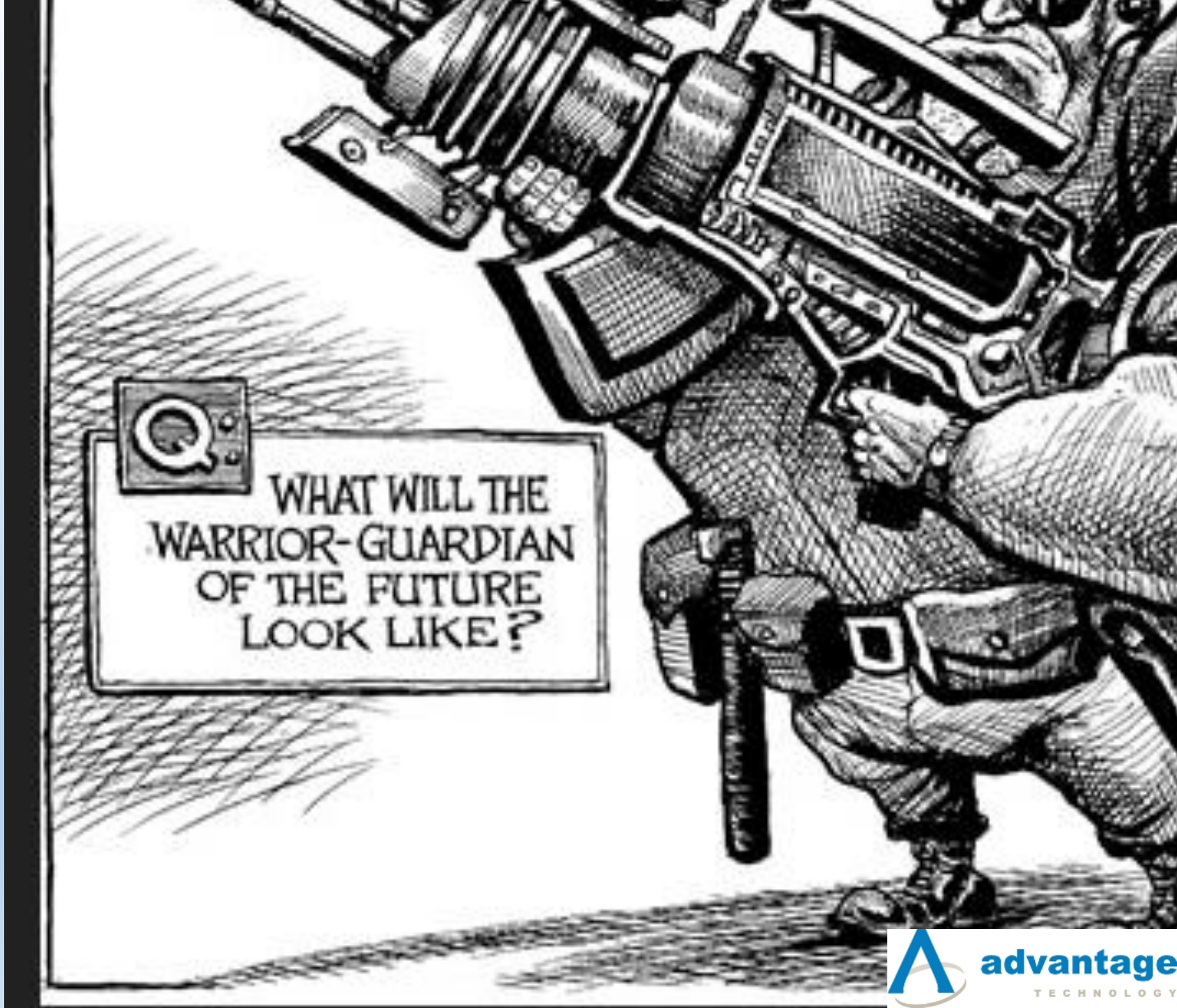

advantage
TECHNOLOGY
Cybersecurity:
Building Out With
Strategy

•#Whoami

Chris May

Director of Security

Advantage Technology



advantage
TECHNOLOGY

Recent Headlines*

- Surveys: Employees at fault in majority of breaches
- Deeper Dive: Human Error Is to Blame for Most Breaches
- The Biggest Cybersecurity Threats Are Inside Your Company
- Employee Errors Cause Most Data Breach Incidents in Cyber Attacks
- CISOs blame lack of competent staff for data breaches
- Undertrained employees are organizations' biggest cyber security weakness
- Companies' Employees To Blame For Cyber-Attacks: Report
- Fed Employees and Contractors to Blame for Half of Cyber-attacks
- Organizations blame their own staff for cloud security incidents

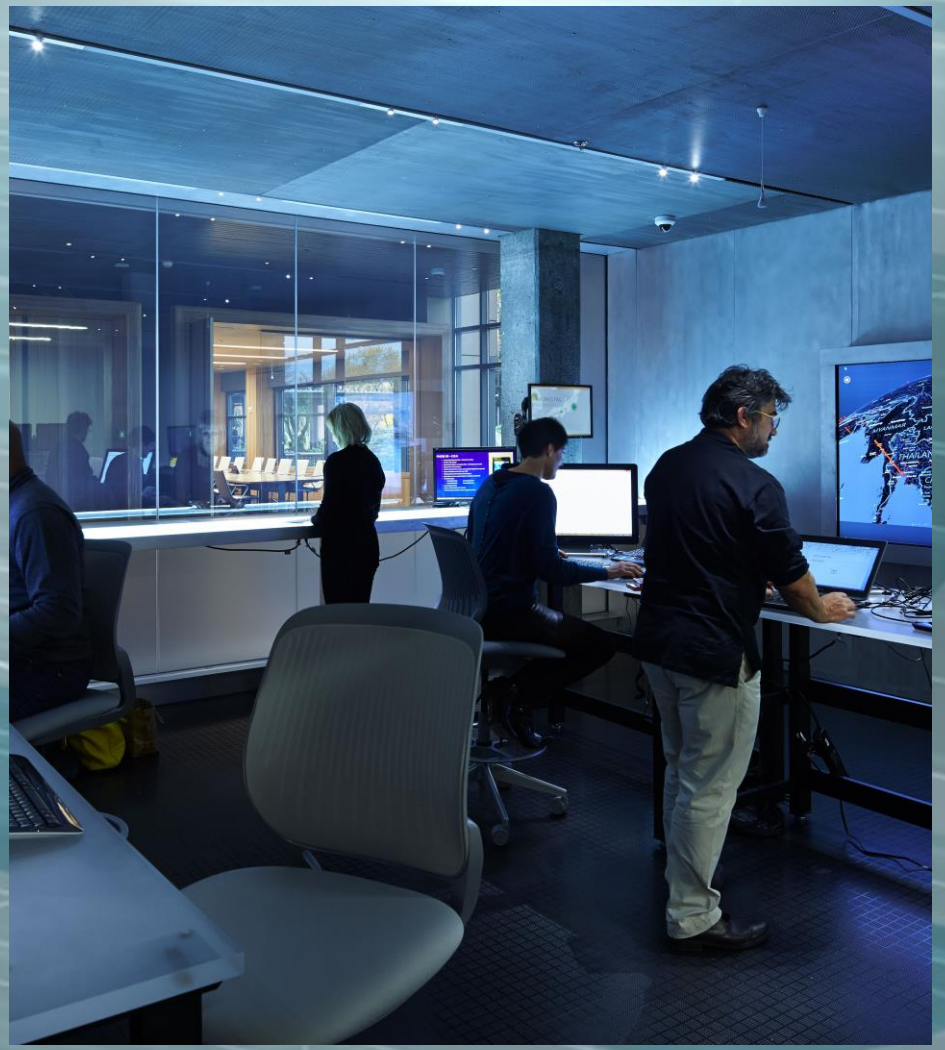
The Finger of Blame

“93 percent of all money is digital. That’s what is at risk here”

–Bill Nelson | Financial Services Information Sharing & Analysis Center

Agenda

- Overview of Cybercrime
- Today's Cyber Threats
- Cybercrime as a Service
- Best Practices

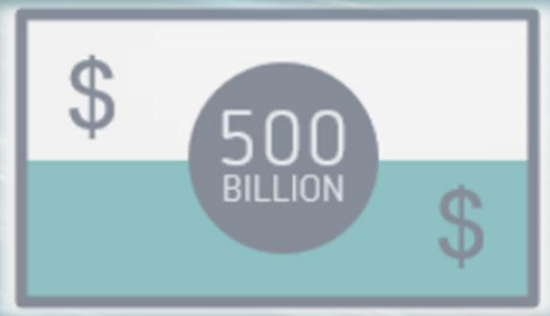


What is cybercrime?

Cybercrime is criminal activity involving the internet, a computer system, or computer technology.

50% of online adults

About half of online adults were cybercrime victims in the past year.



$500 billion

Cybercrime costs the global economy up to $500 billion annually.

20% of businesses

One in five small and medium businesses have been targeted.

What is **Blackhat** cybercrime?

Blackhat cybercrime is a form of malicious online behavior motivated by *profit* and a *predictable ROI*

Today's Cyber Threats

eCrime

- A botnet is a network of devices infected with malicious software that is centrally controlled
- "Good" malware cannot be detected by users

Phishing

- Email, Phone, SMS, FAX, Vmail, US Mail
- Campaigns can include spam, SMSishing, Vishing, etc.
- Credential Harvesting

Ransomware

- Got Bitcoin?
- It holds your PC or files for "ransom."
- Prevents you from using your PC
- Victim has to pay to regain access

Physical Security

- Access Cards
- ID Badges
- Delivery Personnel

Ransomware is the fastest growing threat…

How	Do	We	Prevent
• Train employees • Filter emails • Scan emails • Configure firewalls • Patch patch, patch • Good updated AV	• Manage the use of privileged accounts • Control access to network locations • Disable macros in emailed Office files • Implement Software Restriction Policies	• Disable Remote Desktop Protocol (RPD) • Use Whitelisting • Execute in a virtualized environment	• Physical and logical separation of networks

“Bad news isn't wine. It doesn't improve with age”

— Colin Powell | Retired four-star General United States Army

HELP!!

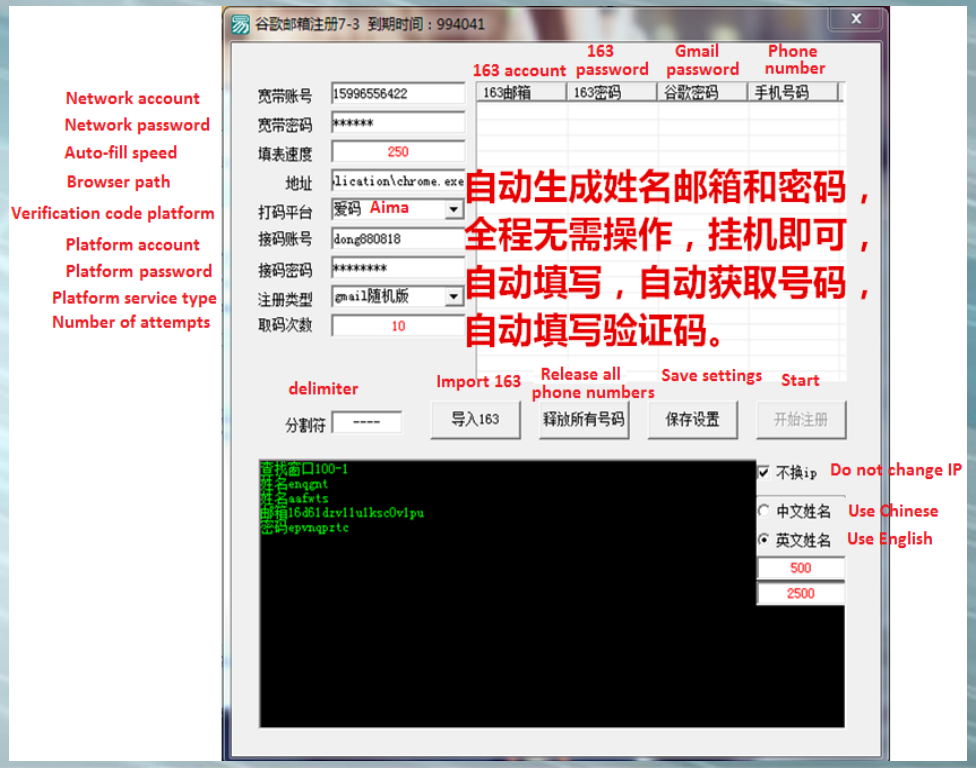
“If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked”

— Richard Clarke | Former White House Cyber Czar

It has never been easier for new entrants into the market

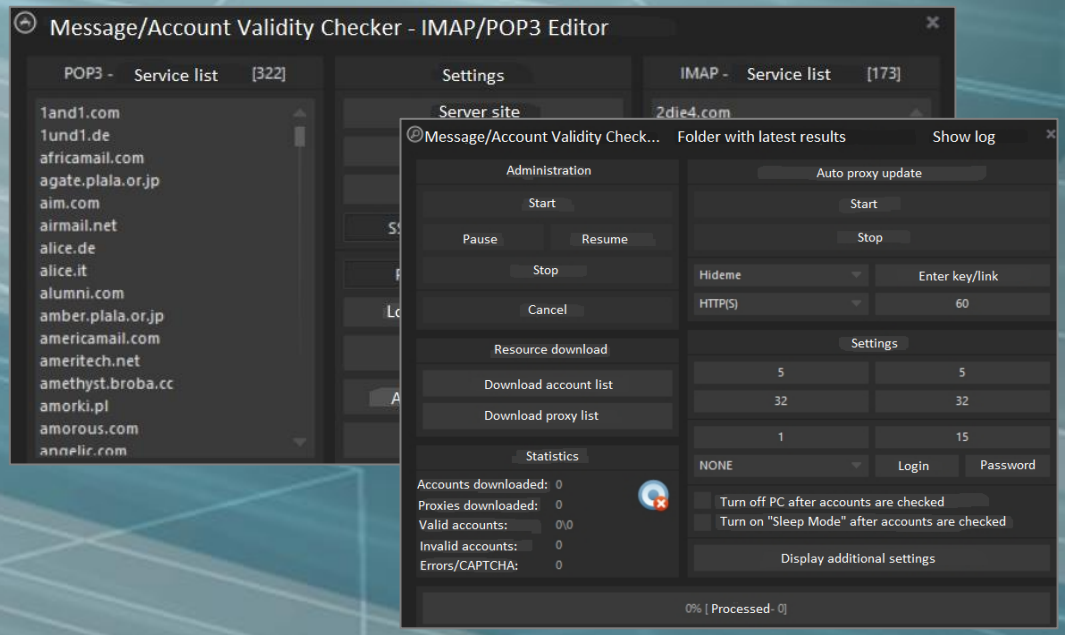
Cybercrime as a Service (CaaS): Crimekits and services available

Tools to create abuse accounts



Chinese **Gmail account creation tool**, interfaces with SMS and CAPTCHA solving services

Account Checkers

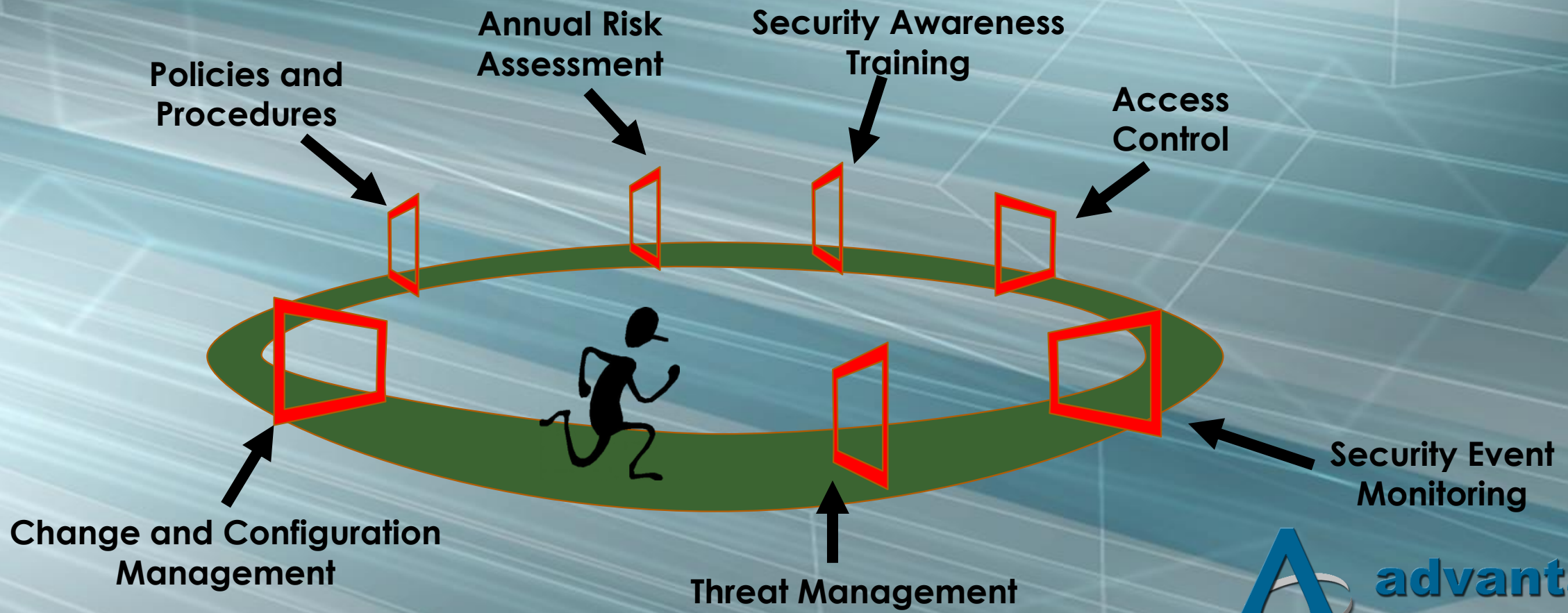


Russian checker **Private Keeper**. It is a universal checking tool supporting 17 different web services (PSN, PayPal, Skype, Twitter, etc.) and many email providers. It has an IMAP/POP3 server editor that supports "almost any email [illegible] to parse the content of messages and check email accounts [illegible]

Sources: Various

Best Practices To Safeguard Your Data

Information Security Process and Program



advantage TECHNOLOGY

Policies, Procedures and Information Security Program Consulting

- External CISO Advisory Services
- Staff Augmentation

advantage TECHNOLOGY

Vet your vendors

- Select service providers with strong security programs
- Make sure that they have adequate cyber insurance
- Contracts with vendors should have provisions related to audits/audit reports, insurance, breach notification, restrictions on use/disclosure of data, warranties about compliance with privacy obligations, & data return and disposal

advantage TECHNOLOGY

Security Awareness Training

- Instructor Led
- Testing
- Continuing Education
- On-line content

advantage TECHNOLOGY

Risk Analysis and Assessment

- Security Risk Assessments
  - NIST 800-53
- Vulnerability Scans
  - NESSUS
- Penetration Testing

advantage TECHNOLOGY

Risk assessment

Legal risk

- Sector specific enforcement (energy, health care, financial services, retail, etc.)
- FTC enforcement
- State AG enforcement
- Congressional investigations
- Class Action lawsuits

advantage TECHNOLOGY

Risk assessment

Legal assessment

- Policies/procedures
- Governance and implementation of policies
- Incident response plan
- Vendor selection
- Training
- Data mapping

advantage TECHNOLOGY

Risk assessment

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) released a voluntary methodology to assess and reduce cyber risks in *critical infrastructure* sectors. It was updated in 2017.

Your security program should be proportional to the data you handle and the size and nature of the business.

advantage TECHNOLOGY

Risk assessment

NIST recommends that you:

- Perform an company-wide vulnerability assessment
- Implement a comprehensive information security program
- Review your program periodically
- Implement data security policies, like data classification, password strength, access control, encryption, data disposal, and patch management
- Implement an incident response plan

advantage TECHNOLOGY

Difference between Penetration Testing and Vulnerability Assessment?

- *Vulnerability Assessment:*
  - Typically is general in scope and includes a large assessment.
  - Predictable. (I know when those darn Security guys scan us)
  - Unreliable at times and high rate of false positives. (I've got a banner)
  - Vulnerability assessment invites debate among System Admins.
  - Produces a report with mitigation guidelines and action items.

- *Penetration Testing:*
  - Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
  - Unpredictable by the recipient. (Don't know the "how?" and "when?")
  - Highly accurate and reliable. (I've got root!)
  - Penetration Testing = Proof of Concept against vulnerabilities.
  - Produces a binary result: Either the team owned you, or they didn't.

advantage TECHNOLOGY

Scope of Penetration Testing

- Targeted Recon.
  - Targeted exploitation of vulnerable software.
- Social Engineering
  - Hi HelpDesk…I'm Mr. Jones…Can you tell me what my password is?
- Physical facilities audit
  - Hmm, I forgot my badge… but there's 200 yards of fence missing on the east side of the center
- Wireless War Driving
  - Detection of rogue or weakly encrypted AP's.
- Dumpster Diving
  - How much fun can I have in the dumpster…whoops…I've found someone's Tax forms with SSN.

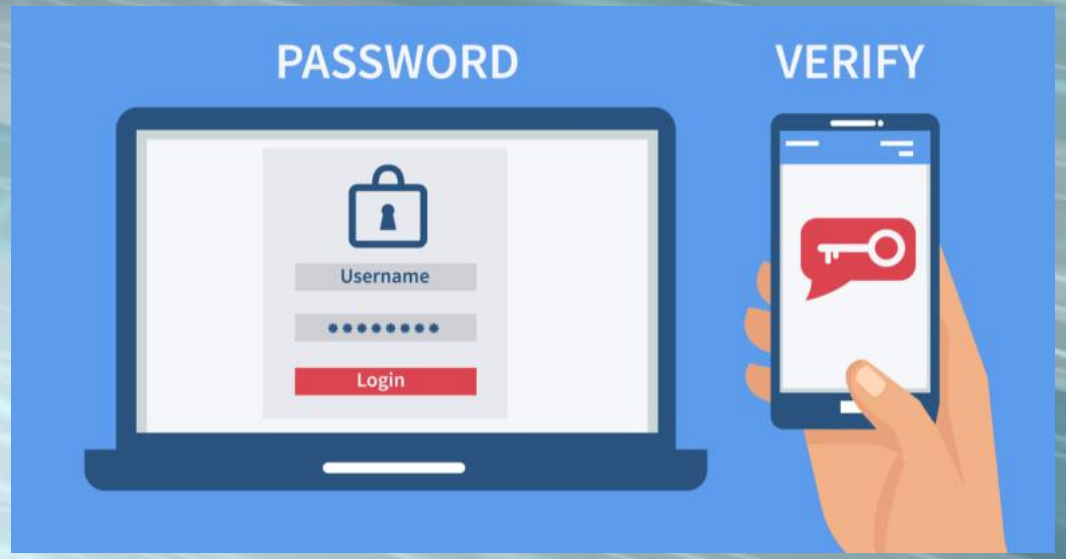
advantage TECHNOLOGY

Why Bother?

- Active pen-testing teaches you things that security planning will not
  - What are the vulnerability scanners missing?
- Are your users and system administrators actually following their own policies?
  - host that claims one thing in security plan but it totally different in reality
    - Audit Physical Security
    - Just what is in that building no one ever goes in?
    - The strongest network based protections are useless if there is a accessible unlocked terminal, unlocked tape vault, etc.
- Raises security awareness
  - I better not leave my terminal unlocked because I know that those security guys are lurking around somewhere.
- Helps identify weakness that may be leveraged by insider threat or accidental exposure.
- Provides Senior Management a realistic view of their security posture
- Great tool to advocate for more funding to mitigate flaws discovered
- If I can break into it, so could someone else!

advantage TECHNOLOGY

Authentication and Authorization



- Two factor or multi-factor authentication
  - Password and PIN
  - Biometrics
- Password managers
- Group Policies
  - Enforce “Least Privileges” rule

advantage TECHNOLOGY


SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

Change and Configuration Management

- Automation of configurations
  - Security Automation
- Patch management / automatic updates
- Change management software

advantage TECHNOLOGY

Threat Management

- Endpoint protection
  - Anti-virus
  - Spam filtering
  - Encryption
- Firewall
- Content Filtering
- Backup / Disaster recovery

advantage TECHNOLOGY


It’s OK,
You have a good backup, right?

Proper Backup Procedure

- Choose your application
- Scheduling
- Implementation
- Inventory (content and media)
- Verify
- Automate
- Secure

advantage TECHNOLOGY

Evolution of Security

Where most commercial companies want to be

SOC as a Service plays here

Where most commercial companies are today.

GAP

Containment and Remediation

Intrusion Containment

Remediation

Policy Update

Detection And Response

Log Aggregation & Correlation

Human / Threat Intelligence

Incident Detection & Response

Defense-in-Depth

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS/IPS/CASB

Perimeter

Firewalls

SPAM / Web Filters

WAF/Proxy

Basic

Passwords / AD

Patch Management

Backups

Prevention is not enough…

advantage TECHNOLOGY

What is the evolution?

NIST

53% cost per incident is spent in detection and response

240 days to detect a security incident

46 days to respond to security incident

1 Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

2 Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

3 Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

4 Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

5 Recover

- Recovery Planning
- Improvements
- Communications

Requires People & Time

advantage TECHNOLOGY

Security Positions in the US are a Challenge:

Talent is very expensive with familiarity building a SOC (Security Operations Center)

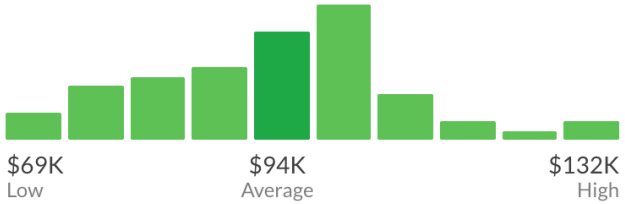
Senior Information Security Analyst Salaries

1,485 Salaries Updated Jul 13, 2018

Industries | Company Sizes | Years of Experience

Average Base Pay

$94,344 /yr



Additional Cash Compensation

Average	$6,291
Range	$1,223 - $16,981

How much does a Senior Information Security Analyst make?
The national average salary for a Senior Information Security Analyst is $94,344 in United States. Filter by... More

Information Security Architect Salaries

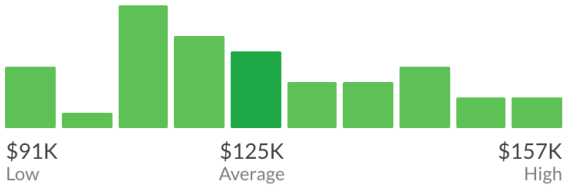
307 Salaries Updated Jun 5, 2018

Industries | Company Sizes | Years of Experience

To filter salaries for Information Security Architect, Sign In or Register.

Average Base Pay

$124,637 /yr



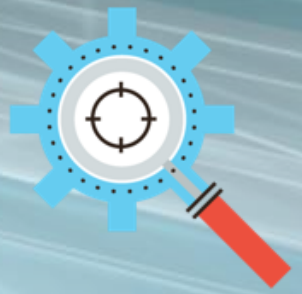
Additional Cash Compensation

Average	$xx,xxx
Range	$xx,xxx

How much does a Information Security Architect make?
The national average salary for a Information Security Architect is $124,637 in United States. Filter by... More

advantage TECHNOLOGY

Solution: SOC-as-a-**Service**



Comprehensive

Unified Security with centralized view

24x7 Monitoring

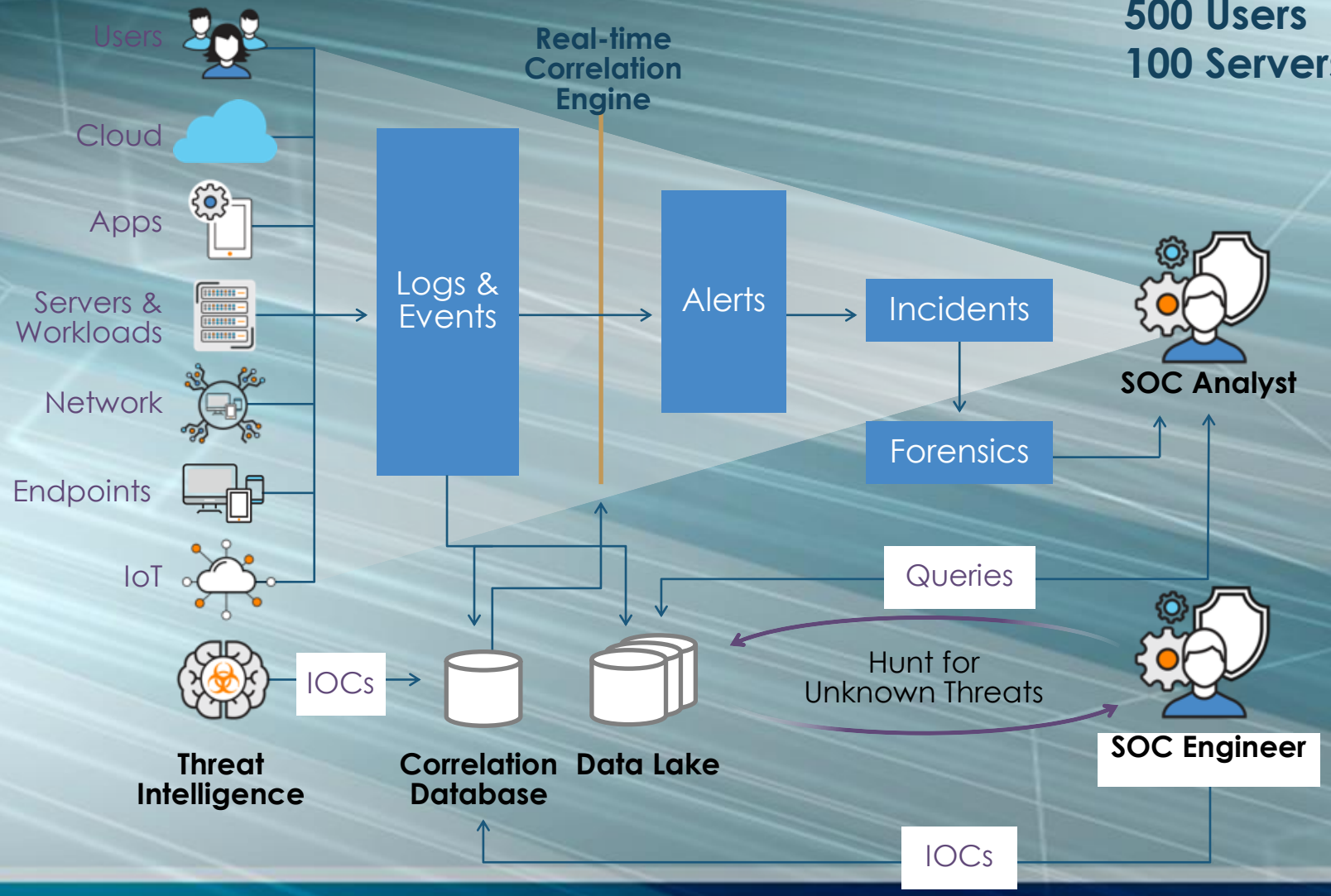
Focused on Managed Detection and Response

Predictable Pricing

Fixed monthly price faster, better, cheaper

advantage TECHNOLOGY

Backend Process



500 Users
100 Servers

~600M+ Observations/Week
~700-1000 Investigations/Week
~1-5 Incidents/Week

Real-time Correlation

- Analyze billions of events
- Real-time correlation against IOCs
- Reduced false positives

Forensics

- Search and research quickly
- Construct blast zone analysis and remediate

Hunt

- Hunt for unknown threats with deep analytics and machine learning
- Identify new IOCs to improve monitoring

advantage TECHNOLOGY

I finally realized it.
People are **prisoners**
of their phones,
that's why they are
called **cell** phones.

Spirit Science

Q & A