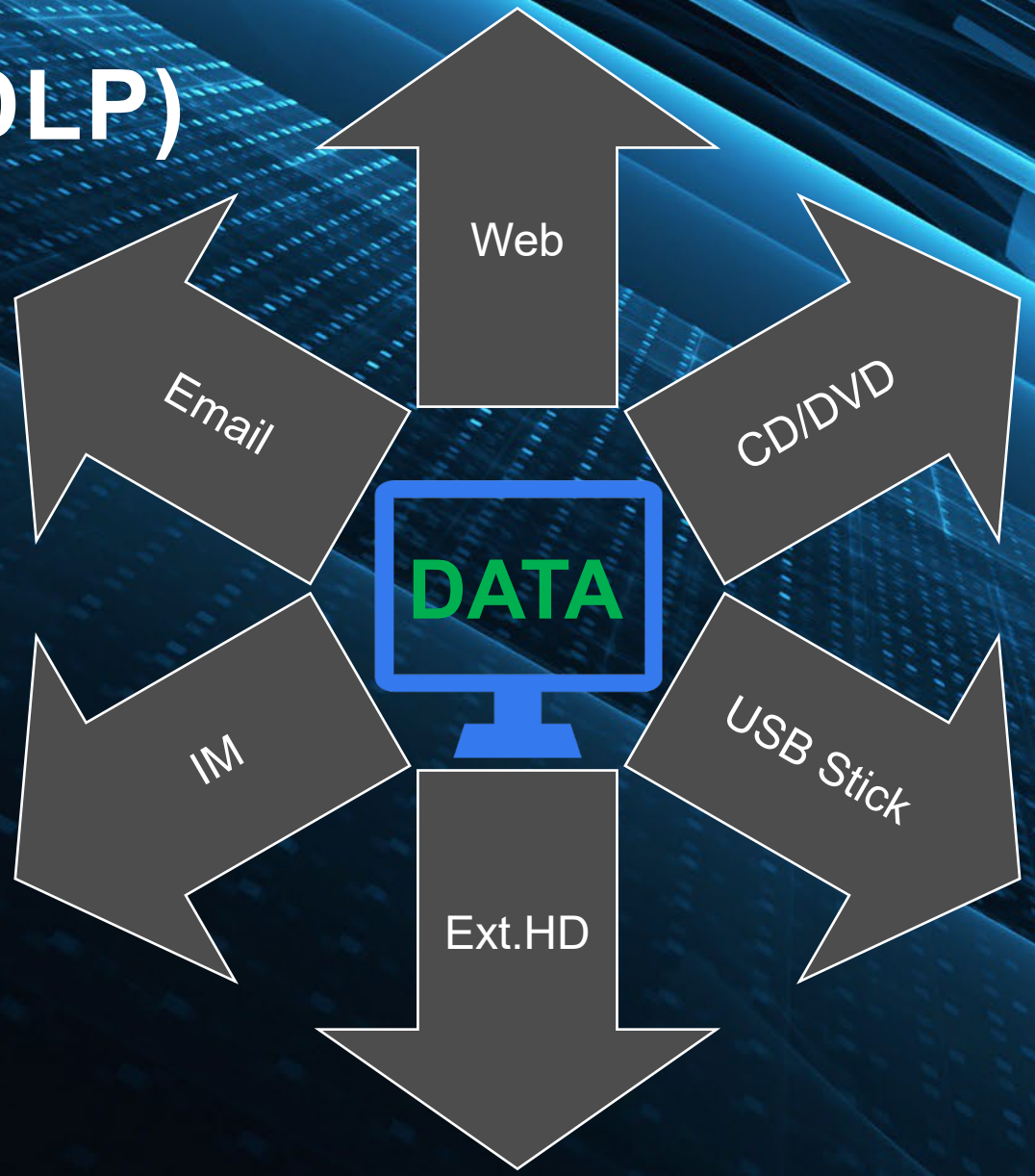
TECHNICAL CONTROLS (CONTINUED)

- Consider Threats from SLDC.
  - Visibility into Change Control.
- **Secure** backup/recovery.
- Strong Password Management.
- Logging & auditing of privileged actions.
- SIEM – behavioral analytics.

CYBERARK

DATA LOSS PREVENTION (DLP)

- Excellent for preventing data exfiltration.
  - Hard to implement successfully.
  - ProTip: Identify and classify data before deploying DLP
- DLP is not an access control system and not be seen as a replacement to one.
- Systems still vulnerable to sabotage



CYBERARK

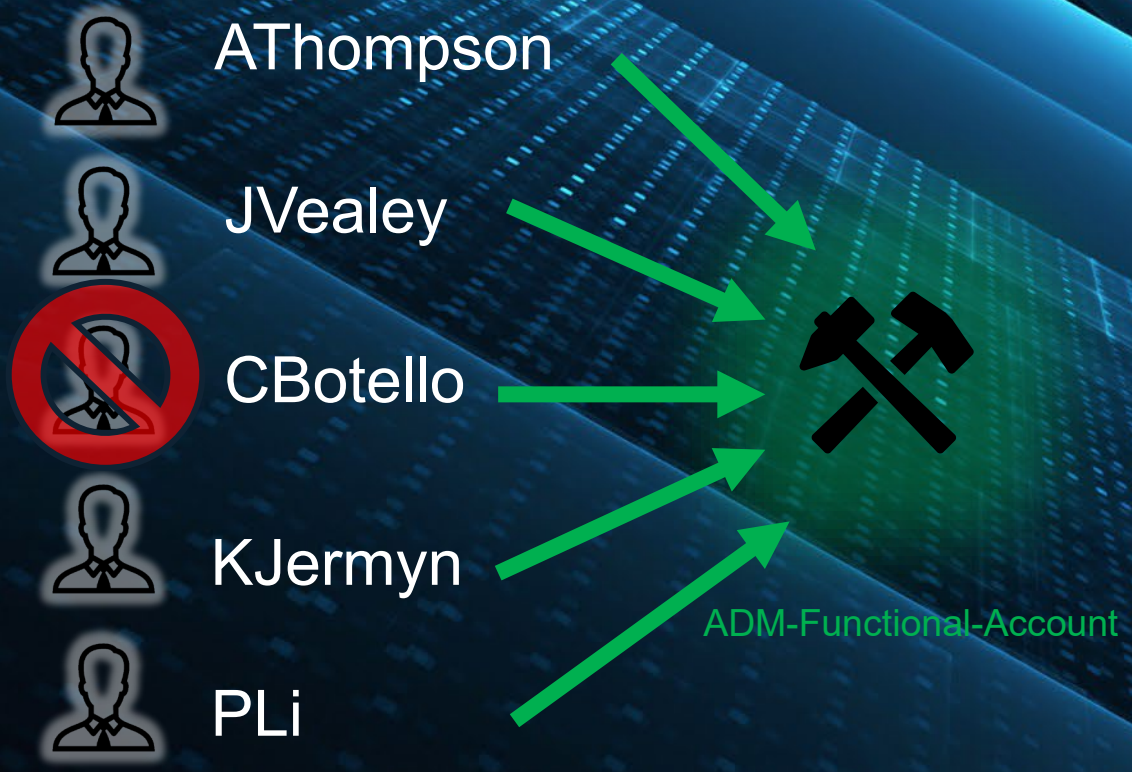
DEACTIVATE ACCESS

- Remove privileged access as soon as notice is tendered.
- D/C immediately upon termination.
  - No Exceptions!
- Use Functional Account Model.

CYBERARK

FUNCTIONAL ACCOUNT MODEL

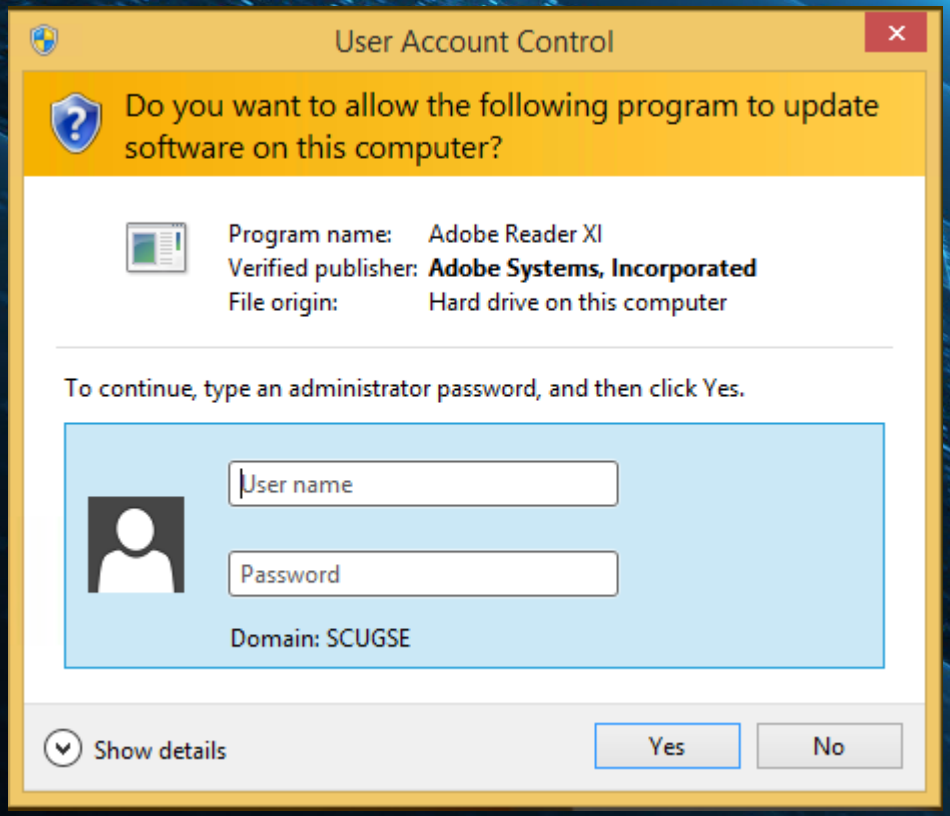
5 Privileged Accounts



1 Privileged Account

LEAST PRIVILEGE & APPLICATION CONTROL

- Prevents users from exceeding boundaries.
  - Malicious
  - Accidental
- Prevents malicious software installation.
- Prevents malicious activities.



CYBERARK

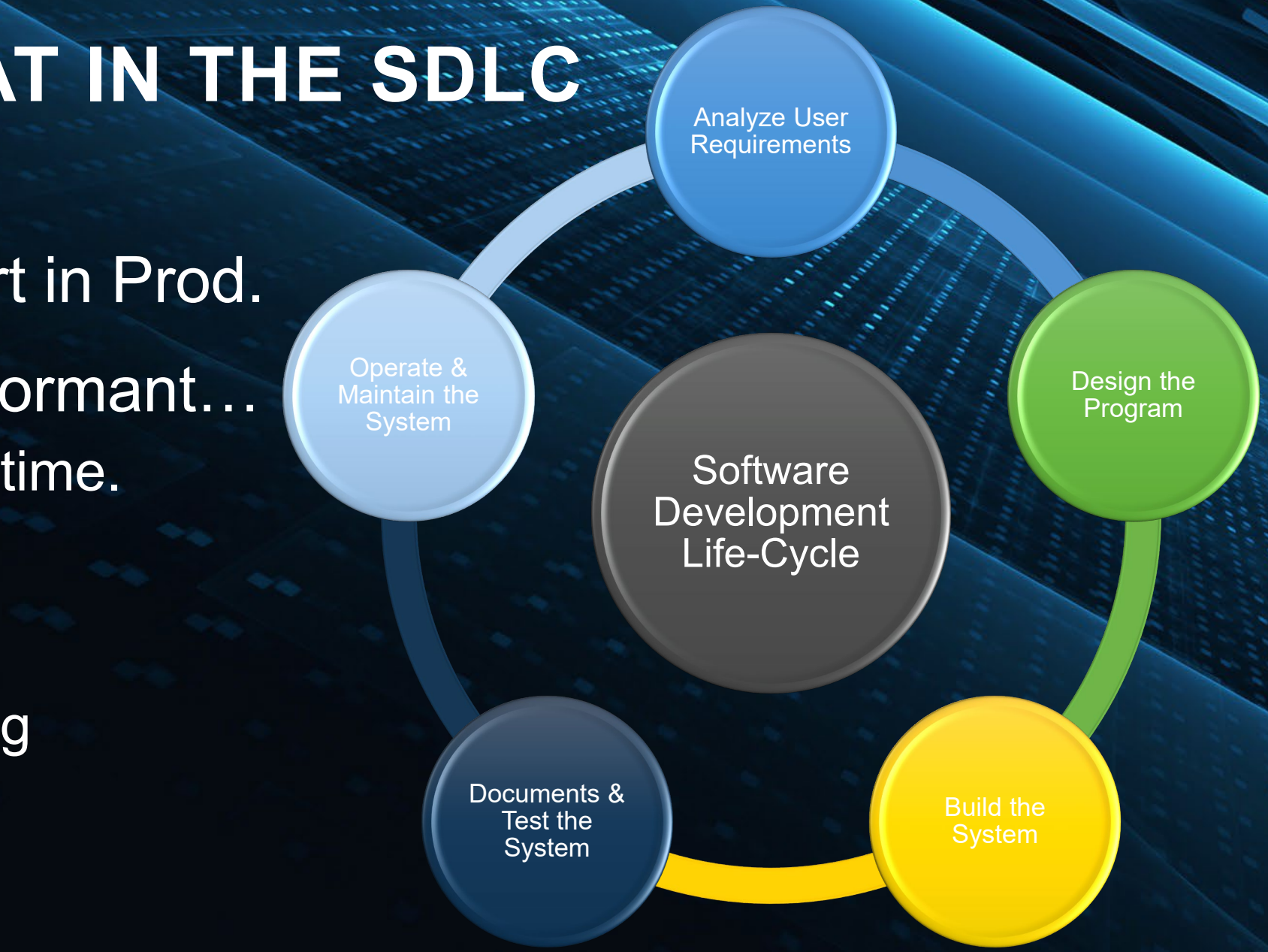
ENCRYPTION

- Good in a defense in depth strategy.
  - Not so much with espionage & malicious insiders
- Authorized users bypass the control…by design.
- Malicious insiders can siphon off to non-encrypted media.
- Story Time with Phineas Fisher…

CYBERARK

INSIDER THREAT IN THE SDLC

- Not all attacks start in Prod.
- Logic bombs lay dormant…
  - Until the “perfect” time.
- Solutions:
  - Code review
  - Integrity monitoring
  - Change control

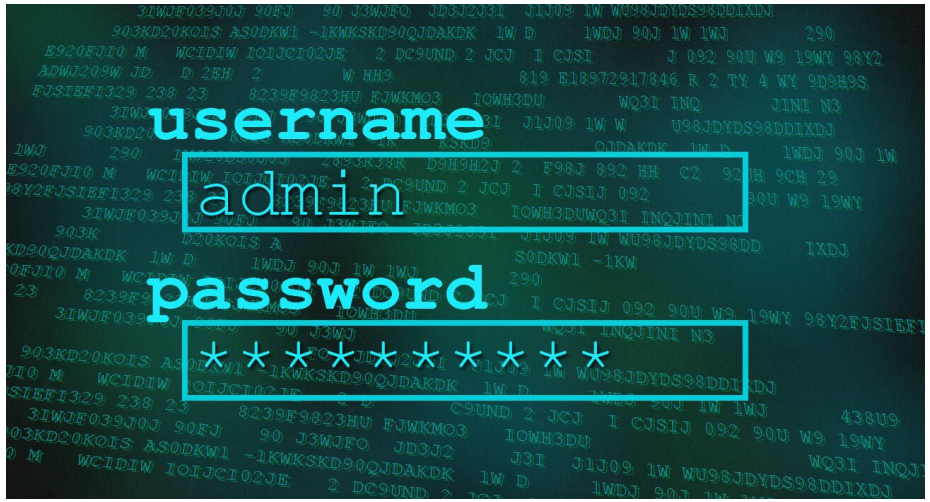


CYBERARK

SECURE BACKUP & RECOVERY

- Backups are sensitive to attack.
- Offsite & disconnected
- Availability is a target.
- Solution:
  - DR Tests
  - Integrity checks
    - Full backups
    - And Incrementals too!

PRIVILEGED ACCESS MANAGEMENT

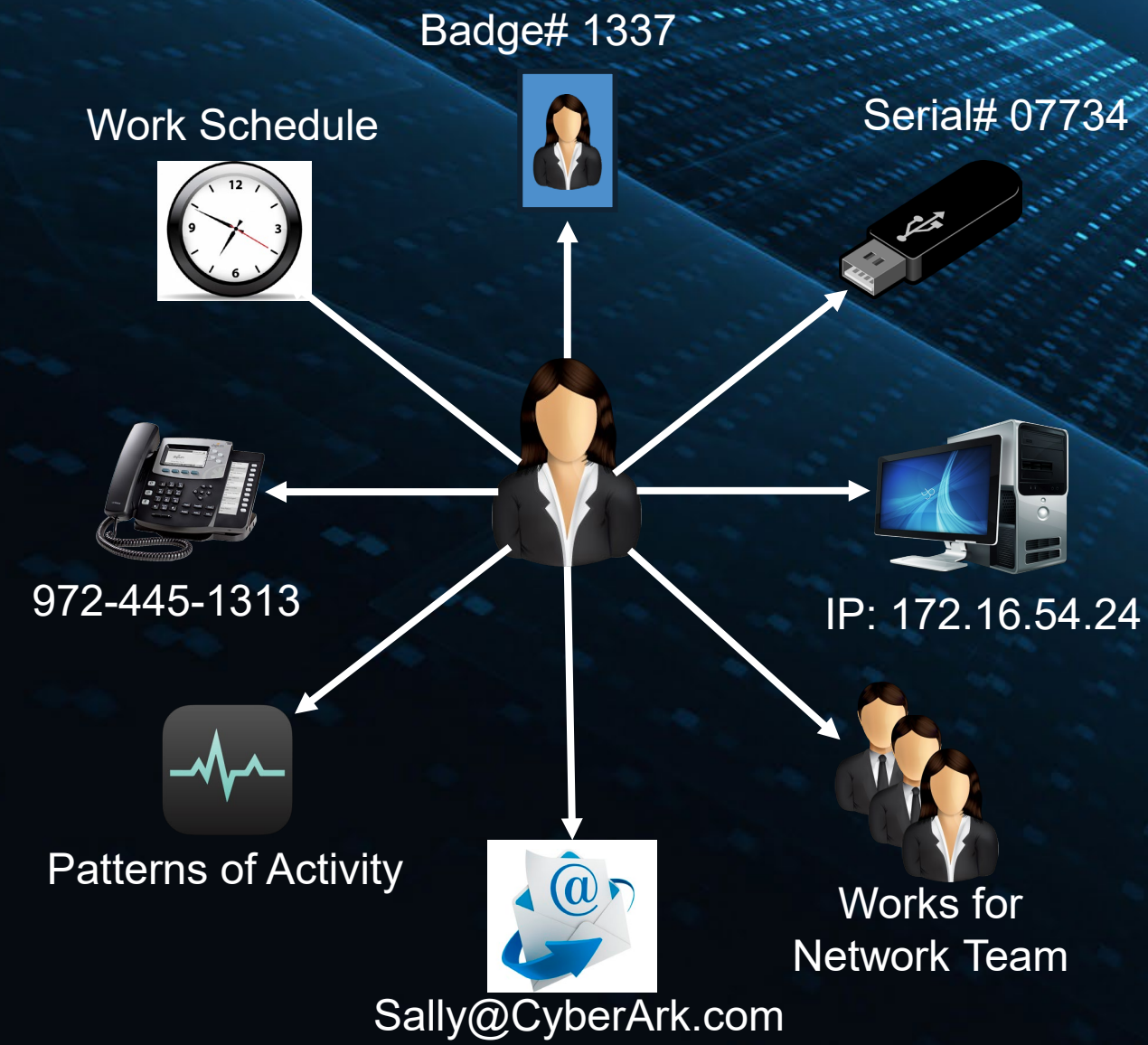


- Discover & Manage
  - Complex
  - Frequently Changing
  - Unique
- Single Conduit for Privileged Accounts.
- Limit an attacker's window & scope of attack opportunity.

LOGGING, MONITORING, & AUDITING

- Centralized logging to prevent log tampering.
- Gain visibility into the session itself.
  - Not just metadata.
- Can assist with recovering from sabotage

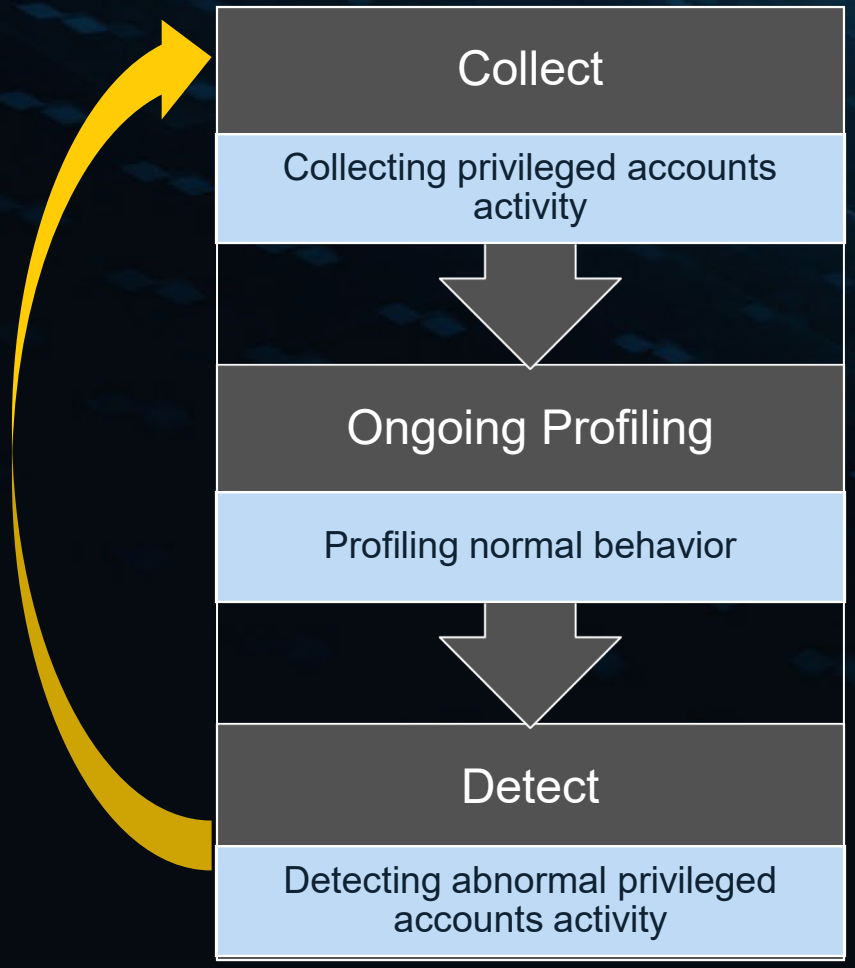
KNOW YOUR PEOPLE



SIEMS, ANALYTICS & HEURISTIC DETECTION

- Suspected credential theft.
- Unmanaged privileged access.
- Access via irregular hours.
- Access from irregular IP’s.
- Active vs dormant users.
- Anomalous access to multiple machines.
- Suspicious activities detected in privileged sessions.

LOOK FOR OUTLIERS IN BEHAVIORAL ANALYTICS



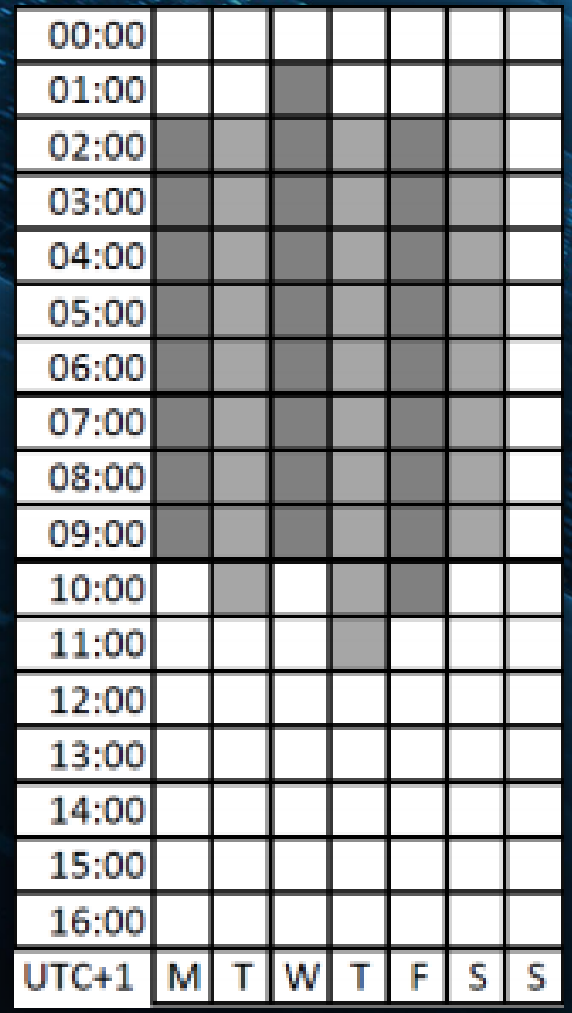
- Detect malicious privileged user behavior.
- Compare current activity to user and entity profiles.
- Patented CyberArk analytic technology detects and alerts on malicious behavior.
- Reduces the attacker's window of opportunity.
- One solution to detect both advanced external and insider threats.

CYBERARK

EXHIBIT A: TIME OF DAY. CRITICAL INDICATOR

- "…we were able to identify their working hours. Here is the average working hours for a week (the hour on the graph is UTC+1): Figure 1: Attackers working hours generally, the attackers worked between 2AM and 10AM from Monday to Saturday included."

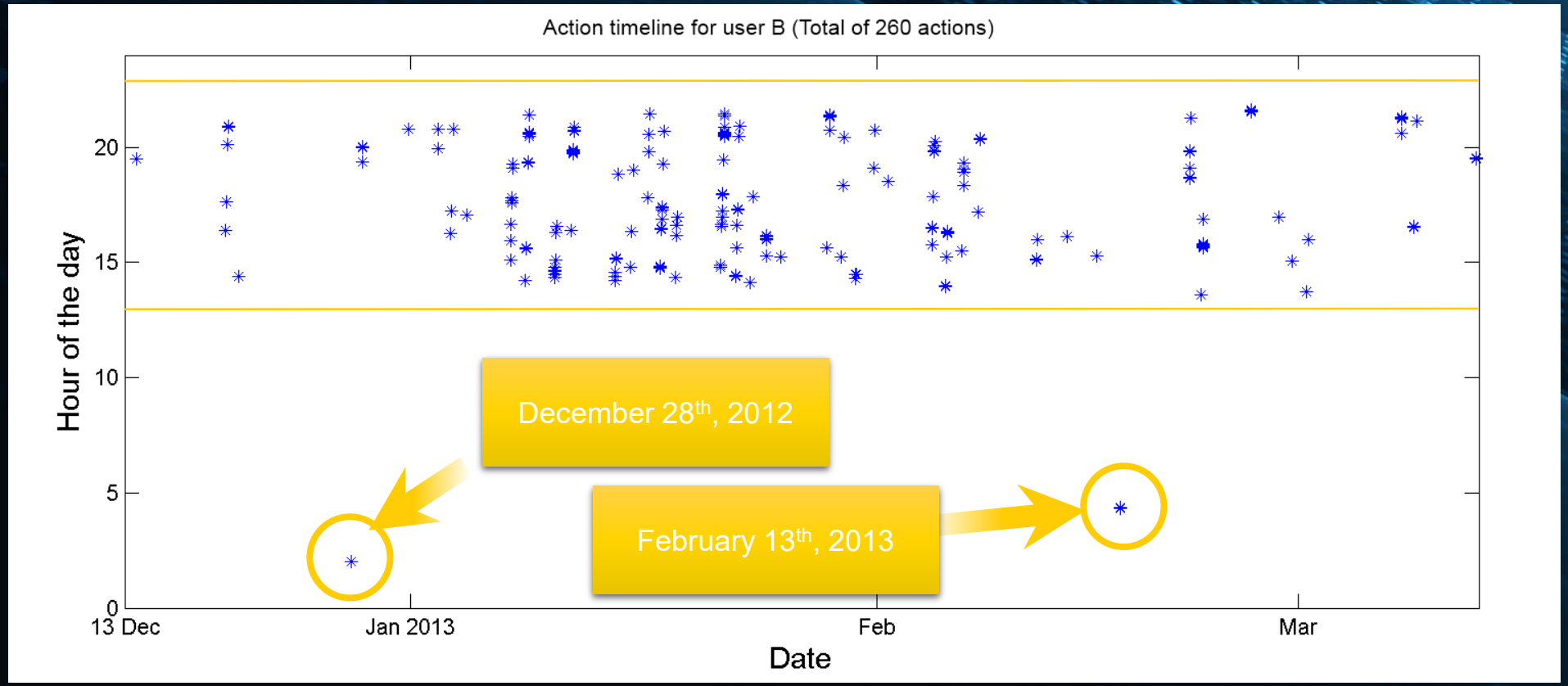
- The attacks came during the day in China, which is after hours in Europe and the US



Mandiant, APT1 Report – February 2013

CYBERARK

ACTIVITIES DURING IRREGULAR HOURS



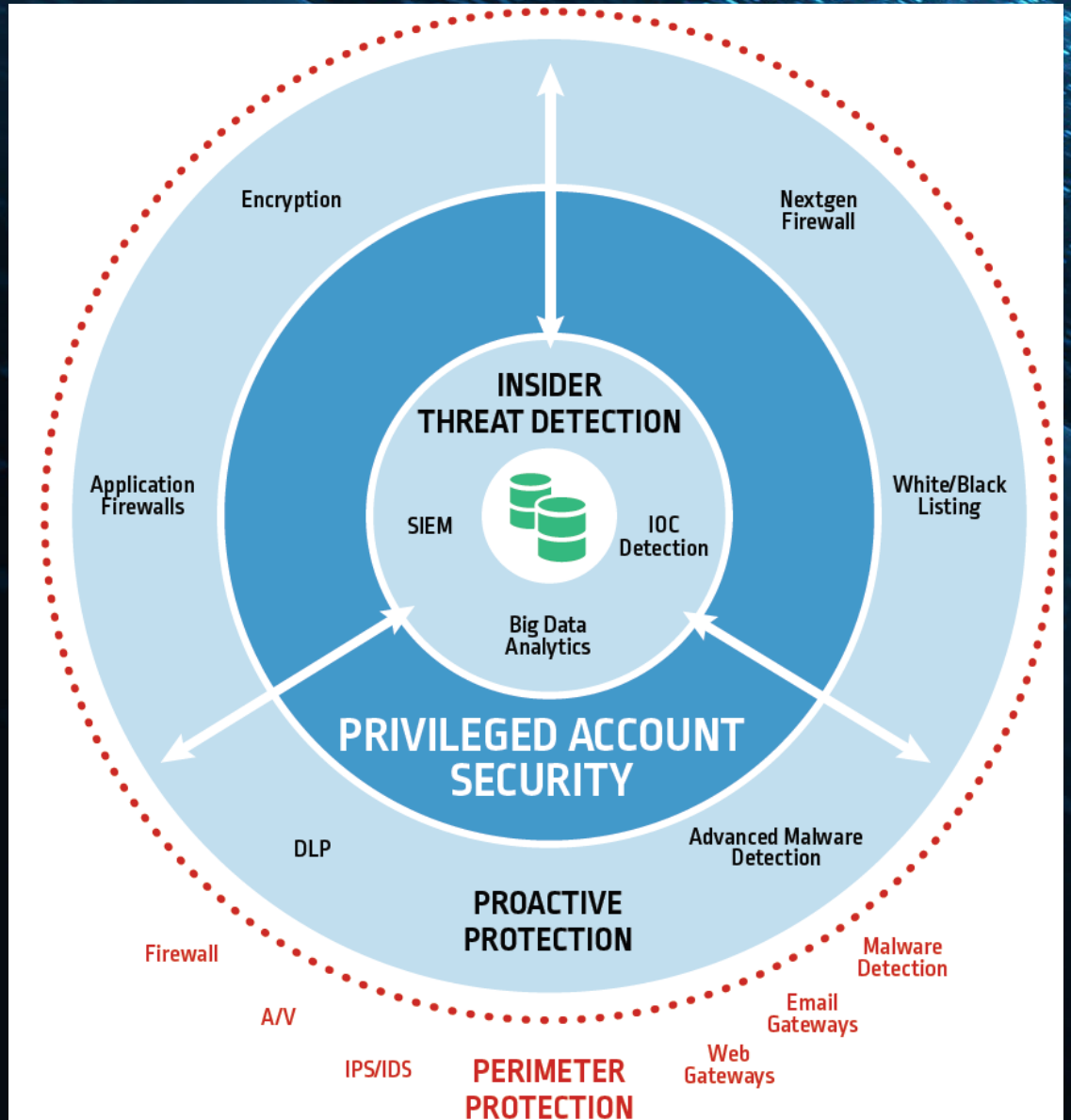
INSIDER THREAT: PRO-TIPS

- Look for Resume.doc
- Monitor frequent web traffic to:
  - LinkedIn
  - Monster.com, Jobs.com, etc
  - Pastebin, data dump sites
  - Competitors
- Pay close attention to disenfranchised employees
  - Passed over for promotion
  - Low performance evaluations
  - Recent HR events

PASTEBIN

CYBERARK

A ROBUST INSIDER THREAT PROGRAM



CONCLUSION

- Your organization's greatest asset is also it’s greatest threat.
- “It takes a village…”
- Technical Controls provide layers of security.
- Takeaways of things to monitor against.


CYBERARK
QUESTIONS?